Gestire la crittografia NetApp

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestire la crittografia NetApp

Decrittografare i dati del volume

È possibile utilizzare `volume move start` comando per spostare e rimuovere la crittografia dei dati del volume.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "Delegare l'autorità per eseguire il comando di spostamento del volume".

Fasi

1. Spostare un volume crittografato esistente e annullare la crittografia dei dati sul volume:

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

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

   Il seguente comando sposta un volume esistente denominato `vol1` all'aggregato di destinazione `aggr3` e annulla la crittografia dei dati sul volume:

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

   Il sistema elimina la chiave di crittografia per il volume. I dati del volume non sono crittografati.

2. Verificare che il volume sia disattivato per la crittografia:

   `volume show -encryption`

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

   Il seguente comando indica se i volumi sono accesi `cluster1` sono crittografati:

   ```
   cluster1::> volume show -encryption

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

Spostare un volume crittografato

È possibile utilizzare `volume move start` comando per spostare un volume crittografato. Il volume spostato può risiedere sullo stesso aggregato o su un aggregato

diverso.

A proposito di questa attività

Lo spostamento non riesce se il nodo di destinazione o il volume di destinazione non supporta la crittografia del volume.

Il `-encrypt-destination` opzione per `volume move start` l'impostazione predefinita è true per i volumi crittografati. Il requisito di specificare che non si desidera che il volume di destinazione venga crittografato garantisce che i dati sul volume non vengano inavvertitamente decrittografati.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "delegare l'autorità per eseguire il comando di spostamento del volume".

Fasi

1. Spostare un volume crittografato esistente e lasciare crittografati i dati sul volume:

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

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

   Il seguente comando sposta un volume esistente denominato `vol1` all'aggregato di destinazione `aggr3` e lascia crittografati i dati sul volume:

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

2. Verificare che il volume sia abilitato per la crittografia:

   `volume show -is-encrypted true`

   Per la sintassi completa dei comandi, vedere la pagina man del 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    aggr3     online    RW  200GB    160.0GB  20%
   ```

Delegare l'autorità per eseguire il comando di spostamento del volume

È possibile utilizzare `volume move` comando per crittografare un volume esistente,

spostare un volume crittografato o annullare la crittografia di un volume. Gli amministratori del cluster possono eseguire `volume move` Oppure possono delegare l'autorità per eseguire il comando agli amministratori SVM.

A proposito di questa attività

Per impostazione predefinita, agli amministratori SVM viene assegnato il `vsadmin` ruolo, che non include l'autorità per spostare i volumi. È necessario assegnare `vsadmin-volume` Agli amministratori di SVM per consentire loro di eseguire `volume move` comando.

Fase

1. Delegare l'autorità per eseguire `volume move` comando:

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

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

   Il seguente comando concede all'amministratore SVM l'autorizzazione per eseguire `volume move` comando.

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

Modificare la chiave di crittografia per un volume con il comando di avvio della chiave di crittografia del volume

È consigliabile modificare periodicamente la chiave di crittografia di un volume. A partire da ONTAP 9.3, è possibile utilizzare `volume encryption rekey start` per modificare la chiave di crittografia.

A proposito di questa attività

Una volta avviata un'operazione di rekey, questa deve essere completata. Non è possibile tornare alla vecchia chiave. Se si verificano problemi di prestazioni durante l'operazione, è possibile eseguire `volume encryption rekey pause` per sospendere l'operazione e il `volume encryption rekey resume` per riprendere l'operazione.

Fino al termine dell'operazione di rekey, il volume avrà due tasti. Le nuove scritture e le corrispondenti letture utilizzeranno la nuova chiave. In caso contrario, Read utilizzerà la vecchia chiave.

> Non è possibile utilizzare `volume encryption rekey start` Per modificare la chiave di un volume SnapLock.

Fasi

1. Modifica di una chiave di crittografia:

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

Il seguente comando modifica la chiave di crittografia per `vol1` Su SVM`vs1`:

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

2. Verificare lo stato dell'operazione di rekey:

   `volume encryption rekey show`

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

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

```
cluster1::> volume encryption rekey show

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

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

   `volume show -is-encrypted true`

   Per la sintassi completa dei comandi, vedere la pagina man del 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%
```

Modificare la chiave di crittografia per un volume con il comando di avvio spostamento volume

È consigliabile modificare periodicamente la chiave di crittografia di un volume. È possibile utilizzare `volume move start` per modificare la chiave di crittografia. È necessario utilizzare `volume move start` In ONTAP 9.2 e versioni precedenti. Il volume spostato può risiedere sullo stesso aggregato o su un aggregato diverso.

A proposito di questa attività

Non è possibile utilizzare `volume move start` Per modificare la chiave di un volume SnapLock o FlexGroup.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "delegare l'autorità per eseguire il comando di spostamento del volume".

Fasi

1. Spostare un volume esistente e modificare la chiave di crittografia:

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

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

   Il seguente comando sposta un volume esistente denominato **`vol1`** all'aggregato di destinazione **`aggr2`** e modifica la chiave di crittografia:

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

   Viene creata una nuova chiave di crittografia per il volume. I dati sul volume rimangono crittografati.

