Gestire la crittografia con la CLI

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestire la crittografia con la CLI

Panoramica sulla crittografia NetApp

NetApp offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

- La crittografia basata su software con NetApp Volume Encryption (NVE) supporta la crittografia dei dati di un volume alla volta
- La crittografia basata su hardware con NetApp Storage Encryption (NSE) supporta la crittografia completa dei dati su disco (FDE) durante la scrittura.

Configurare NetApp Volume Encryption

Panoramica sulla configurazione di NetApp Volume Encryption

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. Una chiave di crittografia accessibile solo al sistema di storage impedisce la lettura dei dati del volume in caso di riallocazione, restituzione, smarrimento o furto del dispositivo sottostante.

Comprensione di NVE

Con NVE, sia i metadati che i dati (incluse le copie Snapshot) vengono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume. Un server di gestione delle chiavi esterno o Onboard Key Manager (OKM) serve le chiavi ai nodi:

- Il 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). Si consiglia di configurare i server di gestione delle chiavi esterni su un sistema storage diverso dai dati.
- Onboard Key Manager è uno strumento integrato che serve le chiavi ai nodi dello stesso sistema storage dei dati.

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. La licenza VE è inclusa con "ONTAP uno". Ogni volta che viene configurato un gestore di chiavi esterno o integrato, viene modificato il modo in cui viene configurata la crittografia dei dati inattivi per aggregati nuovi di zecca e volumi nuovi di zecca. I nuovi aggregati avranno NetApp aggregate Encryption (NAE) abilitato per impostazione predefinita. I volumi nuovi di zecca che non fanno parte di un aggregato NAE avranno NetApp Volume Encryption (NVE) abilitato per impostazione predefinita. Se una macchina virtuale per lo storage dei dati (SVM) viene configurata con un proprio gestore delle chiavi utilizzando la gestione delle chiavi multi-tenant, il volume creato per tale SVM viene configurato automaticamente con NVE.

È possibile attivare la crittografia su un volume nuovo o esistente. NVE supporta la gamma completa di funzionalità per l'efficienza dello storage, tra cui deduplica e compressione. A partire da ONTAP 9.14.1, è possibile Abilitazione di NVE su volumi root SVM esistenti.

> Se si utilizza SnapLock, è possibile attivare la crittografia solo su volumi SnapLock nuovi e vuoti. Non è possibile attivare la crittografia su un volume SnapLock esistente.

È possibile utilizzare NVE su qualsiasi tipo di aggregato (HDD, SSD, ibrido, LUN array), con qualsiasi tipo di RAID e in qualsiasi implementazione ONTAP supportata, incluso ONTAP Select. È inoltre possibile utilizzare NVE con crittografia basata su hardware per "crittografare `ddoppio`" i dati su dischi con crittografia automatica.

Quando NVE è abilitato, anche il core dump è crittografato.

Crittografia a livello di aggregato

Normalmente, a ogni volume crittografato viene assegnata una chiave univoca. Quando il volume viene cancellato, la chiave viene eliminata con esso.

A partire da ONTAP 9.6, è possibile utilizzare la crittografia aggregata NetApp per assegnare le chiavi all'aggregato contenente per i volumi da crittografare. Quando si elimina un volume crittografato, le chiavi dell'aggregato vengono conservate. Le chiavi vengono eliminate se l'intero aggregato viene cancellato.

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

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.

I volumi NVE e NAE possono coesistere sullo stesso aggregato. Per impostazione predefinita, i volumi crittografati con crittografia a livello di aggregato sono volumi NAE. È possibile ignorare l'impostazione predefinita quando si crittografa il volume.

È possibile utilizzare `volume move` Per convertire un volume NVE in un volume NAE e viceversa. È possibile replicare un volume NAE in un volume NVE.

Non è possibile utilizzare `secure purge` Comandi su un volume NAE.

Quando utilizzare server di gestione delle chiavi esterni

Sebbene sia meno costoso e generalmente più conveniente utilizzare il gestore delle chiavi integrato, è necessario configurare i server KMIP se si verifica una delle seguenti condizioni:

- La soluzione di gestione delle chiavi di crittografia deve essere conforme agli standard FIPS (Federal Information Processing Standards) 140-2 o ALLO standard OASIS KMIP.
- Hai bisogno di una soluzione multi-cluster, con gestione centralizzata delle chiavi di crittografia.
- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

Scopo della gestione esterna delle chiavi

L'ambito della gestione esterna delle chiavi determina se i server di gestione delle chiavi proteggono tutte le SVM nel cluster o solo le SVM selezionate:

- È possibile utilizzare un *ambito del cluster* per configurare la gestione delle chiavi esterne per tutte le SVM nel cluster. L'amministratore del cluster ha accesso a tutte le chiavi memorizzate sui server.

- A partire da ONTAP 9.6, è possibile utilizzare un *ambito SVM* per configurare la gestione delle chiavi esterne per una SVM denominata nel cluster. Questo è il meglio per gli ambienti multi-tenant in cui ciascun tenant utilizza una SVM (o un insieme di SVM) diversa per la distribuzione dei dati. Solo l'amministratore SVM di un determinato tenant ha accesso alle chiavi del tenant.
- A partire da ONTAP 9.10.1, è possibile utilizzare Azure Key Vault e Google Cloud KMS Proteggere le chiavi NVE solo per dati SVM. Questa funzione è disponibile per i sistemi KMS di AWS a partire dal 9.12.0.

È possibile utilizzare entrambi gli ambiti nello stesso cluster. Se i server di gestione delle chiavi sono stati configurati per una SVM, ONTAP utilizza solo questi server per proteggere le chiavi. In caso contrario, ONTAP protegge le chiavi con i server di gestione delle chiavi configurati per il cluster.

Un elenco di Key Manager esterni validati è disponibile in "Tool di matrice di interoperabilità NetApp (IMT)". Per trovare questo elenco, inserire il termine "Key Manager" nella funzione di ricerca di IMT.

Dettagli del supporto

La seguente tabella mostra i dettagli del supporto NVE:

Risorsa o funzione	Dettagli del supporto
Piattaforme	Funzionalità di offload AES-NI richiesta. Consultare il Hardware Universe (HWU) per verificare che NVE e NAE siano supportati per la piattaforma in uso.

