Configurar criptografia de volume e agregação do NetApp

ONTAP 9

NetApp
February 12, 2026

Índice

Configurar criptografia de volume e agregação do NetApp

Saiba mais sobre criptografia agregada e de volume do ONTAP 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 snapshots) 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 9.17.1, você pode usar Barbican KMS para proteger chaves NVE somente para SVMs de dados.
  - 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.

Os fornecedores de KMS em nuvem, como o Azure Key Vault e o AWS KMS, não são compatíveis com KMIP. Como resultado, eles não estão listados no 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 o Cloud Volumes ONTAP está disponível no ONTAP 9.5 e versões posteriores.
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	O MetroCluster é suportado a partir do ONTAP 9.8. A partir do ONTAP 9.6, o NVE oferece suporte ao escopo SVM somente para gerenciamento de chaves externas, não para o Onboard Key Manager.
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	O SnapLock é suportado nos modos Compliance e Enterprise, somente para novos volumes. Não é possível ativar a encriptação num volume SnapLock existente.

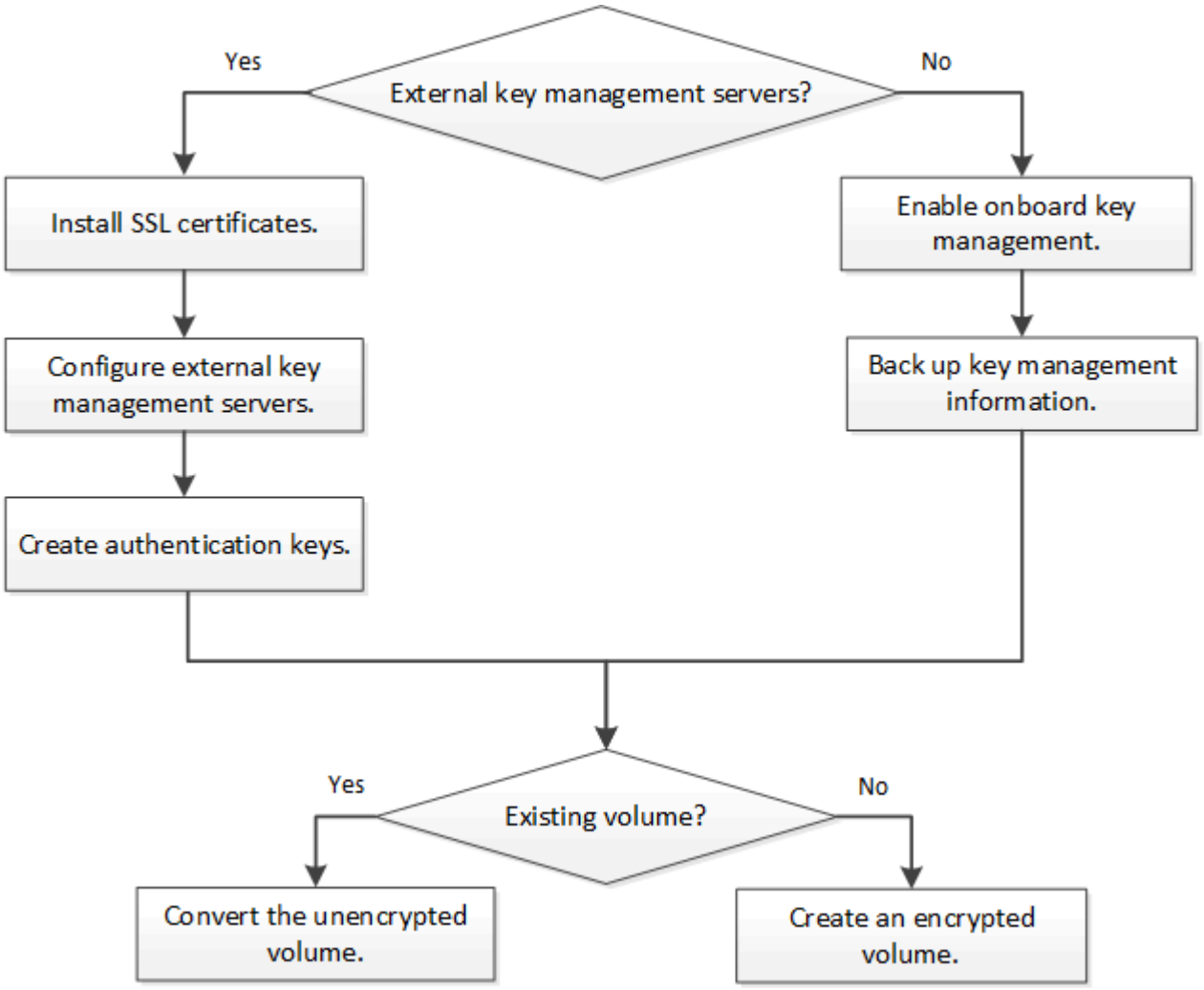
Volumes FlexGroup	Volumes FlexGroup são suportados. Os agregados de destino devem ser do mesmo tipo que os agregados de origem, tanto em nível de volume como em nível de agregado. A partir do ONTAP 9.5, é suportada a rechavear no local de volumes FlexGroup.
Transição de 7 modos	A partir da ferramenta 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"
- "criação de agregado de armazenamento"

