Crittografare i dati del volume con NVE

ONTAP 9

NetApp
September 12, 2024

Sommario

Crittografare i dati del volume con NVE

Crittografare i dati del volume con la panoramica di NVE

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita quando si dispone della licenza VE e della gestione delle chiavi integrata o esterna. Per ONTAP 9.6 e versioni precedenti, è possibile attivare la crittografia su un nuovo volume o su un volume esistente. Prima di attivare la crittografia dei volumi, è necessario aver installato la licenza VE e attivato la gestione delle chiavi. NVE è conforme a FIPS-140-2 livello 1.

Abilitare la crittografia a livello aggregato con la licenza VE

A partire da ONTAP 9.7, gli aggregati e i volumi appena creati sono criptati per impostazione predefinita quando si dispone della "Licenza VE"gestione delle chiavi integrata o esterna. A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare.

A proposito di questa attività

Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato. La deduplica a livello di aggregato non è altrimenti supportata da NVE.

Un aggregato abilitato per la crittografia a livello di aggregato è denominato *aggregato NAE* (per NetApp aggregate Encryption). Tutti i volumi in un aggregato NAE devono essere crittografati con crittografia NAE o NVE. Con la crittografia a livello di aggregato, i volumi creati nell'aggregato vengono crittografati con la crittografia NAE per impostazione predefinita. È possibile eseguire l'override del valore predefinito per utilizzare la crittografia NVE.

I volumi di testo normale non sono supportati negli aggregati NAE.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Attivare o disattivare la crittografia a livello di aggregato:

Per…	Utilizzare questo comando…
Creare un aggregato NAE con ONTAP 9.7 o versione successiva	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Crea un aggregato NAE con ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

Convertire un aggregato non NAE in un aggregato NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Convertire un aggregato NAE in un aggregato non NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando attiva la crittografia a livello di aggregato `aggr1`:

- ONTAP 9.7 o versione successiva:

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

- ONTAP 9.6 o versioni precedenti:

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

2. Verificare che l'aggregato sia abilitato per la crittografia:

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

   Per la sintassi completa dei comandi, vedere la pagina man.

   Il seguente comando verifica `aggr1` è abilitato per la crittografia:

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

Al termine

Eseguire `volume create` per creare i volumi crittografati.

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia automaticamente" una chiave di crittografia al server quando si crittografa un volume.

Attivare la crittografia su un nuovo volume

È possibile utilizzare `volume create` per attivare la crittografia su un nuovo volume.

A proposito di questa attività

È possibile crittografare i volumi utilizzando NetApp Volume Encryption (NVE) e, a partire da ONTAP 9.6, NetApp aggregate Encryption (NAE). Per ulteriori informazioni su NAE e NVE, fare riferimento a. panoramica sulla crittografia dei volumi.

La procedura per attivare la crittografia su un nuovo volume in ONTAP varia in base alla versione di ONTAP in uso e alla configurazione specifica:

- A partire da ONTAP 9.4, se si attiva `cc-mode` Quando si configura Onboard Key Manager, i volumi creati con `volume create` i comandi vengono crittografati automaticamente, indipendentemente dal fatto che l'utente lo specifichi o meno `-encrypt true`.
- In ONTAP 9.6 e versioni precedenti, è necessario utilizzare `-encrypt true` con `volume create` comandi per attivare la crittografia (a condizione che non sia stata attivata) `cc-mode`).
- Se si desidera creare un volume NAE in ONTAP 9.6, è necessario attivare NAE a livello di aggregato. Fare riferimento a. Abilitare la crittografia a livello di aggregato con la licenza VE per ulteriori dettagli su questa attività.
- A partire da ONTAP 9.7, i volumi appena creati sono criptati per impostazione predefinita quando si dispone della "Licenza VE"gestione della chiave integrata o esterna. Per impostazione predefinita, i nuovi volumi creati in un aggregato NAE saranno di tipo NAE anziché NVE.
  - In ONTAP 9.7 e versioni successive, se si aggiunge `-encrypt true` al `volume create` Comando per creare un volume in un aggregato NAE, il volume avrà la crittografia NVE invece di NAE. Tutti i volumi in un aggregato NAE devono essere crittografati con NVE o NAE.

> I volumi non in testo normale non sono supportati negli aggregati NAE.

Fasi

1. Creare un nuovo volume e specificare se la crittografia è attivata sul volume. Se il nuovo volume si trova in un aggregato NAE, per impostazione predefinita il volume sarà un volume NAE:

Per creare…	Utilizzare questo comando…
Un volume NAE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Un volume NVE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` In ONTAP 9.6 e versioni precedenti, dove non è supportato il servizio NAE, `-encrypt true` Specifica che il volume deve essere crittografato con NVE. In ONTAP 9.7 e versioni successive, dove i volumi vengono creati in aggregati NAE, `-encrypt true` Esegue l'override del tipo di crittografia predefinito di NAE per creare un volume NVE.