Crittografia	A partire da ONTAP 9.7, gli aggregati e i volumi appena creati vengono crittografati per impostazione predefinita quando si aggiunge una licenza VE (Volume Encryption) e si dispone di un gestore di chiavi integrato o esterno configurato. Se è necessario creare un aggregato non crittografato, utilizzare il seguente comando:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Se è necessario creare un volume di testo normale, utilizzare il seguente comando:
	
	`volume create -encrypt false`
	
	La crittografia non è attivata per impostazione predefinita quando:
	
	• La licenza VE non è installata.
	• Gestore chiavi non configurato.
	• La piattaforma o il software non supportano la crittografia.
	• La crittografia hardware è attivata.

ONTAP	Tutte le implementazioni ONTAP. Il supporto per il cloud ONTAP è disponibile in ONTAP 9.5 e versioni successive.
Dispositivi	HDD, SSD, ibrido, LUN array.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.

Volumi	Volumi di dati e volumi root della SVM esistenti. Non puoi crittografare i dati sui volumi di metadati MetroCluster. Nelle versioni di ONTAP precedenti alla 9.14.1, non è possibile crittografare i dati sul volume root della SVM con NVE. A partire da ONTAP 9.14.1, ONTAP supporta NVE su volumi root SVM.
Crittografia a livello di aggregato	A partire da ONTAP 9.6, NVE supporta la crittografia a livello aggregato (NAE): • Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato. • Non è possibile reimmettere la chiave di un volume di crittografia a livello di aggregato. • L'eliminazione sicura non è supportata sui volumi di crittografia a livello di aggregato. • Oltre ai volumi di dati, NAE supporta la crittografia dei volumi root SVM e del volume di metadati MetroCluster. NAE non supporta la crittografia del volume root.
Ambito SVM	A partire da ONTAP 9.6, NVE supporta l'ambito SVM solo per la gestione delle chiavi esterne, non per Onboard Key Manager. MetroCluster è supportato a partire da ONTAP 9.8.
Efficienza dello storage	Deduplica, compressione, compattazione, FlexClone. I cloni utilizzano la stessa chiave del padre, anche dopo aver sdoppiato il clone dal padre. Eseguire una `volume move` su un clone split, dopodiché il clone split avrà una chiave diversa.
Replica	• Per la replica dei volumi, i volumi di origine e di destinazione possono avere impostazioni di crittografia diverse. La crittografia può essere configurata per l'origine e non configurata per la destinazione e viceversa. • Per la replica SVM, il volume di destinazione viene crittografato automaticamente, a meno che la destinazione non contenga un nodo che supporti la crittografia del volume, nel qual caso la replica riesce, ma il volume di destinazione non viene crittografato. • Per le configurazioni MetroCluster, ogni cluster estrae le chiavi di gestione delle chiavi esterne dai relativi server delle chiavi configurati. Le chiavi OKM vengono replicate nel sito del partner dal servizio di replica della configurazione.
Conformità	A partire da ONTAP 9.2, SnapLock è supportato sia in modalità Compliance che Enterprise, solo per nuovi volumi. Non è possibile attivare la crittografia su un volume SnapLock esistente.
FlexGroups	A partire da ONTAP 9.2, sono supportati FlexGroups. Gli aggregati di destinazione devono essere dello stesso tipo degli aggregati di origine, a livello di volume o aggregato. A partire da ONTAP 9.5, è supportata la rekey in-place dei volumi FlexGroup.

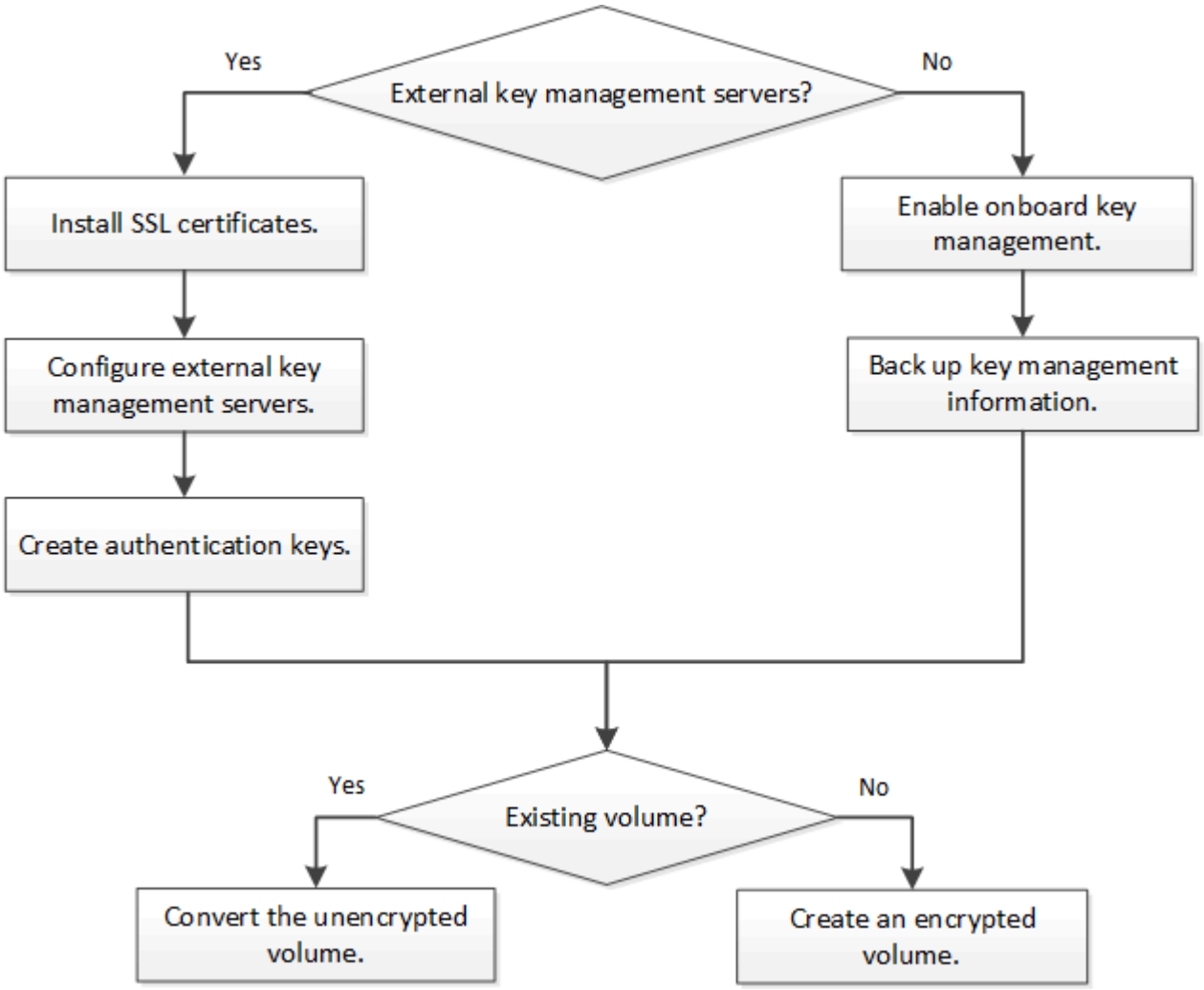
Transizione 7-Mode	A partire da 7-Mode Transition Tool 3.3, è possibile utilizzare 7-Mode Transition Tool CLI per eseguire una transizione basata su copia a volumi di destinazione abilitati per NVE sul sistema in cluster.