2. Verificare che il volume sia abilitato per la crittografia:

   `volume show -is-encrypted true`

   Per la sintassi completa dei comandi, vedere la pagina man del 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%
   ```

Ruotare le chiavi di autenticazione per NetApp Storage Encryption

È possibile ruotare le chiavi di autenticazione quando si utilizza NetApp Storage Encryption (NSE).

A proposito di questa attività

La rotazione delle chiavi di autenticazione in un ambiente NSE è supportata se si utilizza External Key Manager (KMIP).

> La rotazione delle chiavi di autenticazione in un ambiente NSE non è supportata da Onboard Key Manager (OKM).

Fasi

1. Utilizzare `security key-manager create-key` per generare nuove chiavi di autenticazione.

   Prima di poter modificare le chiavi di autenticazione, è necessario generare nuove chiavi di autenticazione.

2. Utilizzare `storage encryption disk modify -disk * -data-key-id` per modificare le chiavi di autenticazione.

Eliminare un volume crittografato

È possibile utilizzare `volume delete` comando per eliminare un volume crittografato.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "delegare l'autorità per eseguire il comando di spostamento del volume".
- Il volume deve essere offline.

Fase

1. Eliminazione di un volume crittografato:

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

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

   Il seguente comando elimina un volume crittografato denominato `vol1`:

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

   Invio `yes` quando viene richiesto di confermare l'eliminazione.

   Il sistema elimina la chiave di crittografia per il volume dopo 24 ore.

   Utilizzare `volume delete` con `-force true` opzione per eliminare un volume e distruggere immediatamente la chiave di crittografia corrispondente. Questo comando richiede privilegi avanzati. Per ulteriori informazioni, consulta la pagina man.

Al termine

È possibile utilizzare `volume recovery-queue` comando per ripristinare un volume cancellato durante il periodo di conservazione dopo l'emissione di `volume delete` comando:

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

"Come utilizzare la funzione Volume Recovery (Ripristino volume)"

Eliminare in modo sicuro i dati su un volume crittografato

Elimina in modo sicuro i dati su una panoramica dei volumi crittografati

A partire da ONTAP 9.4, è possibile utilizzare l'eliminazione sicura per eseguire lo scrubbing dei dati senza interruzioni su volumi abilitati per NVE. Lo scrubbing dei dati su un volume crittografato garantisce che non sia possibile ripristinarli dal supporto fisico, ad esempio in caso di "ssaccheggio", in cui le tracce dei dati potrebbero essere state lasciate indietro quando i blocchi sono stati sovrascritti o per eliminare in modo sicuro i dati di un tenant vuoto.

L'eliminazione sicura funziona solo per i file precedentemente cancellati sui volumi abilitati per NVE. Non è possibile eseguire lo scrubbing di un volume non crittografato. È necessario utilizzare i server KMIP per fornire le chiavi, non il gestore delle chiavi integrato.

Considerazioni per l'utilizzo della rimozione sicura

- I volumi creati in un aggregato abilitato per NetApp aggregate Encryption (NAE) non supportano l'eliminazione sicura.
- L'eliminazione sicura funziona solo per i file precedentemente cancellati sui volumi abilitati per NVE.
- Non è possibile eseguire lo scrubbing di un volume non crittografato.
- È necessario utilizzare i server KMIP per fornire le chiavi, non il gestore delle chiavi integrato.

L'eliminazione sicura funziona in modo diverso a seconda della versione di ONTAP in uso.

ONTAP 9.8 e versioni successive

- L'eliminazione sicura è supportata da MetroCluster e FlexGroup.
- Se il volume da rimuovere è l'origine di una relazione SnapMirror, non è necessario interrompere la relazione SnapMirror per eseguire un'eliminazione sicura.
- Il metodo di ricEncryption è diverso per i volumi che utilizzano la protezione dei dati SnapMirror rispetto ai volumi che non utilizzano la protezione dei dati SnapMirror o quelli che utilizzano la protezione estesa dei dati SnapMirror.
  - Per impostazione predefinita, i volumi che utilizzano la modalità di protezione dati SnapMirror (DP) crittografano nuovamente i dati utilizzando il metodo di ricifratura dello spostamento del volume.
  - Per impostazione predefinita, i volumi che non utilizzano la protezione dei dati SnapMirror o i volumi che utilizzano la modalità XDP (Extended Data Protection) di SnapMirror utilizzano il metodo di riscrittazione in-place.
  - È possibile modificare queste impostazioni predefinite utilizzando `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- Per impostazione predefinita, tutte le copie Snapshot nei volumi FlexVol vengono eliminate automaticamente durante l'operazione di eliminazione sicura. Per impostazione predefinita, le istantanee nei volumi e nei volumi FlexGroup che utilizzano la protezione dei dati SnapMirror non vengono eliminate automaticamente durante l'operazione di eliminazione sicura. È possibile modificare queste impostazioni predefinite utilizzando `secure purge delete-all-snapshots [true|false]` comando.

ONTAP 9.7 e versioni precedenti:

- L'eliminazione sicura non supporta quanto segue:
  - FlexClone
  - SnapVault
  - FabricPool
- Se il volume da rimuovere è l'origine di una relazione SnapMirror, è necessario interrompere la relazione SnapMirror prima di poter eliminare il volume.

  Se nel volume sono presenti copie Snapshot occupate, è necessario rilasciare le copie Snapshot prima di poter eliminare il volume. Ad esempio, potrebbe essere necessario separare un volume FlexClone dal volume padre.

- Il corretto richiamo della funzione di eliminazione sicura attiva uno spostamento del volume che crittografa nuovamente i dati rimanenti non eliminati con una nuova chiave.

  Il volume spostato rimane nell'aggregato corrente. La vecchia chiave viene automaticamente distrutta, garantendo che i dati rimossi non possano essere ripristinati dal supporto di storage.

Eliminazione sicura dei dati su un volume crittografato senza una relazione SnapMirror

A partire da ONTAP 9.4, è possibile utilizzare la funzione Secure-purge per i dati "scrub" senza interruzioni su volumi abilitati per NVE.

A proposito di questa attività

Il completamento dell'eliminazione sicura può richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell'operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l'operazione.

> Per eseguire un'eliminazione sicura su un host SAN, è necessario eliminare l'intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un'eliminazione sicura.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
   - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
   - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.
2. Sul sistema storage, passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

3. Se i file che si desidera eliminare in modo sicuro si trovano in snapshot, eliminare le snapshot:

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

4. Eliminare in modo sicuro i file cancellati:

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

   Il seguente comando elimina in modo sicuro i file cancellati su `vol1` Su SVM`vs1`:

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

5. Verificare lo stato dell'operazione di eliminazione sicura:

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

Eliminare in modo sicuro i dati su un volume crittografato con una relazione asincrona SnapMirror

A partire da ONTAP 9.8, è possibile utilizzare un purge sicuro per i dati "scrub" senza interruzioni su volumi abilitati per NVE con una relazione asincrona SnapMirror.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

A proposito di questa attività

Il completamento dell'eliminazione sicura può richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell'operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l'operazione.

> Per eseguire un'eliminazione sicura su un host SAN, è necessario eliminare l'intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un'eliminazione sicura.

Fasi

1. Nel sistema di archiviazione, passare al livello di privilegi avanzato:

   ```
   set -privilege advanced
   ```

2. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
   - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
   - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.
3. Preparare il volume di destinazione nella relazione asincrona per la rimozione sicura:

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

   Ripetere questo passaggio su ciascun volume nella relazione di SnapMirror asincrona.

4. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot, eliminare le copie Snapshot:

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

5. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot di base, procedere come segue:

   a. Creare una copia Snapshot sul volume di destinazione nella relazione SnapMirror asincrona:

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

   b. Aggiornare SnapMirror per spostare in avanti la copia Snapshot di base:

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

   Ripetere questo passaggio per ogni volume nella relazione di SnapMirror asincrona.

a. Ripetere i passaggi (a) e (b) pari al numero di copie Snapshot di base più una.

   Ad esempio, se si dispone di due copie Snapshot di base, ripetere i passaggi (a) e (b) tre volte.

b. Verificare che la copia Snapshot di base sia presente:
   `snapshot show -vserver SVM_name -volume volume_name`

c. Eliminare la copia Snapshot di base:
   `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Eliminare in modo sicuro i file cancellati:

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

   Ripetere questo passaggio su ciascun volume nella relazione di SnapMirror asincrona.

   Il seguente comando elimina in modo sicuro i file cancellati su “vol1” su SVM “vs1”:

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

7. Verificare lo stato dell’operazione di eliminazione sicura:

   `volume encryption secure-purge show`

Eseguire lo scrubbing dei dati su un volume crittografato con una relazione SnapMirror sincrona

A partire da ONTAP 9,8, puoi utilizzare una pulizia sicura per "scrub" senza interruzioni dei dati su volumi abilitati per NVE con una relazione di SnapMirror sincrono.

A proposito di questa attività

Il completamento di una rimozione sicura potrebbe richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell’operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l’operazione.

> Per eseguire un’eliminazione sicura su un host SAN, è necessario eliminare l’intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un’eliminazione sicura.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Sul sistema storage, passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
   - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
   - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.
3. Preparare il volume di destinazione nella relazione asincrona per la rimozione sicura:

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

   Ripetere questo passaggio per l'altro volume nella relazione di Synchronous SnapMirror.

4. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot, eliminare le copie Snapshot:

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

5. Se il file di eliminazione sicuro si trova nelle copie Snapshot di base o comuni, aggiornare SnapMirror per spostare la copia Snapshot comune in avanti:

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

   Esistono due copie Snapshot comuni, quindi questo comando deve essere emesso due volte.

6. Se il file di eliminazione sicuro si trova nella copia Snapshot coerente con l'applicazione, eliminare la copia Snapshot su entrambi i volumi nella relazione SnapMirror sincrona:

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

   Eseguire questa operazione su entrambi i volumi.

7. Eliminare in modo sicuro i file cancellati:

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

   Ripetere questo passaggio su ciascun volume nella relazione SnapMirror sincrona.

   Il seguente comando elimina in modo sicuro i file cancellati su "vol1" su SMV "vs1".

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

8. Verificare lo stato dell'operazione di eliminazione sicura:

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

Modificare la passphrase di gestione della chiave integrata

È consigliabile modificare periodicamente la passphrase di gestione delle chiavi integrate. Copiare la nuova passphrase di gestione della chiave integrata in una posizione sicura all'esterno del sistema di storage per un utilizzo futuro.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Modificare la passphrase di gestione della chiave integrata:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager onboard update-passphrase`
ONTAP 9.5 e versioni precedenti	`security key-manager update-passphrase`

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

   Il seguente comando ONTAP 9.6 consente di modificare la passphrase di gestione delle chiavi integrata per `cluster1`:

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

3. Invio `y` quando viene richiesto di modificare la passphrase di gestione della chiave integrata.
4. Inserire la passphrase corrente al prompt della passphrase corrente.
5. Al prompt della nuova passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per "cc-mode", una passphrase compresa tra 64 e 256 caratteri.

   Se la passphrase "cc-mode" specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l'operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

6. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.

Al termine

In un ambiente MetroCluster, è necessario aggiornare la passphrase sul cluster partner:

- In ONTAP 9.5 e versioni precedenti, è necessario eseguire `security key-manager update-passphrase` con la stessa passphrase sul cluster partner.
- In ONTAP 9.6 e versioni successive, viene richiesto di eseguire `security key-manager onboard sync` con la stessa passphrase sul cluster partner.

Copiare la passphrase di gestione della chiave integrata in una posizione sicura all'esterno del sistema di storage per un utilizzo futuro.

È necessario eseguire il backup manuale delle informazioni di gestione delle chiavi ogni volta che si modifica la passphrase di gestione delle chiavi integrata.

"Backup manuale delle informazioni di gestione delle chiavi integrate"

Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario copiare le informazioni di gestione delle chiavi integrate in una posizione sicura all'esterno del sistema di storage.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

A proposito di questa attività

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster. È inoltre necessario eseguire il backup manuale delle informazioni di gestione delle chiavi per utilizzarle in caso di disastro.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Visualizzare le informazioni di backup della gestione delle chiavi per il cluster:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager onboard show-backup`
ONTAP 9.5 e versioni precedenti	`security key-manager backup show`

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

+ il seguente comando 9.6 visualizza le informazioni di backup per la gestione delle chiavi per `cluster1`:

+

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

    --------------------------BEGIN BACKUP--------------------------
    TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
    QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
    dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAA
    3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAA
    IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
    QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
    BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
    AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
    AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAA
    KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
    AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
    LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAAA
    1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAkA
    ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
    AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAA
    gAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
    rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    ---------------------------END BACKUP---------------------------
```

