Configurare la gestione esterna delle chiavi

ONTAP 9

NetApp
February 12, 2026

Sommario

Configurare la gestione esterna delle chiavi

Scopri come configurare la gestione delle chiavi esterne ONTAP

È possibile utilizzare uno o più server di gestione delle chiavi esterni per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. Un server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

È possibile implementare la crittografia dei volumi NetApp (NVE) con il gestore delle chiavi integrato. In ONTAP 9.3 e versioni successive, NVE può essere implementato con gestione delle chiavi esterna (KMIP) e Gestione delle chiavi integrata. A partire da ONTAP 9.11.1, è possibile configurare più manager delle chiavi esterne in un cluster. Vedere Configurare i server delle chiavi in cluster.

Installare i certificati SSL sul cluster ONTAP

Il cluster e il server KMIP utilizzano i certificati SSL KMIP per verificare l'identità reciproca e stabilire una connessione SSL. Prima di configurare la connessione SSL con il server KMIP, è necessario installare i certificati SSL del client KMIP per il cluster e il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.

A proposito di questa attività

In una coppia ha, entrambi i nodi devono utilizzare gli stessi certificati SSL KMIP pubblici e privati. Se si collegano più coppie ha allo stesso server KMIP, tutti i nodi delle coppie ha devono utilizzare gli stessi certificati SSL KMIP pubblici e privati.

Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.
- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.

> È possibile installare i certificati client e server sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

Fasi

1. Installare i certificati del client KMIP SSL per il cluster:

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

   Viene richiesto di immettere i certificati SSL KMIP pubblici e privati.

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

2. Installare il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP:

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

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

Informazioni correlate

- "installazione del certificato di sicurezza"

Abilita la gestione delle chiavi esterne per la crittografia basata su hardware in ONTAP 9.6 e versioni successive

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

A partire da ONTAP 9.11.1, è possibile aggiungere fino a 3 server chiavi secondari per server chiavi primario per creare un server chiavi in cluster. Per ulteriori informazioni, vedere Configurare i server di chiavi esterne in cluster.

Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- In un ambiente MetroCluster :
  - È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
  - È necessario installare lo stesso certificato SSL KMIP su entrambi i cluster.

Fasi

1. Configurare la connettività del gestore delle chiavi per il 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
```

  - Il `security key-manager external enable` comando sostituisce il `security key-manager setup` comando. È possibile eseguire `security key-manager external modify` il comando per modificare la configurazione della gestione esterna delle chiavi. Ulteriori informazioni su `security key-manager external enable` nella "Riferimento al comando ONTAP".
  - In un ambiente MetroCluster, se si sta configurando la gestione esterna delle chiavi per la SVM amministrativa, è necessario ripetere `security key-manager external enable` sul cluster partner.

Il seguente comando abilita la gestione esterna delle chiavi per `cluster1` con tre key server esterni. Il primo server chiavi viene specificato utilizzando il nome host e la porta, il secondo viene specificato utilizzando un indirizzo IP e la porta predefinita, mentre il terzo viene specificato utilizzando un indirizzo

IPv6 e una porta:

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

2. Verificare che tutti i server KMIP configurati siano connessi:

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

> Il `security key-manager external show-status` comando sostituisce il `security key-manager show -status` comando. Ulteriori informazioni su `security key-manager external show-status` nella "Riferimento al comando ONTAP".

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

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

6 entries were displayed.
```

Informazioni correlate

- Configurare i server di chiavi esterne in cluster
- "gestore-chiavi-di-sicurezza-abilita-esterno"
- "gestore-chiavi-di-sicurezza-esterno-mostra-stato"

Abilita la gestione delle chiavi esterne per la crittografia basata su hardware in ONTAP 9.5 e versioni precedenti

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster

per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

A proposito di questa attività

ONTAP configura la connettività del server KMIP per tutti i nodi del cluster.

Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare lo stesso certificato SSL KMIP su entrambi i cluster.