Informazioni correlate

"FAQ - NetApp Volume Encryption e NetApp aggregate Encryption"

Workflow di NetApp Volume Encryption

È necessario configurare i servizi di gestione delle chiavi prima di poter attivare la crittografia dei volumi. È possibile attivare la crittografia su un nuovo volume o su un volume esistente.



"È necessario installare la licenza VE" E configurare i servizi di gestione delle chiavi prima di poter criptare i dati con NVE. Prima di installare la licenza, è necessario "Determinare se la versione di ONTAP in uso supporta NVE".

Configurare NVE

Determinare se la versione del cluster supporta NVE

Prima di installare la licenza, è necessario determinare se la versione del cluster supporta NVE. È possibile utilizzare `version` per determinare la versione del cluster.

A proposito di questa attività

La versione del cluster è la versione più bassa di ONTAP in esecuzione su qualsiasi nodo del cluster.

Fase

1. Determinare se la versione del cluster supporta NVE:

   ```
   version -v
   ```

   NVE non è supportato se l'output del comando visualizza il testo "1Ono-DARE" (per "no Data at Rest Encryption") o se si utilizza una piattaforma non elencata nella "Dettagli del supporto".

   Il seguente comando determina se NVE è supportato su `cluster1`.

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   L'output di `1Ono-DARE` Indica che NVE non è supportato sulla versione del cluster.

Installare la licenza

Una licenza VE consente di utilizzare la funzione su tutti i nodi del cluster. Questa licenza è necessaria prima di poter crittografare i dati con NVE. È incluso con "ONTAP uno".

Prima di ONTAP One, la licenza VE era inclusa nel pacchetto crittografia. Il pacchetto di crittografia non è più disponibile, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo "Eseguire l'aggiornamento a ONTAP One".

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver ricevuto la chiave di licenza VE dal rappresentante di vendita o avere installato ONTAP ONE.

Fasi

1. "Verificare che la licenza VE sia installata".

   Il nome del pacchetto di licenza VE è `VE`.

2. Se la licenza non è installata, "Utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per installarlo".

Configurare la gestione esterna delle chiavi

Configurare una panoramica sulla gestione esterna delle chiavi

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).

> Per ONTAP 9.1 e versioni precedenti, è necessario assegnare le LIF di gestione dei nodi alle porte configurate con il ruolo di gestione dei nodi prima di poter utilizzare il gestore delle chiavi esterno.

NetApp Volume Encryption (NVE) supporta Onboard Key Manager in ONTAP 9.1 e versioni successive. A partire da ONTAP 9.3, NVE supporta la gestione delle chiavi esterne (KMIP) e Onboard Key Manager. A partire da ONTAP 9.10.1, è possibile utilizzare Azure Key Vault o Google Cloud Key Manager Service Per proteggere le chiavi NVE. A partire da ONTAP 9.11.1, è possibile configurare più Key Manager esterni in un cluster. Vedere Configurare i server delle chiavi in cluster.

Gestisci i manager delle chiavi esterne con System Manager

A partire da ONTAP 9.7, è possibile memorizzare e gestire le chiavi di autenticazione e crittografia con Onboard Key Manager. A partire da ONTAP 9.13.1, è possibile utilizzare anche i gestori delle chiavi esterni per memorizzare e gestire queste chiavi.

Onboard Key Manager memorizza e gestisce le chiavi in un database sicuro interno al cluster. Il suo scopo è il cluster. Un gestore delle chiavi esterno memorizza e gestisce le chiavi all'esterno del cluster. Il suo ambito può essere il cluster o la VM di storage. È possibile utilizzare uno o più gestori di chiavi esterne. Si applicano le seguenti condizioni:

- Se Onboard Key Manager è attivato, non è possibile attivare un gestore di chiavi esterno a livello di cluster, ma può essere attivato a livello di storage VM.
- Se un gestore delle chiavi esterno è abilitato a livello di cluster, il gestore delle chiavi integrato non può essere abilitato.

Quando si utilizzano key manager esterni, è possibile registrare fino a quattro key server primari per storage VM e cluster. Ogni server principale delle chiavi può essere cluster con un massimo di tre server secondari delle chiavi.

Configurare un gestore di chiavi esterno

Per aggiungere un gestore di chiavi esterno per una VM di storage, è necessario aggiungere un gateway opzionale quando si configura l'interfaccia di rete per la VM di storage. Se la VM di storage è stata creata senza il percorso di rete, sarà necessario creare il percorso in modo esplicito per il gestore delle chiavi esterno. Vedere "Creazione di una LIF (interfaccia di rete)".

Fasi

È possibile configurare un gestore di chiavi esterno partendo da posizioni diverse in System Manager.

1. Per configurare un gestore di chiavi esterno, eseguire una delle seguenti operazioni iniziali.

Workflow	Navigazione	Fase di avvio
Configurare Key Manager	**Cluster** > **Impostazioni**	Scorrere fino alla sezione **sicurezza**. In **Encryption**, selezionare ⚙. Selezionare **External Key Manager**.

Aggiungi Tier locale	**Storage** > **Tier**	Selezionare **+ Aggiungi livello locale**. Selezionare la casella di controllo "Configure Key Manager" (Configura gestore chiavi). Selezionare **External Key Manager**.
Preparare lo storage	**Dashboard**	Nella sezione **capacità**, selezionare **Prepare Storage** (prepara storage). Quindi, selezionare "Configure Key Manager" (Configura gestore chiavi). Selezionare **External Key Manager**.
Configurare la crittografia (solo gestore delle chiavi nell'ambito delle macchine virtuali di storage)	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **Encryption** sotto **Security**, selezionare ⚙.