1. Copiare le informazioni di backup in una posizione sicura all’esterno del sistema di storage per utilizzarle in caso di disastro.

Ripristinare le chiavi di crittografia integrate per la gestione delle chiavi

La procedura che segui per ripristinare le chiavi di crittografia della gestione delle chiavi integrate varia in base alla tua versione di ONTAP.

Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno. Per ulteriori informazioni, vedere "transizione alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

> Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

ONTAP 9,8 e versioni successive con volume root crittografato

> Se si esegue ONTAP 9,8 o versione successiva e il volume root non è crittografato, seguire la procedura per ONTAP 9,6 o versione successiva.

Se si utilizza ONTAP 9.8 e versioni successive e il volume root è crittografato, è necessario impostare una passphrase di ripristino per la gestione delle chiavi integrata nel menu di avvio. Questo processo è necessario anche se si esegue una sostituzione dei supporti di avvio.

1. Avviare il nodo dal menu di boot e selezionare l'opzione `(10) Set onboard key management recovery secrets`.
2. Invio `y` per utilizzare questa opzione.
3. Quando richiesto, inserire la passphrase di gestione della chiave integrata per il cluster.
4. Quando richiesto, inserire i dati della chiave di backup.

   Il nodo torna al menu di boot.

5. Dal menu di avvio, selezionare opzione `(1) Normal Boot`.

ONTAP 9.6 e versioni successive

1. Verificare che la chiave debba essere ripristinata:
   `security key-manager key query -node` *`node`*
2. Ripristinare la chiave:
   `security key-manager onboard sync`

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

   Il seguente comando ONTAP 9.6 sincronizza le chiavi nella gerarchia di chiavi integrate:

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

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

3. Al prompt della passphrase, inserire la passphrase di gestione della chiave integrata per il cluster.

ONTAP 9.5 e versioni precedenti

1. Verificare che la chiave debba essere ripristinata:
   `security key-manager key show`
2. Se si utilizza ONTAP 9.8 e versioni successive e il volume root è crittografato, attenersi alla seguente procedura:

   Se si utilizza ONTAP 9.6 o 9.7, o se si utilizza ONTAP 9.8 o versione successiva e il volume root non è crittografato, ignorare questo passaggio.

3. Ripristinare la chiave:
   `security key-manager setup -node node`

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

4. Al prompt della passphrase, inserire la passphrase di gestione della chiave integrata per il cluster.

Ripristinare le chiavi di crittografia esterne per la gestione delle chiavi

È possibile ripristinare manualmente le chiavi di crittografia della gestione esterna delle chiavi e inviarle a un nodo diverso. Questa operazione potrebbe essere utile se si sta riavviando un nodo temporaneamente inattivo quando sono state create le chiavi per il cluster.

A proposito di questa attività

In ONTAP 9.6 e versioni successive, è possibile utilizzare `security key-manager key query -node node_name` per verificare se la chiave deve essere ripristinata.

In ONTAP 9.5 e versioni precedenti, è possibile utilizzare `security key-manager key show` per verificare se la chiave deve essere ripristinata.

> Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

Prima di iniziare

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

Fasi

1. Se si utilizza ONTAP 9.8 o versione successiva e il volume root è crittografato, procedere come segue:

   Se si utilizza ONTAP 9.7 o versioni precedenti o se si utilizza ONTAP 9.8 o versioni successive e il volume root non è crittografato, ignorare questo passaggio.

   a. Impostare il bootargs:
      `setenv kmip.init.ipaddr <ip-address>`+ `setenv kmip.init.netmask <netmask>`+ `setenv kmip.init.gateway <gateway>`+ `setenv kmip.init.interface e0M`+ `boot_ontap`
   b. Avviare il nodo dal menu di boot e selezionare l'opzione `(11) Configure node for external key management`.

c. Seguire le istruzioni per inserire il certificato di gestione.

   Una volta inserite tutte le informazioni del certificato di gestione, il sistema torna al menu di avvio.

d. Dal menu di avvio, selezionare opzione `(1) Normal Boot`.

2. Ripristinare la chiave:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 e versioni precedenti

> `node` per impostazione predefinita, tutti i nodi. Per la sintassi completa dei comandi, vedere le pagine man. Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.

Il seguente comando ONTAP 9.6 ripristina le chiavi di autenticazione esterne per la gestione delle chiavi in tutti i nodi in `cluster1`:

```
cluster1::> security key-manager external restore
```

Sostituire i certificati SSL

Tutti i certificati SSL hanno una data di scadenza. È necessario aggiornare i certificati prima che scadano per evitare la perdita di accesso alle chiavi di autenticazione.

Prima di iniziare

- È necessario aver ottenuto il certificato pubblico e la chiave privata sostitutivi per il cluster (certificato del client KMIP).
- È necessario aver ottenuto il certificato pubblico sostitutivo per il server KMIP (certificato KMIP server-ca).
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- In un ambiente MetroCluster, è necessario sostituire il certificato SSL KMIP su entrambi i cluster.

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

Fasi

1. Installare il nuovo certificato KMIP server-ca:

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

2. Installare il nuovo certificato del client KMIP:

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

3. Aggiornare la configurazione del gestore delle chiavi per utilizzare i certificati appena installati:

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

   Se si esegue ONTAP 9.6 o versione successiva in un ambiente MetroCluster e si desidera modificare la configurazione del gestore delle chiavi nella SVM amministrativa, è necessario eseguire il comando su entrambi i cluster della configurazione.

> L'aggiornamento della configurazione del gestore delle chiavi per utilizzare i certificati appena installati restituisce un errore se le chiavi pubbliche/private del nuovo certificato client sono diverse dalle chiavi installate in precedenza. Consultare l'articolo della Knowledge base "Le chiavi pubbliche o private del nuovo certificato client sono diverse dal certificato client esistente" per istruzioni su come ignorare questo errore.

Sostituire un'unità FIPS o SED

È possibile sostituire un'unità FIPS o SED nello stesso modo in cui si sostituisce un disco normale. Assicurarsi di assegnare nuove chiavi di autenticazione dei dati all'unità sostitutiva. Per un'unità FIPS, potrebbe essere necessario assegnare una nuova chiave di autenticazione FIPS 140-2.

