Criptografia de dados de volume com NVE

ONTAP 9

NetApp
January 17, 2025

Índice

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
```

Informações sobre direitos autorais

Informações sobre marcas comerciais