2. Per aggiungere un server delle chiavi principale, selezionare + Add E compilare i campi **IP Address (Indirizzo IP) o host Name (Nome host)** e **Port** (porta).
3. I certificati esistenti installati sono elencati nei campi **certificati CA del server KMIP** e **certificato client KMIP**. È possibile eseguire una delle seguenti operazioni:
   - Selezionare ⌄ per selezionare i certificati installati che si desidera mappare al gestore delle chiavi. (È possibile selezionare più certificati CA di servizio, ma è possibile selezionare un solo certificato client).
   - Selezionare **Aggiungi nuovo certificato** per aggiungere un certificato non ancora installato e associarlo al gestore delle chiavi esterno.
   - Selezionare × accanto al nome del certificato per eliminare i certificati installati che non si desidera mappare al gestore delle chiavi esterno.
4. Per aggiungere un server chiavi secondario, selezionare **Aggiungi** nella colonna **Server chiavi secondari** e fornire i relativi dettagli.
5. Selezionare **Salva** per completare la configurazione.

Modificare un gestore di chiavi esterno esistente

Se è già stato configurato un gestore di chiavi esterno, è possibile modificarne le impostazioni.

Fasi

1. Per modificare la configurazione di un gestore di chiavi esterno, eseguire una delle seguenti operazioni iniziali.

Scopo	Navigazione	Fase di avvio
Gestore delle chiavi esterne dell'ambito del cluster	**Cluster** > **Impostazioni**	Scorrere fino alla sezione **sicurezza**. In **Encryption**, selezionare ⋮, Quindi selezionare **Edit External Key Manager** (Modifica gestore chiavi esterno).

Storage VM Scope External Key Manager	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **Encryption** sotto **Security**, selezionare ⋮, Quindi selezionare **Edit External Key Manager** (Modifica gestore chiavi esterno).

2. I server delle chiavi esistenti sono elencati nella tabella **Server delle chiavi**. È possibile eseguire le seguenti operazioni:
   - Aggiungere un nuovo server chiavi selezionando + Add .
   - Eliminare un server delle chiavi selezionando ⋮ alla fine della cella della tabella che contiene il nome del server delle chiavi. Anche i server di chiavi secondari associati a quel server di chiavi primario vengono rimossi dalla configurazione.

Eliminare un gestore di chiavi esterno

Se i volumi non sono crittografati, è possibile eliminare un gestore di chiavi esterno.

Fasi

1. Per eliminare un gestore di chiavi esterno, eseguire una delle seguenti operazioni.

Scopo	Navigazione	Fase di avvio
Gestore delle chiavi esterne dell'ambito del cluster	**Cluster** > **Impostazioni**	Scorrere fino alla sezione **sicurezza**. In **Encryption**, selezionare ⋮, Quindi selezionare **Delete External Key Manager** (Elimina gestore chiavi esterne).
Storage VM Scope External Key Manager	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **Encryption** sotto **Security**, selezionare ⋮, Quindi selezionare **Delete External Key Manager** (Elimina gestore chiavi esterne).

Migrare le chiavi tra i principali manager

Quando su un cluster sono attivati più gestori di chiavi, è necessario migrare le chiavi da un gestore di chiavi a un altro. Questo processo viene completato automaticamente con System Manager.

- Se Onboard Key Manager o un gestore di chiavi esterno è abilitato a livello di cluster e alcuni volumi sono crittografati, Quindi, quando si configura un gestore di chiavi esterno a livello di storage VM, le chiavi devono essere migrate da Onboard Key Manager o da un gestore di chiavi esterno a livello di cluster a un gestore di chiavi esterno a livello di storage VM. Questo processo viene completato automaticamente da System Manager.
- Se i volumi sono stati creati senza crittografia su una VM di storage, non è necessario migrare le chiavi.

Installare i certificati SSL sul cluster

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
   ```

Abilitare la gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (NVE)

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. A partire da ONTAP 9.6, è possibile configurare un gestore di chiavi esterno separato per proteggere le chiavi utilizzate da un SVM di dati per accedere ai dati crittografati.

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.

A proposito di questa attività

È possibile collegare fino a quattro server KMIP a un cluster o a una SVM. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

L'ambito della gestione esterna delle chiavi determina se i server di gestione delle chiavi proteggono tutte le SVM nel cluster o solo le SVM selezionate:

- È possibile utilizzare un *ambito del cluster* per configurare la gestione delle chiavi esterne per tutte le SVM nel cluster. L'amministratore del cluster ha accesso a tutte le chiavi memorizzate sui server.
- A partire da ONTAP 9.6, è possibile utilizzare un *ambito SVM* per configurare la gestione delle chiavi esterne per una SVM di dati nel cluster. Questo è il meglio per gli ambienti multi-tenant in cui ciascun tenant utilizza una SVM (o un insieme di SVM) diversa per la distribuzione dei dati. Solo l'amministratore SVM di un determinato tenant ha accesso alle chiavi del tenant.
- Per gli ambienti multi-tenant, installare una licenza per *MT_EK_MGMT* utilizzando il seguente comando:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

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

È possibile utilizzare entrambi gli ambiti nello stesso cluster. Se i server di gestione delle chiavi sono stati configurati per una SVM, ONTAP utilizza solo questi server per proteggere le chiavi. In caso contrario, ONTAP protegge le chiavi con i server di gestione delle chiavi configurati per il cluster.

È possibile configurare la gestione delle chiavi integrata nell'ambito del cluster e la gestione delle chiavi esterne nell'ambito SVM. È possibile utilizzare `security key-manager key migrate` Comando per la migrazione delle chiavi dalla gestione delle chiavi integrata nell'ambito del cluster ai key manager esterni nell'ambito SVM.

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 o di SVM.
- Se si desidera attivare la gestione esterna delle chiavi per un ambiente MetroCluster, MetroCluster deve essere completamente configurato prima di attivare la gestione esterna delle chiavi.
- In un ambiente MetroCluster, è necessario installare il 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` il comando sostituisce `security key-manager setup` comando. Se si esegue il comando al prompt di login del cluster, *`admin_SVM`* Per impostazione predefinita, viene impostata la SVM amministrativa del cluster corrente. Per configurare l'ambito del cluster, è necessario essere l'amministratore del cluster. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne.
   - 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:

```
clusterl::> security key-manager external enable -vserver cluster1 -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. Configurare un gestore delle chiavi e una SVM:

   `security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   - Se si esegue il comando al prompt di accesso SVM, `SVM` Per impostazione predefinita, viene impostata la SVM corrente. Per configurare l'ambito di SVM, è necessario essere un amministratore del cluster o di SVM. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne.
   - In un ambiente MetroCluster, se si configura la gestione esterna delle chiavi per una SVM di dati, non è necessario ripetere `security key-manager external enable` sul cluster partner.