Un volume di testo normale	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

Per la sintassi completa dei comandi, fare riferimento alla pagina di riferimento dei comandi per `volume create`.

2. Verificare che i volumi siano abilitati per la crittografia:

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

   Per la sintassi completa dei comandi, vedere "Riferimento al comando ONTAP".

Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia" automaticamente una chiave di crittografia al server quando si crittografa un volume.

= :allow-uri-read:

Attivare la crittografia su un volume esistente

È possibile utilizzare il `volume move start` o il `volume encryption conversion start` per abilitare la crittografia su un volume esistente.

A proposito di questa attività

- A partire da ONTAP 9.3, è possibile utilizzare `volume encryption conversion start` comando per abilitare la crittografia di un volume esistente "sul posto", senza dover spostare il volume in una posizione diversa. In alternativa, è possibile utilizzare `volume move start` comando.
- Per ONTAP 9,2 e versioni precedenti, è possibile utilizzare solo `volume move start` per attivare la crittografia spostando un volume esistente.

Attivare la crittografia su un volume esistente con il comando di avvio della conversione della crittografia del volume

A partire da ONTAP 9.3, è possibile utilizzare `volume encryption conversion start` comando per abilitare la crittografia di un volume esistente "sul posto", senza dover spostare il volume in una posizione diversa.

Dopo aver avviato un'operazione di conversione, è necessario completarla. Se si verificano problemi di prestazioni durante l'operazione, è possibile eseguire `volume encryption conversion pause` per sospendere l'operazione e il `volume encryption conversion resume` per riprendere l'operazione.

> Non è possibile utilizzare `volume encryption conversion start` Per convertire un volume SnapLock.

Fasi

1. Abilitare la crittografia su un volume esistente:

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

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando consente la crittografia sul volume esistente `vol1`:

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

Il sistema crea una chiave di crittografia per il volume. I dati del volume vengono crittografati.