Fluxo de trabalho de criptografia de volume ONTAP NetApp

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 seu cluster ONTAP oferece suporte a 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.

Passos

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

   ```
   version -v
   ```

   O 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".

Instalar a licença de criptografia de volume em um cluster ONTAP

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

Saiba mais sobre como configurar o gerenciamento de chaves externas com o ONTAP NetApp Volume Encryption

Você pode usar um ou mais servidores externos de gerenciamento de chaves para proteger as chaves que o cluster usa para acessar dados criptografados. Um servidor

externo de gerenciamento de chaves é um sistema de terceiros em seu ambiente de armazenamento que fornece chaves para nós usando o Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). Além do Gerenciador de Chaves Onboard, o ONTAP oferece suporte a vários servidores externos de gerenciamento de chaves.

A partir do ONTAP 9.10.1, você pode usar Azure Key Vault ou serviço Google Cloud Key Manager para proteger suas chaves NVE para SVMs de dados. A partir do ONTAP 9.11.1, é possível configurar vários gerenciadores de chaves externos em um cluster. VerConfigure servidores de chave em cluster . A partir do ONTAP 9.12.0, você pode usar "KMS DA AWS" para proteger suas chaves NVE para SVMs de dados. A partir do ONTAP 9.17.1, você pode usar o OpenStack. Barbican KMS para proteger suas chaves NVE para SVMs de dados.

Gerencie gerenciadores de chaves externas com o ONTAP 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**.

Migrar chaves entre os gerenciadores-chave

Quando vários gerenciadores de chaves estão habilitados em um cluster, as chaves devem ser migradas de um gerenciador de chaves para outro. Este processo é concluído automaticamente com o System Manager.

- Se o Gerenciador de chaves integrado ou um gerenciador de chaves externo estiver habilitado em um nível de cluster e alguns volumes estiverem criptografados, então, quando você configurar um gerenciador de chaves externo no nível de VM de armazenamento, as chaves devem ser migradas do Gerenciador de chaves integrado ou do gerenciador de chaves externo no nível do cluster para o gerenciador de chaves externo no nível de VM de armazenamento. Este processo é concluído automaticamente pelo System Manager.
- Se os volumes tiverem sido criados sem criptografia em uma VM de armazenamento, as chaves não precisarão ser migradas.

Instalar certificados SSL no cluster ONTAP

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
   ```

Informações relacionadas

- "instalação do certificado de segurança"

Habilitar gerenciamento de chaves externas para NVE no ONTAP 9.6 e posterior

Use 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

Você pode conectar até quatro servidores KMIP a um cluster ou SVM. Use pelo menos 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>`

  Saiba mais sobre `system license add` o "Referência do comando ONTAP"na .

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.

Saiba mais sobre `security key-manager key migrate` o "Referência do comando ONTAP"na .

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- O servidor KMIP deve ser acessível a partir da LIF de gerenciamento de nós de cada nó.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Em um ambiente MetroCluster :
  - O MetroCluster deve ser totalmente configurado antes de habilitar o gerenciamento de chaves externas.
  - Você deve instalar o mesmo certificado SSL KMIP em ambos os clusters.
  - Um gerenciador de chaves externo deve ser configurado 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 é o SVM de administração do cluster atual. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.

   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 do SVM, `SVM` o padrão é o SVM atual. 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. Saiba mais sobre `security key-manager external add-servers` o "Referência do comando ONTAP"na .

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. Saiba mais sobre `security key-manager external show-status` o "Referência do comando ONTAP"na .