   Il seguente comando abilita la gestione esterna delle chiavi per `svm1` con un server a chiave singola in ascolto sulla porta predefinita 5696:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

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

   È inoltre possibile utilizzare `security key-manager external add-servers` Comando per configurare SVM aggiuntive. Il `security key-manager external add-servers` il comando sostituisce `security key-manager add` comando. Per la sintassi completa dei comandi, vedere la pagina man.

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

   `security key-manager external show-status -node node_name`

   Il `security key-manager external show-status` il comando sostituisce `security key-manager show -status` comando. Per la sintassi completa dei comandi, vedere la pagina man.

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

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 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.

Abilitare la gestione esterna delle chiavi 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 il 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.

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 la sintassi completa dei comandi, vedere la pagina man.

```
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.

Gestire le chiavi con un cloud provider

A partire da ONTAP 9.10.1, è possibile utilizzare "Azure Key Vault (AKV)" e. "Servizio di gestione delle chiavi di Google Cloud Platform (Cloud KMS)" Per proteggere le chiavi di crittografia ONTAP in un'applicazione ospitata nel cloud. A partire da ONTAP 9.12.0, è anche possibile proteggere le chiavi NVE con "KMS DI AWS".

AWS KMS, AKV e Cloud KMS possono essere utilizzati per proteggere "Chiavi NetApp Volume Encryption (NVE)" Solo per SVM di dati.

A proposito di questa attività

La gestione delle chiavi con un provider cloud può essere abilitata con l'interfaccia CLI o l'API REST ONTAP.

Quando si utilizza un cloud provider per proteggere le chiavi, tenere presente che per impostazione predefinita viene utilizzata una LIF SVM dati per comunicare con l'endpoint di gestione delle chiavi cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione del provider cloud (login.microsoftonline.com per Azure; oauth2.googleapis.com per Cloud KMS). Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Quando si utilizza un servizio di gestione delle chiavi di un provider cloud, è necessario tenere presenti le seguenti limitazioni:

- La gestione delle chiavi con cloud provider non è disponibile per crittografia dello storage NetApp (NSE) e crittografia aggregata di NetApp (NAE). "KMIP esterni" può essere utilizzato in alternativa.
- La gestione delle chiavi del provider cloud non è disponibile per le configurazioni MetroCluster.
- La gestione delle chiavi del cloud provider può essere configurata solo su una SVM dati.

Prima di iniziare

- È necessario aver configurato il KMS sul cloud provider appropriato.
- I nodi del cluster ONTAP devono supportare NVE.
- "È necessario aver installato le licenze Volume Encryption (VE) e Encryption Key Management (MTEKM) multi-tenant". Queste licenze sono incluse con "ONTAP uno".
- Devi essere un amministratore del cluster o di SVM.
- I dati SVM non devono includere volumi crittografati né utilizzare un gestore delle chiavi. Se i dati SVM includono volumi crittografati, è necessario eseguirne la migrazione prima di configurare il KMS.

Abilitare la gestione esterna delle chiavi

L'attivazione della gestione esterna delle chiavi dipende dal gestore specifico delle chiavi utilizzato. Scegliere la scheda del gestore delle chiavi e dell'ambiente appropriati.

AWS

Prima di iniziare

- È necessario creare una concessione per la chiave AWS KMS che verrà utilizzata dal ruolo IAM che gestisce la crittografia. Il ruolo IAM deve includere una policy che consenta le seguenti operazioni:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

    Per ulteriori informazioni, consultare la documentazione AWS per "sovvenzioni".

Abilitare AWS KMV su una SVM ONTAP

1. Prima di iniziare, procurarsi l'ID della chiave di accesso e la chiave segreta da AWS KMS.
2. Impostare il livello di privilegio su Advanced (avanzato):
   `set -priv advanced`
3. Abilitare AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando richiesto, inserire la chiave segreta.
5. Verificare che AWS KMS sia stato configurato correttamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Azure

Abilitare il vault delle chiavi Azure su una SVM ONTAP

1. Prima di iniziare, è necessario ottenere le credenziali di autenticazione appropriate dall'account Azure, un certificato o un segreto client. È inoltre necessario garantire che tutti i nodi del cluster siano integri. Puoi controllare questo con il comando `cluster show`.
2. Impostare il livello di privilegi su avanzato
   `set -priv advanced`
3. Abilitare AKV su SVM
   `security key-manager external azure enable -client-id *client_id* -tenant-id *tenant_id* -name -key-id *key_id* -authentication-method {certificate|client-secret}` Quando richiesto, immettere il certificato del client o il segreto del client dall'account Azure.
4. Verificare che AKV sia attivato correttamente:
   `security key-manager external azure show vserver` *`svm_name`*
   Se la raggiungibilità del servizio non è corretta, stabilire la connettività con il servizio di gestione delle chiavi AKV tramite data SVM LIF.

Google Cloud

Abilitare KMS cloud su una SVM ONTAP

1. Prima di iniziare, ottenere la chiave privata per il file delle chiavi dell'account Google Cloud KMS in formato JSON. Questo è disponibile nel tuo account GCP.
   È inoltre necessario garantire che tutti i nodi del cluster siano integri. Puoi controllare questo con il comando `cluster show`.
2. Impostare il livello di privilegi su avanzato:

```
set -priv advanced
```

3. Abilitare Cloud KMS su SVM
   `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
   Quando richiesto, inserire il contenuto del file JSON con la chiave privata dell'account di servizio
4. Verificare che Cloud KMS sia configurato con i parametri corretti:
   `security key-manager external gcp show vserver svm_name`
   Lo stato di `kms_wrapped_key_status` lo sarà `"UNKNOWN"` se non sono stati creati volumi crittografati.
   Se la raggiungibilità del servizio non è corretta, stabilire la connettività al servizio di gestione delle chiavi GCP tramite data SVM LIF.

Se uno o più volumi crittografati sono già configurati per un SVM di dati e le chiavi NVE corrispondenti sono gestite dal gestore delle chiavi integrato SVM di amministrazione, tali chiavi devono essere migrate al servizio di gestione delle chiavi esterno. Per eseguire questa operazione con la CLI, eseguire il comando: `security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*` Non è possibile creare nuovi volumi crittografati per i dati SVM del tenant fino a quando tutte le chiavi NVE dei dati SVM non vengono migrate correttamente.

Informazioni correlate

- "Crittografia dei volumi con le soluzioni di crittografia NetApp per Cloud Volumes ONTAP"

Abilitare la gestione delle chiavi integrata in ONTAP 9.6 e versioni successive (NVE)

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager onboard sync` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, è necessario eseguire `security key-manager onboard enable` eseguire prima il comando sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi. Quando si esegue `security key-manager onboard enable` dal cluster locale, quindi eseguire la sincronizzazione sul cluster remoto, non è necessario eseguire `enable` comando di nuovo dal cluster remoto.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. È possibile utilizzare `cc-mode-enabled=yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `cc-mode-enabled=yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

Quando si configura la crittografia dei dati ONTAP a riposo, per soddisfare i requisiti per le soluzioni commerciali per classificati (CSFC), è necessario utilizzare NSE con NVE e assicurarsi che il gestore delle chiavi integrato sia attivato in modalità Criteri comuni. Fare riferimento a. "CSFC Solution Brief" Per ulteriori

informazioni su CSFC.

> Quando Onboard Key Manager è attivato in modalità Common Criteria (Criteri comuni) (`cc-mode-enabled=yes`), il comportamento del sistema viene modificato nei seguenti modi:
>
> - Il sistema monitora i tentativi consecutivi di passphrase del cluster non riusciti quando si opera in modalità Common Criteria.
>
> Se non si riesce a inserire la passphrase del cluster corretta all'avvio, i volumi crittografati non vengono montati. Per risolvere questo problema, riavviare il nodo e inserire la passphrase del cluster corretta. Una volta avviato, il sistema consente fino a 5 tentativi consecutivi di inserire correttamente la passphrase del cluster in un periodo di 24 ore per qualsiasi comando che richieda la passphrase del cluster come parametro. Se il limite viene raggiunto (ad esempio, non è stato possibile inserire correttamente la passphrase del cluster 5 volte di seguito), è necessario attendere che il periodo di timeout di 24 ore sia trascorso oppure riavviare il nodo per ripristinare il limite.
>
> - Gli aggiornamenti delle immagini di sistema utilizzano il certificato di firma del codice NetApp RSA-3072 insieme ai digest con firma del codice SHA-384 per controllare l'integrità dell'immagine invece del certificato di firma del codice NetApp RSA-2048 e dei digest con firma del codice SHA-256.
>
> Il comando upgrade verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida ha esito positivo, il processo di aggiornamento dell'immagine passa alla fase successiva; in caso contrario, l'aggiornamento dell'immagine non riesce. Vedere `cluster image` pagina man per informazioni relative agli aggiornamenti del sistema.

> Onboard Key Manager memorizza le chiavi nella memoria volatile. I contenuti della memoria volatile vengono cancellati quando il sistema viene riavviato o arrestato. In condizioni operative normali, il contenuto della memoria volatile viene cancellato entro 30 secondi quando il sistema viene arrestato.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare la configurazione di Key Manager:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

> Impostare `cc-mode-enabled=yes` per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `cc-mode-enabled=yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Il `- cc-mode-enabled` L'opzione non è supportata nelle configurazioni MetroCluster. Il `security key-manager onboard enable` il comando sostituisce `security key-manager setup` comando.

Nell'esempio seguente viene avviato il comando di configurazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

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

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

2. Al prompt della 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.

3. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
4. Verificare che le chiavi di autenticazione siano state create:

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

   > Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina man.

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

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                Key Type Encryption   Restored

-----------------------------------  -------- ------------ --------

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

   `volume encryption conversion start`

   Onboard Key Manager deve essere completamente configurato prima di convertire i volumi. In un ambiente MetroCluster, il gestore delle chiavi integrato deve essere configurato su entrambi i siti.

Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere "Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate".

Abilitare la gestione delle chiavi integrata in ONTAP 9.5 e versioni precedenti (NVE)

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e. `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

> Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

Prima di iniziare

- Se si utilizza NSE o NVE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

  "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare la configurazione di Key Manager:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente.

   Nell'esempio seguente viene avviata l'impostazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Invio `yes` quando viene richiesto di configurare la gestione delle chiavi integrata.
3. Al prompt della 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.

4. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
5. Verificare che le chiavi siano configurate per tutti i nodi:

   ```
   security key-manager key show
   ```

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

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

   ```
   volume encryption conversion start
   ```

   Onboard Key Manager deve essere completamente configurato prima di convertire i volumi. In un ambiente MetroCluster, il gestore delle chiavi integrato deve essere configurato su entrambi i siti.

Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere "Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate".

Abilitare la gestione delle chiavi integrata nei nodi appena aggiunti

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

> Per ONTAP 9.5 e versioni precedenti, è necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.
>
> Per ONTAP 9.6 e versioni successive, è necessario eseguire `security key-manager sync` ogni volta che si aggiunge un nodo al cluster.
>
> Se si aggiunge un nodo a un cluster che ha configurato la gestione delle chiavi integrate, eseguire questo comando per aggiornare le chiavi mancanti.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- A partire da ONTAP 9.6, è necessario eseguire `security key-manager onboard enable` sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e. `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

> Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

Crittografare i dati del volume con NVE

Crittografare i dati del volume con la panoramica di NVE

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

Abilitare la crittografia a livello aggregato con la licenza VE

A partire da ONTAP 9,7, gli aggregati e i volumi appena creati sono crittografati per impostazione predefinita, quando si dispone di "Licenza VE" e gestione della chiave integrata o esterna. A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare.

A proposito di questa attività

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

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

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

Prima di iniziare

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

Fasi

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

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

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

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

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

- ONTAP 9.7 o versione successiva:

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

- ONTAP 9.6 o versioni precedenti:

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

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

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

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

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

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

Al termine

Eseguire `volume create` per creare i volumi crittografati.

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

Attivare la crittografia su un nuovo volume

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

A proposito di questa attività

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

sulla crittografia dei volumi.

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

- A partire da ONTAP 9.4, se si attiva `cc-mode` Quando si configura Onboard Key Manager, i volumi creati con `volume create` i comandi vengono crittografati automaticamente, indipendentemente dal fatto che l'utente lo specifichi o meno `-encrypt true`.
- In ONTAP 9.6 e versioni precedenti, è necessario utilizzare `-encrypt true` con `volume create` comandi per attivare la crittografia (a condizione che non sia stata attivata) `cc-mode`).
- Se si desidera creare un volume NAE in ONTAP 9.6, è necessario attivare NAE a livello di aggregato. Fare riferimento a. Abilitare la crittografia a livello di aggregato con la licenza VE per ulteriori dettagli su questa attività.
- A partire da ONTAP 9,7, i volumi appena creati vengono crittografati per impostazione predefinita quando si dispone di "Licenza VE" e gestione della chiave integrata o esterna. Per impostazione predefinita, i nuovi volumi creati in un aggregato NAE saranno di tipo NAE anziché NVE.
  - In ONTAP 9.7 e versioni successive, se si aggiunge `-encrypt true` al `volume create` Comando per creare un volume in un aggregato NAE, il volume avrà la crittografia NVE invece di NAE. Tutti i volumi in un aggregato NAE devono essere crittografati con NVE o NAE.

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

Fasi

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

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

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

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

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

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

Risultato

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

=
:allow-uri-read:

Attivare la crittografia su un volume esistente

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

A proposito di questa attività

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

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

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

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

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

Fasi

1. Abilitare la crittografia su un volume esistente:

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

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

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

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

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

2. Verificare lo stato dell'operazione di conversione:

   `volume encryption conversion show`

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

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