Fasi

1. Configurare la connettività del gestore delle chiavi per i nodi del cluster:

   `security key-manager setup`

   Viene avviata la configurazione di Key Manager.

   In un ambiente MetroCluster , è necessario eseguire questo comando su entrambi i cluster. Scopri di più su `security key-manager setup` nel"Riferimento al comando ONTAP" .

2. Immettere la risposta appropriata a ogni richiesta.
3. Aggiunta di un server KMIP:

   `security key-manager add -address key_management_server_ipaddress`

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

   In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

   `security key-manager add -address key_management_server_ipaddress`

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

   In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

5. Verificare che tutti i server KMIP configurati siano connessi:

   `security key-manager show -status`

   Per saperne di più sui comandi descritti in questa procedura, consultare"Riferimento al 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. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

   `volume encryption conversion start`

   Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

Configurare i server delle chiavi esterne in cluster in ONTAP

A partire da ONTAP 9.11.1, è possibile configurare la connettività ai server di gestione delle chiavi esterne in cluster su una SVM. Con i server chiave in cluster, è possibile designare server chiave primari e secondari su una SVM. Durante la registrazione o il recupero delle chiavi, ONTAP tenta innanzitutto di accedere al server delle chiavi primarie, prima di tentare in sequenza di accedere ai server secondari, finché l'operazione non viene completata correttamente.

È possibile utilizzare server di chiavi esterni per le chiavi NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) e NetApp Aggregate Encryption (NAE). Una SVM può supportare fino a quattro server KMIP esterni primari. Ogni server primario può supportare fino a tre server chiave secondari.

A proposito di questa attività

- Questo processo supporta solo i server chiave che utilizzano KMIP. Per un elenco dei server delle chiavi supportati, consultare "Tool di matrice di interoperabilità NetApp".

Prima di iniziare

- "La gestione delle chiavi di KMIP deve essere abilitata per la SVM".
- Tutti i nodi del cluster devono eseguire ONTAP 9.11.1 o versione successiva.
- L'ordine dei server elencati nel `-secondary-key-servers` Il parametro riflette l'ordine di accesso dei server di gestione delle chiavi esterne (KMIP).

Creare un server di chiavi in cluster

La procedura di configurazione dipende dal fatto che sia stato configurato o meno un server di chiavi primario.

Aggiunta di server di chiavi primari e secondari a una SVM

Fasi

1. Verificare che non sia stata abilitata alcuna gestione delle chiavi per il cluster (SVM di amministrazione):

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

   Se l'SVM ha già abilitato il massimo di quattro server chiave primaria, è necessario rimuovere uno dei server chiave primaria esistenti prima di aggiungerne uno nuovo.

2. Abilita il gestore delle chiavi primarie:

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - Se non si specifica una porta nel `-key-servers` parametro, viene utilizzata la porta predefinita 5696.

   > Se stai eseguendo il `security key-manager external enable` comando per l'SVM di amministrazione in una configurazione MetroCluster , è necessario eseguire il comando su entrambi i cluster. Se si esegue il comando per una singola SVM di dati, non è necessario eseguirlo su entrambi i cluster. NetApp consiglia vivamente di utilizzare gli stessi server chiave su entrambi i cluster.

3. Modificare il server delle chiavi primarie per aggiungere server delle chiavi secondarie. IL `-secondary-key-servers` il parametro accetta un elenco separato da virgole di un massimo di tre server chiave:

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - Non includere un numero di porta per i server chiave secondari nel `-secondary-key-servers` parametro. Utilizza lo stesso numero di porta del server della chiave primaria.

   > Se stai eseguendo il `security key-manager external` comando per l'SVM di amministrazione in una configurazione MetroCluster , è necessario eseguire il comando su entrambi i cluster. Se si esegue il comando per una singola SVM di dati, non è necessario eseguirlo su entrambi i cluster. NetApp consiglia vivamente di utilizzare gli stessi server chiave su entrambi i cluster.