> Se è in uso una coppia ha "Crittografia dei dischi SAS o NVMe (SED, NSE, FIPS)", è necessario seguire le istruzioni riportate nell'argomento "Ripristino di un'unità FIPS o SED in modalità non protetta" Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

Prima di iniziare

- È necessario conoscere l'ID della chiave di autenticazione utilizzata dal disco.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Assicurarsi che il disco sia stato contrassegnato come guasto:

   ```
   storage disk show -broken
   ```

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

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

2. Rimuovere il disco guasto e sostituirlo con un nuovo disco FIPS o SED, seguendo le istruzioni nella guida hardware del modello di shelf di dischi in uso.
3. Assegnare la proprietà del disco appena sostituito:

   ```
   storage disk assign -disk disk_name -owner node
   ```

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

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

4. Verificare che il nuovo disco sia stato assegnato:

   ```
   storage encryption disk show
   ```

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Assegnare le chiavi di autenticazione dei dati all'unità FIPS o SED.

   "Assegnazione di una chiave di autenticazione dei dati a un disco FIPS o SED (gestione esterna delle chiavi)"

6. Se necessario, assegnare una chiave di autenticazione FIPS 140-2 all'unità FIPS.

   "Assegnazione di una chiave di autenticazione FIPS 140-2 a un disco FIPS"

Rendere i dati su un disco FIPS o SED inaccessibili

Rendere i dati su un disco FIPS o panoramica SED inaccessibili

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili, mantenendo lo spazio inutilizzato dell'unità disponibile per i nuovi dati, è possibile disinfettare il disco. Se si desidera rendere i dati inaccessibili in modo permanente e non è necessario riutilizzare il disco, è possibile distruggerli.

- Pulizia dei dischi

  Quando si disigienizza un'unità con crittografia automatica, il sistema modifica la chiave di crittografia del disco in un nuovo valore casuale, ripristina lo stato di blocco all'accensione su false e imposta l'ID della chiave su un valore predefinito, ovvero l'ID protetto del produttore 0x0 (unità SAS) o una chiave nulla (unità NVMe). In questo modo, i dati sul disco non sono accessibili e non possono essere recuperati. È possibile riutilizzare i dischi sanitizzati come dischi di riserva non azzerati.

- Distruggere il disco

  Quando si distrugge un disco FIPS o SED, il sistema imposta la chiave di crittografia del disco su un valore casuale sconosciuto e blocca il disco in modo irreversibile. In questo modo, il disco risulta inutilizzabile in modo permanente e i dati in esso contenuti sono inaccessibili in modo permanente.

È possibile sanificare o distruggere singole unità con crittografia automatica o tutte le unità con crittografia

automatica per un nodo.

Sanificare un disco FIPS o SED

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili e utilizzare l'unità per i nuovi dati, è possibile utilizzare `storage encryption disk sanitize` comando per la pulizia del disco.

A proposito di questa attività

Quando si disigienizza un'unità con crittografia automatica, il sistema modifica la chiave di crittografia del disco in un nuovo valore casuale, ripristina lo stato di blocco all'accensione su false e imposta l'ID della chiave su un valore predefinito, ovvero l'ID protetto del produttore 0x0 (unità SAS) o una chiave nulla (unità NVMe). In questo modo, i dati sul disco non sono accessibili e non possono essere recuperati. È possibile riutilizzare i dischi sanitizzati come dischi di riserva non azzerati.

Prima di iniziare

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

Fasi

1. Migrare tutti i dati che devono essere conservati in un aggregato su un altro disco.
2. Eliminare l'aggregato sull'unità FIPS o SED da sanificare:

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

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

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

3. Identificare l'ID del disco per l'unità FIPS o SED da sanificare:

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

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

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ----------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Se un disco FIPS è in esecuzione in modalità di conformità FIPS, impostare nuovamente l'ID della chiave

di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

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

È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

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

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

5. Igienizzare il disco:

   `storage encryption disk sanitize -disk disk_id`

   È possibile utilizzare questo comando per sanificare solo i dischi hot spare o rotti. Per sanificare tutti i dischi, indipendentemente dal tipo, utilizzare `-force-all-state` opzione. Per la sintassi completa dei comandi, vedere la pagina man.

   > ONTAP richiede di inserire una frase di conferma prima di continuare. Inserire la frase esattamente come mostrato sullo schermo.

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

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

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

Distruggere un disco FIPS o SED

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili e non è necessario riutilizzarli, è possibile utilizzare `storage encryption disk destroy` comando per distruggere il disco.

A proposito di questa attività

Quando si distrugge un disco FIPS o SED, il sistema imposta la chiave di crittografia del disco su un valore casuale sconosciuto e blocca l'unità in modo irreversibile. In questo modo, il disco risulta praticamente inutilizzabile e i dati in esso contenuti permanentemente inaccessibili. Tuttavia, è possibile ripristinare le impostazioni predefinite del disco utilizzando l'ID fisico sicuro (PSID) stampato sull'etichetta del disco. Per ulteriori informazioni, vedere "Restituzione di un disco FIPS o SED in caso di smarrimento delle chiavi di autenticazione".

Non distruggere un disco FIPS o SED a meno che non si disponga del servizio non-Returnable Disk Plus (NRD Plus). La distruzione di un disco annulla la garanzia.

Prima di iniziare

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

Fasi

1. Migrare tutti i dati che devono essere conservati in un aggregato su un altro disco diverso.
2. Eliminare l'aggregato sull'unità FIPS o SED da distruggere:

   `storage aggregate delete -aggregate aggregate_name`

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

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

3. Identificare l'ID del disco per l'unità FIPS o SED da distruggere:

   `storage encryption disk show`

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

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Distruggere il disco:

   `storage encryption disk destroy -disk disk_id`

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

   Viene richiesto di inserire una frase di conferma prima di continuare. Inserire la frase esattamente come mostrato sullo schermo.