```
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 ser totalmente configurado antes de converter os volumes.

Informações relacionadas

- Configurar servidores de chaves externas em cluster
- "adicionar licença do sistema"
- "gerenciador de chaves de segurança migração de chaves"
- "gerenciador de chaves de segurança servidores externos adicionais"
- "gerenciador de chaves de segurança externo show-status"

Habilitar gerenciamento de chaves externas para NVE 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 este comando em ambos os clusters. Saiba mais sobre `security key-manager setup` no"Referência do comando ONTAP" .

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`

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

```
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.

Gerenciar chaves NVE para SVMs de dados ONTAP 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 usará 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`*

   Saiba mais sobre `security key-manager external aws` o "Referência do comando ONTAP"na .

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`. Saiba mais sobre `cluster show` o "Referência do comando ONTAP"na .
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.

   Saiba mais sobre `security key-manager external azure` o "Referência do comando ONTAP"na .

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`. Saiba mais sobre `cluster show` o "Referência do comando ONTAP"na .

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 de `kms_wrapped_key_status` vai ser "`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 SVM LIF de dados.

   Saiba mais sobre `security key-manager external gcp` o "Referência do comando ONTAP"na .

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"
- "gerenciador de chaves de segurança externo"

Gerenciar chaves ONTAP com Barbican KMS

A partir do ONTAP 9.17.1, você pode usar o OpenStack "Barbican KMS" para proteger chaves de criptografia ONTAP . O Barbican KMS é um serviço para armazenamento e acesso seguro a chaves. O Barbican KMS pode ser usado para proteger chaves de Criptografia de Volume NetApp (NVE) para SVMs de dados. O Barbican conta com "OpenStack Keystone" , serviço de identidade do OpenStack, para autenticação.

Sobre esta tarefa

Você pode configurar o gerenciamento de chaves com o Barbican KMS usando a CLI ou a API REST do ONTAP . Com a versão 9.17.1, o suporte ao Barbican KMS apresenta as seguintes limitações:

- O Barbican KMS não é compatível com NetApp Storage Encryption (NSE) e NetApp Aggregate Encryption (NAE). Como alternativa, você pode usar "KMIPs externos" ou o "Gerenciador de Chaves de Bordo (OKM)" para chaves NSE e NVE.
- O Barbican KMS não é compatível com configurações do MetroCluster .
- O Barbican KMS só pode ser configurado para uma SVM de dados. Não está disponível para a SVM de administrador.

Salvo indicação em contrário, os administradores da `admin` nível de privilégio pode executar os seguintes procedimentos.

Antes de começar

- O Barbican KMS e o OpenStack Keystone devem ser configurados. A SVM que você está usando com o Barbican deve ter acesso à rede dos servidores Barbican e OpenStack Keystone .
- Se você estiver usando uma Autoridade de Certificação (CA) personalizada para os servidores Barbican e OpenStack Keystone , você deve instalar o certificado da CA com `security certificate install -type server-ca -vserver <admin_svm>` .

Criar e ativar uma configuração do Barbican KMS

Você pode criar uma nova configuração do Barbican KMS para uma SVM e ativá-la. Uma SVM pode ter várias configurações inativas do Barbican KMS, mas apenas uma pode estar ativa por vez.

Passos

1. Crie uma nova configuração inativa do Barbican KMS para um SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` é o identificador da chave de criptografia da chave Barbican (KEK). Insira um URL completo, incluindo `https://` .

> Algumas URLs incluem o caractere de ponto de interrogação (?). O ponto de interrogação ativa a ajuda ativa da linha de comando do ONTAP . Para inserir uma URL com um ponto de interrogação, você precisa primeiro desativar a ajuda ativa com o comando `set -active-help false` . A ajuda ativa pode ser reativada posteriormente com o comando `set -active-help true` . Saiba mais em "Referência do comando ONTAP" .

   - `-keystone-url` é a URL do host de autorização do OpenStack Keystone . Insira uma URL completa, incluindo `https://` .
   - `-application-cred-id` é o ID das credenciais do aplicativo.

     Após inserir este comando, você será solicitado a inserir a chave secreta das credenciais do aplicativo. Este comando cria uma configuração inativa do Barbican KMS.

     O exemplo a seguir cria uma nova configuração inativa do Barbican KMS chamada `config1` para o SVM `svm1` :

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Ative a nova configuração do Barbican KMS:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

Você pode usar este comando para alternar entre as configurações do Barbican KMS. Se já houver uma configuração ativa do Barbican KMS no SVM, ela será desativada e a nova configuração será ativada.

3. Verifique se a nova configuração do Barbican KMS está ativa:

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

Este comando fornecerá o status da configuração ativa do Barbican KMS no SVM ou nó. Por exemplo, se o SVM `svm1` no nó `node1` tem uma configuração ativa do Barbican KMS, o comando a seguir retornará o status dessa configuração:

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Atualizar as credenciais e configurações de uma configuração do Barbican KMS

Você pode visualizar e atualizar as configurações atuais de uma configuração ativa ou inativa do Barbican KMS.

Passos

1. Veja as configurações atuais do Barbican KMS para um SVM:

```
security key-manager external barbican show -vserver <svm_name>
```

O ID da chave, o URL do OpenStack Keystone e o ID das credenciais do aplicativo são exibidos para cada configuração do Barbican KMS no SVM.

2. Atualizar as configurações de uma configuração do Barbican KMS:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

Este comando atualiza as configurações de tempo limite e verificação da configuração especificada do Barbican KMS. `timeout` determina o tempo em segundos que o ONTAP aguardará a resposta do Barbican antes que a conexão falhe. O padrão `timeout` são dez segundos. `verify` e `verify-host` determinar se a identidade e o nome do host do host Barbican devem ser verificados antes da conexão. Por padrão, esses parâmetros são definidos como `true` . O `vserver` e `config-name` parâmetros são obrigatórios. Os demais parâmetros são opcionais.

3. Se necessário, atualize as credenciais de uma configuração ativa ou inativa do Barbican KMS:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

Após digitar este comando, você será solicitado a informar a nova chave secreta de credenciais do aplicativo.

4. Se necessário, restaure uma chave de criptografia de chave SVM ausente (KEK) para uma configuração ativa do Barbican KMS:
   a. Restaurar uma SVM KEK ausente com `security key-manager external barbican restore` :

```
security key-manager external barbican restore -vserver <svm_name>
```

Este comando restaurará a SVM KEK para a configuração ativa do Barbican KMS comunicando-se com o servidor Barbican.

5. Se necessário, troque a chave SVM KEK para uma configuração Barbican KMS:
   a. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

   b. Redigite o SVM KEK com `security key-manager external barbican rekey-internal` :

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

Este comando gera uma nova KEK SVM para a SVM especificada e reempacota as chaves de criptografia do volume com a nova KEK SVM. A nova KEK SVM será protegida pela configuração ativa do Barbican KMS.

Migrar chaves entre o Barbican KMS e o Onboard Key Manager

Você pode migrar chaves do Barbican KMS para o Gerenciador de Chaves Onboard (OKM) e vice-versa. Para saber mais sobre o OKM, consulte "Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior" .

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Se necessário, migre as chaves do Barbican KMS para o OKM:

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

`svm_name` é o nome do SVM com a configuração do Barbican KMS.

3. Se necessário, migre as chaves do OKM para o Barbican KMS:

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

Desabilitar e excluir uma configuração do Barbican KMS

Você pode desabilitar uma configuração ativa do Barbican KMS sem volumes criptografados e pode excluir uma configuração inativa do Barbican KMS.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Desabilitar uma configuração ativa do Barbican KMS:

```
security key-manager keystore disable -vserver <svm_name>
```

Se existirem volumes criptografados NVE no SVM, você deverá descriptografá-los ou migrar as chaves antes de desabilitar a configuração do Barbican KMS. A ativação de uma nova configuração do Barbican KMS não exige a descriptografia de volumes NVE nem a migração de chaves, e desabilitará a configuração ativa do Barbican KMS.

3. Excluir uma configuração inativa do Barbican KMS:

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Habilitar o gerenciamento de chaves integrado para NVE no ONTAP 9.6 e posterior

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.

Saiba mais sobre `security key-manager onboard enable` e `security key-manager onboard sync` no"Referência do comando ONTAP" .

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 Classificados (CSfC), você deve usar o NSE com o NVE e garantir que o Onboard Key Manager esteja habilitado no modo Common Criteria. Ver"Resumo da solução 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 você não digitar a senha do cluster 5 vezes, aguarde 24 horas ou reinicie o nó para 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 de atualização verifica se o conteúdo da imagem não foi alterado ou corrompido, verificando várias assinaturas digitais. O sistema prossegue para a próxima etapa no processo de atualização da imagem se a validação for bem-sucedida; caso contrário, a atualização da imagem falha. Saiba mais sobre `cluster image` no"Referência do comando ONTAP" .

O Onboard Key Manager armazena chaves na memória volátil. O conteúdo da memória volátil é limpo quando o sistema é reinicializado ou interrompido. O sistema limpa a memória volátil em 30 segundos quando é 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.

2. Digite uma senha entre 32 e 256 caracteres ou, para “cc-mode”, uma senha entre 64 e 256 caracteres.

   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.

Saiba mais sobre `security key-manager key query` o "Referência do comando ONTAP"na .

5. Opcionalmente, você pode converter 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.

Depois de configurar a senha do Onboard Key Manager, faça backup manualmente das informações em um local seguro fora do sistema de armazenamento. Ver"Faça backup manual das informações de gerenciamento de chaves integradas" .

Informações relacionadas

- "comandos de imagem de cluster"
- "gerenciador de chaves de segurança externo habilitado"
- "consulta de chave do gerenciador de chaves de segurança"
- "habilitar gerenciador de chaves de segurança integrado"

Habilitar o gerenciamento de chaves integrado para NVE no ONTAP 9.5 e versões anteriores

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 usar NSE ou NVE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externas.

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

- Você deve ser um administrador de cluster para executar esta tarefa.
- Configure o ambiente MetroCluster antes de configurar o Onboard Key Manager.

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 show-key-store`

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

   Node: node1
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK

   Node: node2
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK
   ```

   Saiba mais sobre `security key-manager show-key-store` no"Referência do comando ONTAP" .

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

   `volume encryption conversion start`

   Configure o Onboard Key Manager antes de converter volumes. Em ambientes MetroCluster , configure-o em ambos os sites.

Depois de terminar

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

Ao configurar a senha do Onboard Key Manager, faça backup das informações em um local seguro fora do sistema de armazenamento, em caso de desastre. Ver"Faça backup manual das informações de gerenciamento de chaves integradas" .

Informações relacionadas

- "Faça backup manual das informações de gerenciamento de chaves integradas"
- "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"
- "gerenciador de chaves de segurança mostrar-armazenamento-de-chaves"

Habilitar o gerenciamento de chaves integrado em nós ONTAP 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 9.6 e versões posteriores, você deve executar o `security key-manager onboard sync` comando a cada vez que você adiciona um nó ao cluster.

Para o ONTAP 9.5 e versões anteriores, você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.

Se você adicionar um nó a um cluster com gerenciamento de chaves integrado, execute este 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.

  Saiba mais sobre `security key-manager onboard enable` e `security key-manager onboard sync` no "Referência do comando ONTAP".

- 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`.

Se a tentativa de senha falhar, reinicie o nó. Após a reinicialização, você pode tentar inserir a senha novamente.

Informações relacionadas

- "comandos de imagem de cluster"
- "gerenciador de chaves de segurança externo habilitado"
- "habilitar gerenciador de chaves de segurança integrado"

Criptografar dados de volume com NVE ou NAE

Aprenda sobre a criptografia de dados de volume ONTAP com 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.

Habilite a criptografia em nível agregado com licença VE no ONTAP

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`

Saiba mais sobre `storage aggregate modify` no "Referência do comando ONTAP" .

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
```

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

2. Verifique se o agregado está habilitado para criptografia:

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

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.
```

Saiba mais sobre `storage aggregate show` o "Referência do comando ONTAP"na .

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 no ONTAP

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`

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

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.

Habilitar NAE ou NVE em um volume ONTAP 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

Você pode usar o `volume encryption conversion start` comando para habilitar a criptografia de um volume existente "no local", sem precisar mover o volume para um local diferente. Como alternativa, você pode usar o comando `volume move start` comando.

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

Você pode usar o `volume encryption conversion start` comando para habilitar a criptografia de um volume existente "no local", sem precisar 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`

   Saiba mais sobre `volume encryption conversion start` o "Referência do comando ONTAP"na .

   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`

   Saiba mais sobre `volume encryption conversion show` o "Referência do comando ONTAP"na .

   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`

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

   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 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`

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

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.

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

   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`

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

   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 NVE em um volume raiz ONTAP 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`

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

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**.

Configurar NVE em um volume raiz de nó ONTAP

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
```

Informações sobre direitos autorais

Informações sobre marcas comerciais