```
cluster1::> volume encryption conversion show

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

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

   `volume show -is-encrypted true`

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

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

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

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

Risultato

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

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

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

A proposito di questa attività

- A partire da ONTAP 9.8, è possibile utilizzare `volume move start` Per attivare la crittografia su un volume SnapLock o FlexGroup.
- A partire da ONTAP 9.4, se si attiva "cc-mode" quando si imposta il Gestore chiavi integrato, i volumi creati con `volume move start` i comandi vengono crittografati automaticamente. Non è necessario specificare `-encrypt-destination true`.
- A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da spostare. Un volume crittografato con una chiave univoca è chiamato *volume NVE* (ovvero utilizza la crittografia del volume NetApp). Un volume crittografato con una

chiave a livello di aggregato viene chiamato *volume NAE* (per NetApp aggregate Encryption). I volumi non in testo normale non sono supportati negli aggregati NAE.

- A partire da ONTAP 9.14.1, puoi crittografare un volume root di una SVM con NVE. Per ulteriori informazioni, vedere Configurare la crittografia dei volumi NetApp su un volume root della SVM.

Prima di iniziare

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

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

Fasi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   `volume show -is-encrypted true`

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

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

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

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

Risultato

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

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

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

A proposito di questa attività

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

Prima di iniziare

- Il volume root della SVM non deve trovarsi in un aggregato crittografato con crittografia degli aggregati NetApp (NAE).
- È necessario aver abilitato la crittografia con Onboard Key Manager o con un gestore di chiavi esterno.
- È necessario eseguire ONTAP 9.14.1 o versione successiva.
- Per migrare una SVM contenente un volume root crittografato con NVE, al termine della migrazione è necessario convertire il volume root della SVM in un volume di testo normale, quindi crittografare di nuovo il volume root della SVM.
  - Se l'aggregato di destinazione della migrazione SVM utilizza NAE, il volume root eredita NAE per impostazione predefinita.
- Se la SVM si trova in una relazione di disaster recovery della SVM:
  - Le impostazioni di crittografia su una SVM con mirroring non vengono copiate nella destinazione. Se abiliti NVE sull'origine o sulla destinazione, devi abilitare NVE separatamente sul volume root della SVM con mirroring.
  - Se tutti gli aggregati nel cluster di destinazione utilizzano NAE, il volume root della SVM utilizzerà NAE.

Fasi

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

CLI

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

Crittografare il volume root in uso

1. Convertire il volume root in un volume crittografato:

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

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

Crittografa il volume root della SVM spostandolo

1. Avvio dello spostamento di un volume:

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

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

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

System Manager

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

Abilitare la crittografia del volume root del nodo

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

A proposito di questa attività

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

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

Prima di iniziare

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

Fasi

1. Crittografare il volume root:

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

2. Verificare lo stato dell'operazione di conversione:

   ```
   volume encryption conversion show
   ```

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

   ```
   volume show -fields
   ```

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

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

Configurare la crittografia basata su hardware NetApp

Configurazione della panoramica della crittografia basata su hardware NetApp

La crittografia basata su hardware di NetApp supporta la crittografia completa dei dischi (FDE) dei dati così come vengono scritti. I dati non possono essere letti senza una chiave di crittografia memorizzata nel firmware. La chiave di crittografia, a sua volta, è accessibile solo a un nodo autenticato.

Comprendere la crittografia basata su hardware NetApp

Un nodo esegue l'autenticazione su un'unità con crittografia automatica utilizzando una chiave di autenticazione recuperata da un server di gestione delle chiavi esterno o da Onboard Key Manager:

- Il 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). Si consiglia di configurare i server di gestione delle chiavi esterni su un sistema storage diverso dai dati.
- Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati.

È possibile utilizzare NetApp Volume Encryption con crittografia basata su hardware per "eseguire la doppia crittografia `d`" dei dati su dischi con crittografia automatica.

Quando i dischi con crittografia automatica sono abilitati, anche il core dump è crittografato.

Se una coppia ha utilizza dischi SAS o NVMe con crittografia (SED, NSE, FIPS), 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.

Tipi di dischi con crittografia automatica supportati

Sono supportati due tipi di dischi con crittografia automatica:

- I dischi SAS o NVMe con crittografia automatica certificati FIPS sono supportati su tutti i sistemi FAS e AFF. Questi dischi, denominati *dischi FIPS,* sono conformi ai requisiti della pubblicazione Federal Information Processing Standard 140-2, livello 2. Le funzionalità certificate consentono di proteggere oltre alla crittografia, ad esempio prevenendo attacchi di tipo Denial-of-service sul disco. I dischi FIPS non possono essere combinati con altri tipi di dischi sullo stesso nodo o coppia ha.
- A partire da ONTAP 9.6, i dischi NVMe con crittografia automatica che non hanno superato i test FIPS sono supportati sui sistemi AFF A800, A320 e successivi. Questi dischi, denominati *SED*, offrono le stesse funzionalità di crittografia dei dischi FIPS, ma possono essere combinati con dischi non crittografanti sullo stesso nodo o coppia ha.
- Tutti i dischi convalidati FIPS utilizzano un modulo di crittografia del firmware che è stato eseguito attraverso la convalida FIPS. Il modulo crittografico del disco FIPS non utilizza chiavi generate al di fuori del disco (la passphrase di autenticazione immessa nel disco viene utilizzata dal modulo crittografico del firmware del disco per ottenere una chiave di crittografia).

