Rendere i dati su un disco FIPS o SED inaccessibili

ONTAP 9

NetApp
September 12, 2024

Sommario

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.
```

6. Annullare l'esecuzione di un errore sul disco crittografato: `storage disk unfail -spare true -disk disk_id`
7. 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`
8. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:

   `system node run -node node_name`

   Eseguire `disk sanitize release` comando.

9. Uscire dalla nodeshell. Annulla errore del disco: `storage disk unfail -spare true -disk disk_id`
10. Verificare che il disco sia ora uno spare e pronto per essere riutilizzato in un aggregato: `storage disk show -disk disk_id`

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.