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

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

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

Dati di emergenza ridotti su un'unità FIPS o SED

In caso di emergenza di sicurezza, è possibile impedire immediatamente l'accesso a un disco FIPS o SED, anche se il sistema storage o il server KMIP non sono in grado di fornire alimentazione.

Prima di iniziare

- Se si utilizza un server KMIP privo di alimentazione, il server KMIP deve essere configurato con un elemento di autenticazione facilmente distrutto (ad esempio, una smart card o un'unità USB).
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Eseguire la cancellazione di emergenza dei dati su un disco FIPS o SED:

Se…	Quindi…

Il sistema di storage è alimentato e hai tempo per portare il sistema di storage offline senza problemi	a. Se il sistema storage è configurato come coppia ha, disattivare il Takeover. b. Portare tutti gli aggregati offline ed eliminarli. c. Impostare il livello di privilegio su Advanced: `set -privilege advanced` d. Se il disco è in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID predefinito: `storage encryption disk modify -disk * -fips-key-id 0x0` e. Arrestare il sistema storage. f. Avviare in modalità di manutenzione. g. Sanificare o distruggere i dischi: ◦ Se si desidera rendere i dati sui dischi inaccessibili e continuare a riutilizzare i dischi, disinfettare i dischi: `disk encrypt sanitize -all` ◦ Se si desidera rendere i dati sui dischi inaccessibili e non è necessario salvarli, distruggere i dischi: `disk encrypt destroy disk_id1 disk_id2 …`	Il sistema storage è alimentato e i dati devono essere immediatamente sottratti

a. **Se si desidera rendere i dati sui dischi inaccessibili e continuare a riutilizzare i dischi, eseguire la pulizia dei dischi:**
b. Se il sistema storage è configurato come coppia ha, disattivare il Takeover.
c. Impostare il livello di privilegio su Advanced (avanzato):
`set -privilege advanced`
d. Se il disco è in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID predefinito:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Igienizzare il disco:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Se si desidera rendere i dati sui dischi inaccessibili e non è necessario salvarli, distruggere i dischi:**
	b. Se il sistema storage è configurato come coppia ha, disattivare il Takeover.
	c. Impostare il livello di privilegio su Advanced (avanzato):
	`set -privilege advanced`
	d. Distruggere i dischi: `storage encryption disk destroy -disk * -force -all-states true`
		Il sistema di storage esegue una panoramica, lasciando il sistema in uno stato di disattivazione permanente con tutti i dati cancellati. Per utilizzare di nuovo il sistema, è necessario riconfigurarlo.

L'alimentazione è disponibile per il server KMIP ma non per il sistema storage	a. Accedere al server KMIP. b. Distruggere tutte le chiavi associate ai dischi FIPS o ai SED che contengono i dati a cui si desidera impedire l'accesso. In questo modo si impedisce l'accesso alle chiavi di crittografia del disco da parte del sistema di storage.	L'alimentazione del server KMIP o del sistema storage non è disponibile

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

Restituire un'unità FIPS o SED al servizio quando le chiavi di autenticazione vengono perse

Il sistema considera un'unità FIPS o SED guasta se si perdono le chiavi di autenticazione

in modo permanente e non è possibile recuperarle dal server KMIP. Sebbene non sia possibile accedere o ripristinare i dati sul disco, è possibile adottare le misure necessarie per rendere nuovamente disponibile lo spazio inutilizzato di SED per i dati.

Prima di iniziare

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

A proposito di questa attività

Utilizzare questo processo solo se si è certi che le chiavi di autenticazione dell'unità FIPS o SED vengano perse in modo permanente e che non sia possibile ripristinarle.

Se i dischi sono partizionati, prima di poter avviare questo processo è necessario che siano dispartizionati.

> Il comando per dispartizionare un disco è disponibile solo a livello di DIAG e deve essere eseguito solo sotto la supervisione del supporto NetApp. **Si consiglia vivamente di contattare il supporto NetApp prima di procedere.** è inoltre possibile consultare l'articolo della Knowledge base "Come dispartizionare un disco spare in ONTAP".

Fasi

1. Restituire un'unità FIPS o SED al servizio:

Se i SEDS sono…	Seguire questa procedura…

Non in modalità di compliance FIPS o in modalità di compliance FIPS e la chiave FIPS è disponibile	a. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced` b. Reimpostare la chiave FIPS sull'ID protetto predefinito 0x0: `storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`* c. Verificare che l'operazione sia riuscita: `storage encryption disk show-status`Se l'operazione non riesce, utilizzare la procedura PSID descritta in questo argomento. d. Sanificare il disco danneggiato: `storage encryption disk sanitize -disk` *`disk_id`*`Verificare che l'operazione sia riuscita con il comando `storage encryption disk show-status` prima di passare alla fase successiva.  e. Annullare l'esecuzione di un errore sul disco crittografato: `storage disk unfail -spare true -disk` *`disk_id`*  f. Verificare se il disco dispone di un proprietario: `storage disk show -disk` *`disk_id`*  Se il disco non dispone di un proprietario, assegnarne uno. `storage disk assign -owner node -disk` *`disk_id`*  i. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:  `system node run -node` *`node_name`*  Eseguire `disk sanitize release` comando.  g. Uscire dalla nodeshell. Annulla errore del disco: `storage disk unfail -spare true -disk` *`disk_id`*  h. Verificare che il disco sia ora uno spare e pronto per essere riutilizzato in un aggregato: `storage disk show -disk` *`disk_id`*