Aggiungere i server di chiavi secondari a un server di chiavi primario esistente

Fasi

1. Modificare il server delle chiavi primarie per aggiungere server delle chiavi secondarie. IL `-secondary-key-servers` il parametro accetta un elenco separato da virgole di un massimo di tre server chiave:

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

- Non includere un numero di porta per i server chiave secondari nel `-secondary-key-servers` parametro. Utilizza lo stesso numero di porta dei server delle chiavi primarie.

> Se stai eseguendo il `security key-manager external modify-server` comando per l'SVM di amministrazione in una configurazione MetroCluster , è necessario eseguire il comando su entrambi i cluster. Se si esegue il comando per una singola SVM di dati, non è necessario eseguirlo su entrambi i cluster. NetApp consiglia vivamente di utilizzare gli stessi server chiave su entrambi i cluster.

Per ulteriori informazioni sui server di chiavi secondarie, vedere [mod-secondary].

Modificare i server delle chiavi in cluster

È possibile modificare i server di chiavi esterni in cluster aggiungendo e rimuovendo server di chiavi secondari, modificando l'ordine di accesso dei server di chiavi secondari o modificando la designazione (primaria o secondaria) di determinati server di chiavi. Se si modificano i server chiave esterni in cluster in una configurazione MetroCluster , NetApp consiglia vivamente di utilizzare gli stessi server chiave su entrambi i cluster.

Modificare i server chiavi secondari

Utilizzare il parametro `-secondary-key-servers` del comando `security key-manager external modify-server` per gestire i server a chiave secondaria. IL `-secondary-key-servers` il parametro accetta un elenco separato da virgole. L'ordine specificato dei server delle chiavi secondarie nell'elenco determina la sequenza di accesso per i server delle chiavi secondarie. È possibile modificare l'ordine di accesso eseguendo il comando `security key-manager external modify-server` con i server di chiavi secondari inseriti in una sequenza diversa. Non includere un numero di porta per i server chiave secondari.

> Se stai eseguendo il `security key-manager external modify-server` comando per l'SVM di amministrazione in una configurazione MetroCluster , è necessario eseguire il comando su entrambi i cluster. Se si esegue il comando per una singola SVM di dati, non è necessario eseguirlo su entrambi i cluster.

Per rimuovere un server di chiavi secondario, includi i server di chiavi che desideri mantenere nel `-secondary-key-servers` parametro e ometti quello che vuoi rimuovere. Per rimuovere tutti i server di chiavi secondarie, utilizzare l'argomento `-` , che significa nessuno.

Convertire i server chiavi primari e secondari

È possibile utilizzare i seguenti passaggi per modificare la designazione (primaria o secondaria) di specifici server chiave.

Convertire un server di chiavi primarie in un server di chiavi secondarie

Fasi

1. Rimuovere il server della chiave primaria dall'SVM:

   ```
   security key-manager external remove-servers
   ```

   > Se stai eseguendo il `security key-manager external remove-servers` comando per l'SVM di amministrazione in una configurazione MetroCluster , è necessario eseguire il comando su entrambi i cluster. Se si esegue il comando per una singola SVM di dati, non è necessario eseguirlo su entrambi i cluster.

2. Eseguire ilCreare un server di chiavi in cluster procedura che utilizza il precedente server di chiavi primarie come server di chiavi secondarie.

Convertire un server di chiavi secondario in un server di chiavi primario

Fasi

1. Rimuovere il server delle chiavi secondario dal suo server delle chiavi primario esistente:

   ```
   security key-manager external modify-server -secondary-key-servers
   ```

- Se stai eseguendo il `security key-manager external modify-server -secondary-key -servers` comando per l'SVM di amministrazione in una configurazione MetroCluster , è necessario eseguire il comando su entrambi i cluster. Se si esegue il comando per una singola SVM di dati, non è necessario eseguirlo su entrambi i cluster.
- Se si converte un server di chiavi secondario in un server di chiavi primario rimuovendo un server di chiavi esistente, il tentativo di aggiungere un nuovo server di chiavi prima di completare la rimozione e la conversione può causare la duplicazione delle chiavi.