2. Verificare lo stato dell'operazione di conversione:

   `volume encryption conversion show`

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza lo stato dell'operazione di conversione:

```
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. Una volta completata l'operazione di conversione, verificare che il volume sia abilitato per la crittografia:

   `volume show -is-encrypted true`

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza i volumi crittografati su `cluster1`:

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

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

Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia automaticamente" una chiave di crittografia al server quando si crittografa un volume.

Attivare la crittografia su un volume esistente con il comando di avvio spostamento volume

È possibile utilizzare `volume move start` per attivare la crittografia spostando un volume esistente. È necessario utilizzare `volume move start` In ONTAP 9.2 e versioni precedenti. È possibile utilizzare lo stesso aggregato o un aggregato diverso.

A proposito di questa attività

- A partire da ONTAP 9.8, è possibile utilizzare `volume move start` Per attivare la crittografia su un volume SnapLock o FlexGroup.
- A partire da ONTAP 9.4, se si attiva “cc-mode” quando si imposta il Gestore chiavi integrato, i volumi creati con `volume move start` i comandi vengono crittografati automaticamente. Non è necessario specificare `-encrypt-destination true`.
- A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all’aggregato contenente per i volumi da spostare. Un volume crittografato con una chiave univoca è chiamato *volume NVE* (ovvero utilizza la crittografia del volume NetApp). Un volume crittografato con una chiave a livello di aggregato viene chiamato *volume NAE* (per NetApp aggregate Encryption). I volumi non in testo normale non sono supportati negli aggregati NAE.
- A partire da ONTAP 9.14.1, puoi crittografare un volume root di una SVM con NVE. Per ulteriori informazioni, vedere Configurare la crittografia dei volumi NetApp su un volume root della SVM.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o un amministratore SVM al quale l’amministratore del cluster ha delegato l’autorità.

"Delega dell’autorizzazione all’esecuzione del comando di spostamento del volume"

Fasi

1. Spostare un volume esistente e specificare se la crittografia è attivata sul volume:

Per convertire…	Utilizzare questo comando…
Un volume non crittografato su un volume NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
Un volume NVE o plaintext su un volume NAE (supponendo che la crittografia a livello di aggregato sia attivata sulla destinazione)	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
Un volume NAE su un volume NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
Un volume NAE su un volume non crittografato	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
Un volume NVE su un volume non crittografato	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

Per l’intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando converte un volume non crittografato denominato `vol1` Su un volume NVE:

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

Supponendo che la crittografia a livello di aggregato sia attivata sulla destinazione, il seguente comando converte un volume NVE o non crittografato denominato `vol1` Su un volume NAE:

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

Il seguente comando converte un volume NAE denominato `vol2` Su un volume NVE:

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

Il seguente comando converte un volume NAE denominato `vol2` su un volume non crittografato:

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

Il seguente comando converte un volume NVE denominato `vol2` su un volume non crittografato:

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

2. Visualizzare il tipo di crittografia dei volumi del cluster:

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

   Il `encryption-type` Field è disponibile in ONTAP 9.6 e versioni successive.

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza il tipo di crittografia dei volumi in `cluster2`:

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

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

3. Verificare che i volumi siano abilitati per la crittografia:

   `volume show -is-encrypted true`

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza i volumi crittografati su `cluster2`:

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

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

Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP invia automaticamente una chiave di crittografia al server quando si crittografa un volume.

Configurare la crittografia dei volumi NetApp su un volume root della SVM

A partire da ONTAP 9.14.1, puoi abilitare NetApp Volume Encryption (NVE) su un volume root di una Storage VM (SVM). Con NVE, il volume root è crittografato con una chiave univoca, abilitando una maggiore sicurezza sulla SVM.

A proposito di questa attività

NVE su un volume root di SVM può essere abilitato solo dopo che è stata creata la SVM.

Prima di iniziare

- Il volume root della SVM non deve trovarsi in un aggregato crittografato con crittografia degli aggregati NetApp (NAE).
- È necessario aver abilitato la crittografia con Onboard Key Manager o con un gestore di chiavi esterno.
- È necessario eseguire ONTAP 9.14.1 o versione successiva.
- Per migrare una SVM contenente un volume root crittografato con NVE, al termine della migrazione è necessario convertire il volume root della SVM in un volume di testo normale, quindi crittografare di nuovo il volume root della SVM.

    - Se l'aggregato di destinazione della migrazione SVM utilizza NAE, il volume root eredita NAE per impostazione predefinita.
- Se la SVM si trova in una relazione di disaster recovery della SVM:
    - Le impostazioni di crittografia su una SVM con mirroring non vengono copiate nella destinazione. Se abiliti NVE sull'origine o sulla destinazione, devi abilitare NVE separatamente sul volume root della SVM con mirroring.
    - Se tutti gli aggregati nel cluster di destinazione utilizzano NAE, il volume root della SVM utilizzerà NAE.

Fasi

Puoi abilitare NVE su un volume root di SVM con l'interfaccia a riga di comando di ONTAP o System Manager.

CLI

È possibile abilitare NVE sul volume root della SVM in-place o spostando il volume tra aggregati.

Crittografare il volume root in uso

1. Convertire il volume root in un volume crittografato:

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

2. Conferma crittografia riuscita. Il `volume show -encryption-type volume` Visualizza un elenco di tutti i volumi che utilizzano NVE.

Crittografa il volume root della SVM spostandolo

1. Avvio dello spostamento di un volume:

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

   Per ulteriori informazioni su `volume move`, vedere Spostare un volume.

2. Confermare `volume move` operazione riuscita con il `volume move show` comando. Il `volume show -encryption-type volume` Visualizza un elenco di tutti i volumi che utilizzano NVE.

System Manager

1. Passare a **archiviazione** > **volumi**.
2. Accanto al nome del volume root SVM che si desidera crittografare, selezionare ⋮ poi **Modifica**.
3. Sotto l'intestazione **archiviazione e ottimizzazione**, selezionare **Abilita crittografia**.
4. Selezionare **Salva**.

Abilitare la crittografia del volume root del nodo

A partire da ONTAP 9.8, è possibile utilizzare la crittografia dei volumi NetApp per proteggere il volume root del nodo.

A proposito di questa attività

Questa procedura si applica al volume root del nodo. Non si applica ai volumi root SVM. I volumi root delle SVM possono essere protetti tramite crittografia a livello di aggregato e A partire da ONTAP 9.14.1, NVE.

Una volta avviata, la crittografia del volume root deve essere completata. Non è possibile sospendere l'operazione. Una volta completata la crittografia, non è possibile assegnare una nuova chiave al volume root e non è possibile eseguire un'operazione di eliminazione sicura.

Prima di iniziare

- Il sistema deve utilizzare una configurazione ha.
- Il volume root del nodo deve essere già creato.
- Il sistema deve disporre di un gestore delle chiavi integrato o di un server di gestione delle chiavi esterno che utilizzi il protocollo KMIP (Key Management Interoperability Protocol).

Fasi

1. Crittografare il volume root:

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

2. Verificare lo stato dell'operazione di conversione:

   `volume encryption conversion show`

3. Una volta completata l'operazione di conversione, verificare che il volume sia crittografato:

   `volume show -fields`

   Di seguito viene riportato un esempio di output per un volume crittografato.

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