In modalità di compliance FIPS, la chiave FIPS non è disponibile e i SED hanno un PSID stampato sull'etichetta	a. Ottenere il PSID del disco dall'etichetta del disco. b. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced` c. Ripristinare le impostazioni predefinite del disco: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`*`Verificare che l'operazione sia riuscita con il comando `storage encryption disk show-status` prima di passare alla fase successiva. d. Se si utilizza ONTAP 9.8P5 o versione precedente, passare alla fase successiva. Se si esegue ONTAP 9.8P6 o versione successiva, annullare la procedura di pulizia del disco. `storage disk unfail -disk` *`disk_id`* e. Verificare se il disco dispone di un proprietario: `storage disk show -disk` *`disk_id`*  Se il disco non dispone di un proprietario, assegnarne uno. `storage disk assign -owner node -disk` *`disk_id`*  i. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:  `system node run -node` *`node_name`*  Eseguire `disk sanitize release` comando.  f. Uscire dalla nodeshell.. Annulla errore del disco: `storage disk unfail -spare true -disk` *`disk_id`* g. Verificare che il disco sia ora uno spare e pronto per essere riutilizzato in un aggregato: `storage disk show -disk` *`disk_id`*

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

Consente di ripristinare un'unità FIPS o SED in modalità non protetta

Un'unità FIPS o SED è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione del nodo è impostato su un valore diverso da quello predefinito. È possibile ripristinare un'unità FIPS o SED in modalità non protetta utilizzando `storage encryption disk modify` Per impostare l'ID della chiave sul valore predefinito.

Se una coppia ha utilizza dischi SAS o NVMe con crittografia (SED, NSE, FIPS), è necessario seguire questa procedura per tutti i dischi all'interno della coppia ha prima di inizializzare il sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

Prima di iniziare

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

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Se un disco FIPS è in esecuzione in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

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

   È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

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

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

   Confermare l'operazione con il comando:

   ```
   storage encryption disk show-status
   ```

   Ripetere il comando show-status fino a quando i numeri in "Disks incomincied" (dischi iniziati) e "Disks Done" (dischi eseguiti) non sono gli stessi.

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

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

3. Impostare nuovamente l'ID della chiave di autenticazione dei dati per il nodo sul valore MSID 0x0 predefinito:

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

   Il valore di `-data-key-id` Deve essere impostato su 0x0 se si sta ripristinando un'unità SAS o NVMe in modalità non protetta.

È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

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

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

Confermare l'operazione con il comando:

```
storage encryption disk show-status
```

Ripetere il comando show-status fino a quando i numeri non coincidono. L'operazione è completa quando i numeri in "dischi iniziati" e "dischi completati" sono gli stessi.

Modalità di manutenzione

A partire da ONTAP 9.7, è possibile modificare la chiave di un disco FIPS dalla modalità di manutenzione. Utilizzare la modalità di manutenzione solo se non è possibile utilizzare le istruzioni dell'interfaccia utente di ONTAP descritte nella sezione precedente.

Fasi

1. Impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Impostare nuovamente l'ID della chiave di autenticazione dei dati per il nodo sul valore MSID 0x0 predefinito:

   `disk encrypt rekey 0x0 *disklist*`

3. Verificare che la chiave di autenticazione FIPS sia stata reinserita correttamente:

   `disk encrypt show_fips`

4. Confermare che la chiave di autenticazione dei dati è stata risigitata correttamente con:

   `disk encrypt show`

   L'output visualizza probabilmente l'ID chiave MSID 0x0 predefinito o il valore di 64 caratteri posseduto dal server delle chiavi. Il `Locked?` il campo si riferisce al blocco dei dati.

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

Rimuovere una connessione di gestione delle chiavi esterna

È possibile scollegare un server KMIP da un nodo quando non è più necessario. Ad esempio, è possibile scollegare un server KMIP durante la transizione alla crittografia del volume.

A proposito di questa attività

Quando si disconnette un server KMIP da un nodo in una coppia ha, il sistema disconnette automaticamente il server da tutti i nodi del cluster.

> Se si prevede di continuare a utilizzare la gestione delle chiavi esterne dopo aver scollegato un server KMIP, assicurarsi che sia disponibile un altro server KMIP per la fornitura delle chiavi di autenticazione.

Prima di iniziare

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

Fase

1. Disconnettere un server KMIP dal nodo corrente:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 e versioni precedenti

In un ambiente MetroCluster, è necessario ripetere questi comandi su entrambi i cluster per la SVM amministrativa.

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

Il seguente comando ONTAP 9.6 disattiva le connessioni a due server di gestione delle chiavi esterni per `cluster1`, il primo nome `ks1`, In attesa sulla porta predefinita 5696, la seconda con l'indirizzo IP 10.0.0.20, in attesa sulla porta 24482:

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

Modificare le proprietà del server di gestione delle chiavi esterno

A partire da ONTAP 9.6, è possibile utilizzare `security key-manager external modify-server` Comando per modificare il timeout i/o e il nome utente di un server di gestione delle chiavi esterno.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Per questa attività sono richiesti privilegi avanzati.
- In un ambiente MetroCluster, è necessario ripetere questi passaggi su entrambi i cluster per la SVM amministrativa.

Fasi

1. Sul sistema storage, passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Modificare le proprietà del server di gestione delle chiavi esterno per il cluster:

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

   > Il valore di timeout viene espresso in secondi. Se si modifica il nome utente, viene richiesto di inserire una nuova password. Se si esegue il comando al prompt di login del cluster, *`admin_SVM`* Per impostazione predefinita, viene impostata la SVM amministrativa del cluster corrente. È necessario essere l'amministratore del cluster per modificare le proprietà del server del gestore delle chiavi esterno.

   Il seguente comando modifica il valore di timeout a 45 secondi per `cluster1` server di gestione delle chiavi esterno in attesa sulla porta predefinita 5696:

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

3. Modificare le proprietà del server di gestione delle chiavi esterne per una SVM (solo NVE):

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

   > Il valore di timeout viene espresso in secondi. Se si modifica il nome utente, viene richiesto di inserire una nuova password. Se si esegue il comando al prompt di accesso SVM, *`SVM`* Per impostazione predefinita, viene impostata la SVM corrente. Per modificare le proprietà del server del gestore delle chiavi esterno, è necessario essere l'amministratore del cluster o SVM.

   Il seguente comando consente di modificare il nome utente e la password di `svm1` server di gestione delle chiavi esterno in attesa sulla porta predefinita 5696:

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

4. Ripetere l'ultimo passaggio per eventuali SVM aggiuntive.

Transizione alla gestione esterna delle chiavi dalla gestione integrata delle chiavi

Se si desidera passare alla gestione esterna delle chiavi dalla gestione integrata delle chiavi, è necessario eliminare la configurazione di gestione integrata delle chiavi prima di attivare la gestione esterna delle chiavi.