1. Eseguire ilCreare un server di chiavi in cluster procedura che utilizza il precedente server di chiavi secondario come server di chiavi primario del nuovo server di chiavi in cluster.

Fare riferimento a[mod-secondary] per maggiori informazioni.

Informazioni correlate

- Scopri di più su `security key-manager external` nel"Riferimento al comando ONTAP"

Creare chiavi di autenticazione in ONTAP 9.6 e versioni successive

È possibile utilizzare `security key-manager key create` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando Onboard Key Manager è attivato. Tuttavia, quando Onboard Key Manager è attivato, vengono create automaticamente due chiavi di autenticazione. I tasti possono essere visualizzati con il seguente comando:

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

- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.
- È possibile utilizzare il `security key-manager key delete` comando per eliminare le chiavi non utilizzate. Il `security key-manager key delete` comando fallisce se la chiave specificata è attualmente in uso da ONTAP. (Per utilizzare questo comando è necessario avere Privileges maggiore di `admin`).

> In un ambiente MetroCluster, prima di eliminare una chiave, è necessario assicurarsi che la chiave non sia in uso nel cluster partner. È possibile utilizzare i seguenti comandi sul cluster partner per verificare che la chiave non sia in uso:
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

Prima di iniziare

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

Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

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

> L'impostazione `prompt-for-key=true` fa sì che il sistema richieda all'amministratore del cluster di utilizzare la passphrase durante l'autenticazione dei dischi crittografati. In caso contrario, il sistema genera automaticamente una passphrase da 32 byte. Il `security key-manager key create` comando sostituisce il `security key-manager create-key` comando. Ulteriori informazioni su `security key-manager key create` nella "Riferimento al comando ONTAP".

Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`, che genera automaticamente una passphrase da 32 byte:

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. Verificare che le chiavi di autenticazione siano state create:

```
security key-manager key query -node node
```

> Il `security key-manager key query` comando sostituisce il `security key-manager query key` comando.
>
> L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

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

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

Ulteriori informazioni su `security key-manager key query` nella "Riferimento al comando ONTAP".

Informazioni correlate

- "mostra disco di crittografia di archiviazione"

Creare chiavi di autenticazione in ONTAP 9.5 e versioni precedenti

È possibile utilizzare `security key-manager create-key` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.
- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.

  È possibile utilizzare il software del server di gestione delle chiavi per eliminare le chiavi inutilizzate, quindi eseguire nuovamente il comando.

Prima di iniziare

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

Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

   `security key-manager create-key`

   Ulteriori informazioni su `security key-manager create-key` nella "Riferimento al comando ONTAP".

   > L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

   Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`:

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

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: <id_value>

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

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

2. Verificare che le chiavi di autenticazione siano state create:

`security key-manager query`

Ulteriori informazioni su `security key-manager query` nella "Riferimento al comando ONTAP".

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

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

  (security key-manager query)

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

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


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

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

Assegnare una chiave di autenticazione dati a un'unità FIPS o SED con gestione delle chiavi esterne ONTAP

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per bloccare o sbloccare i dati crittografati sul disco.

A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

Questa procedura non comporta interruzioni.

Prima di iniziare

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

Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

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

   Ulteriori informazioni su `storage encryption disk modify` nella "Riferimento al comando ONTAP".

   > È possibile utilizzare `security key-manager query -key-type NSE-AK` Per visualizzare gli ID chiave.

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

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

2. Verificare che le chiavi di autenticazione siano state assegnate:

   `storage encryption disk show`

   Ulteriori informazioni su `storage encryption disk show` nella "Riferimento al comando ONTAP".

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

Informazioni correlate

- "mostra disco di crittografia di archiviazione"
- "archiviazione crittografia disco mostra-stato"