Prima di iniziare

- Per la crittografia basata su hardware, è necessario ripristinare il valore predefinito delle chiavi dati di tutti i dischi FIPS o SED.

  "Ripristino di un'unità FIPS o SED in modalità non protetta"

- Per la crittografia basata su software, è necessario annullare la crittografia di tutti i volumi.

  "Annullamento della crittografia dei dati del volume"

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

Fase

1. Eliminare la configurazione di gestione delle chiavi integrata per un cluster:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 e versioni precedenti	`security key-manager delete-key-database`

Per la sintassi completa dei comandi, vedere "Pagine di manuale di ONTAP".

Transizione alla gestione delle chiavi integrata dalla gestione esterna delle chiavi

Se si desidera passare alla gestione delle chiavi integrata dalla gestione delle chiavi esterna, è necessario eliminare la configurazione di gestione delle chiavi esterne prima di poter attivare la gestione delle chiavi integrata.

Prima di iniziare

- Per la crittografia basata su hardware, è necessario ripristinare il valore predefinito delle chiavi dati di tutti i dischi FIPS o SED.

  "Ripristino di un'unità FIPS o SED in modalità non protetta"

- È necessario eliminare tutte le connessioni di gestione delle chiavi esterne.

  "Eliminazione di una connessione di gestione delle chiavi esterna"

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

Procedura

I passaggi necessari per eseguire la transizione della gestione delle chiavi dipendono dalla versione di ONTAP in uso.

ONTAP 9.6 e versioni successive

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Utilizzare il comando:

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

   > In un ambiente MetroCluster, è necessario ripetere il comando su entrambi i cluster per la SVM amministrativa.

ONTAP 9.5 e versioni precedenti

Utilizzare il comando:
`security key-manager delete-kmip-config`

Cosa accade quando i server di gestione delle chiavi non sono raggiungibili durante il processo di avvio

ONTAP prende alcune precauzioni per evitare comportamenti indesiderati nel caso in cui un sistema storage configurato per NSE non riesca a raggiungere nessuno dei server di gestione delle chiavi specificati durante il processo di avvio.

Se il sistema di storage è configurato per NSE, i SED vengono ridigitati e bloccati e i SED sono accesi, il sistema di storage deve recuperare le chiavi di autenticazione richieste dai server di gestione delle chiavi per autenticarsi ai SED prima di poter accedere ai dati.

Il sistema storage tenta di contattare i server di gestione delle chiavi specificati per un massimo di tre ore. Se il sistema storage non riesce a raggiungerne uno dopo tale periodo, il processo di avvio si interrompe e il sistema storage si arresta.

Se il sistema di storage contatta correttamente qualsiasi server di gestione delle chiavi specificato, tenta di stabilire una connessione SSL per un massimo di 15 minuti. Se il sistema di storage non riesce a stabilire una connessione SSL con un server di gestione delle chiavi specificato, il processo di avvio si interrompe e il sistema di storage si arresta.

Mentre il sistema di storage tenta di contattare e connettersi ai server di gestione delle chiavi, visualizza informazioni dettagliate sui tentativi di contatto non riusciti alla CLI. È possibile interrompere i tentativi di contatto in qualsiasi momento premendo Ctrl-C.

Come misura di sicurezza, i SED consentono solo un numero limitato di tentativi di accesso non autorizzati, dopodiché disattivano l’accesso ai dati esistenti. Se il sistema di storage non riesce a contattare alcun server di

gestione delle chiavi specificato per ottenere le chiavi di autenticazione appropriate, può solo tentare di autenticare con la chiave predefinita, il che causa un tentativo di errore e un panico. Se il sistema di storage è configurato per il riavvio automatico in caso di panico, entra in un loop di avvio che porta a tentativi di autenticazione non riusciti continui sui SED.

L'arresto del sistema storage in questi scenari è progettato per impedire al sistema storage di entrare in un loop di avvio e di perdere dati non intenzionale come conseguenza del blocco permanente dei SED dovuto al superamento del limite di sicurezza di un certo numero di tentativi di autenticazione consecutivi non riusciti. Il limite e il tipo di protezione di blocco dipendono dalle specifiche di produzione e dal tipo di SED:

TIPO SED	Numero di tentativi consecutivi di autenticazione non riusciti che hanno determinato il blocco	Tipo di protezione di blocco quando viene raggiunto il limite di sicurezza
DISCO RIGIDO	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.
X440_PHM2800 MCTO SSD NSE da 800 GB con revisioni del firmware NA00 o NA01	5	Temporaneo. Il blocco è valido solo fino a quando il disco non viene spento e riacceso.
X577_PHM2800 MCTO SSD NSE da 800 GB con revisioni del firmware NA00 o NA01	5	Temporaneo. Il blocco è valido solo fino a quando il disco non viene spento e riacceso.
X440_PHM2800MCTO SSD NSE da 800 GB con revisioni del firmware superiori	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.
X577_PHM2800MCTO SSD NSE da 800 GB con revisioni del firmware superiori	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.
Tutti gli altri modelli di SSD	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.

Per tutti i tipi SED, un'autenticazione corretta azzera il numero di proy.

Se si verifica questo scenario in cui il sistema storage viene arrestato a causa di un errore di accesso a uno dei server di gestione delle chiavi specificati, prima di continuare l'avvio del sistema storage è necessario identificare e correggere la causa dell'errore di comunicazione.

Disattivare la crittografia per impostazione predefinita

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita se si dispone di una licenza di crittografia del volume (VE) e si utilizza un gestore di chiavi integrato o esterno. Se necessario, è possibile disattivare la crittografia per impostazione predefinita per l'intero cluster.

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.

Fase

1. Per disattivare la crittografia per impostazione predefinita per l'intero cluster in ONTAP 9.7 o versioni successive, eseguire il seguente comando:

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