Le unità non crittografate sono unità che non sono unità SED o FIPS.

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.

Quando utilizzare la gestione esterna delle chiavi

Sebbene sia meno costoso e generalmente più conveniente utilizzare il gestore delle chiavi integrato, è consigliabile utilizzare la gestione esterna delle chiavi se si verifica una delle seguenti condizioni:

- La policy aziendale richiede una soluzione di gestione delle chiavi che utilizzi un modulo crittografico FIPS 140-2 livello 2 (o superiore).
- Hai bisogno di una soluzione multi-cluster, con gestione centralizzata delle chiavi di crittografia.
- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

Dettagli del supporto

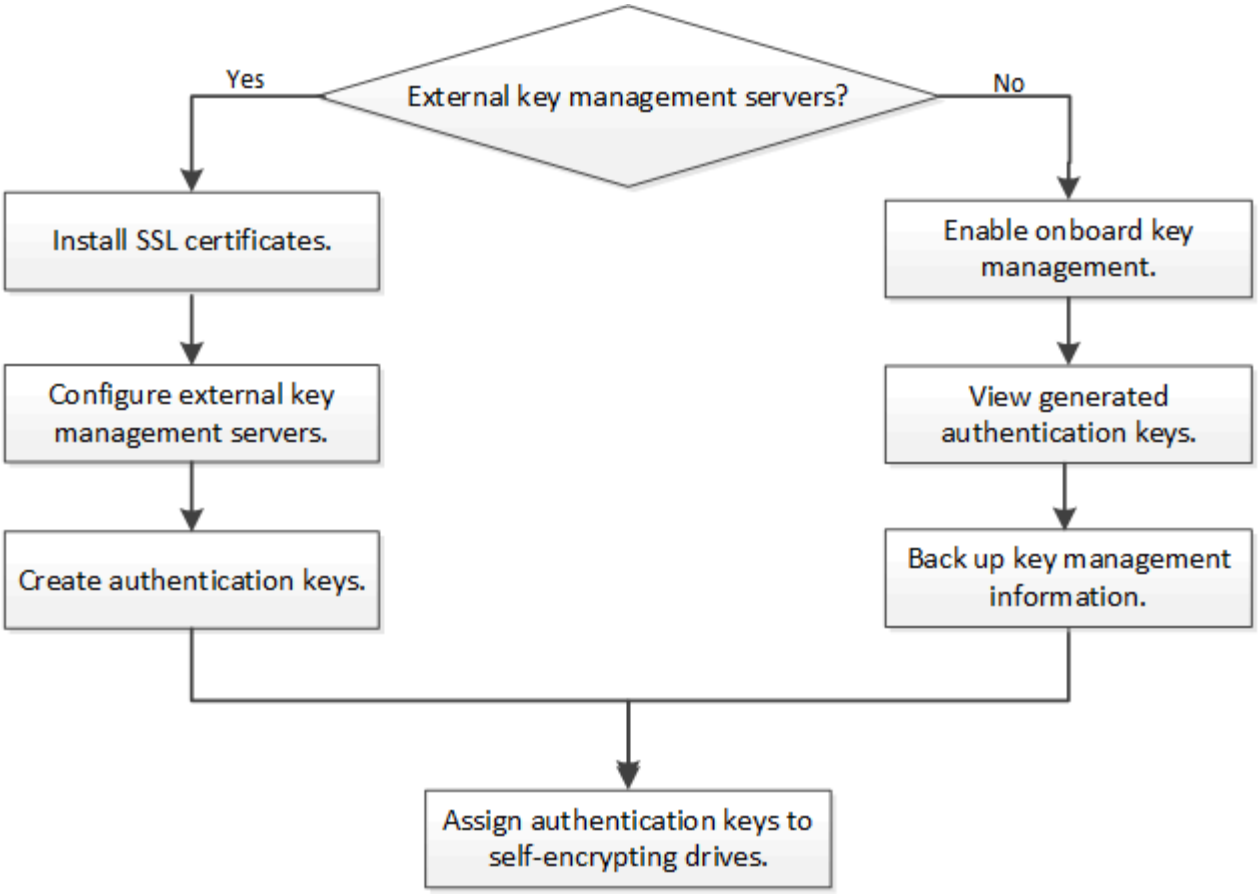
La seguente tabella mostra importanti dettagli sul supporto della crittografia hardware. Consulta la matrice di interoperabilità per le informazioni più recenti su server KMIP, sistemi storage e shelf di dischi supportati.

Risorsa o funzione	Dettagli del supporto

Set di dischi non omogenei	• I dischi FIPS non possono essere combinati con altri tipi di dischi sullo stesso nodo o coppia ha. Le coppie ha conformi possono coesistere con coppie ha non conformi nello stesso cluster. • È possibile combinare i dischi con dischi non crittografanti sullo stesso nodo o coppia ha.
Tipo di disco	• I dischi FIPS possono essere SAS o NVMe. • I dischi Sed devono essere NVMe.
Interfacce di rete da 10 GB	A partire da ONTAP 9.3, le configurazioni di gestione delle chiavi KMIP supportano interfacce di rete da 10 GB per le comunicazioni con server di gestione delle chiavi esterni.
Porte per la comunicazione con il server di gestione delle chiavi	A partire da ONTAP 9.3, è possibile utilizzare qualsiasi porta del controller di storage per la comunicazione con il server di gestione delle chiavi. In caso contrario, utilizzare la porta e0M per la comunicazione con i server di gestione delle chiavi. A seconda del modello di controller di storage, alcune interfacce di rete potrebbero non essere disponibili durante il processo di avvio per la comunicazione con i server di gestione delle chiavi.
MetroCluster (MCC)	• I dischi NVMe supportano MCC. • I dischi SAS non supportano MCC.

Workflow di crittografia basato su hardware

È necessario configurare i servizi di gestione delle chiavi prima che il cluster possa autenticarsi sull'unità con crittografia automatica. È possibile utilizzare un server di gestione delle chiavi esterno o un gestore delle chiavi integrato.



Informazioni correlate

- "NetApp Hardware Universe"
- "NetApp Volume Encryption e NetApp aggregate Encryption"

Configurare la gestione esterna delle chiavi

Configurare una panoramica sulla gestione esterna delle chiavi

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).

Per ONTAP 9.1 e versioni precedenti, è necessario assegnare le LIF di gestione dei nodi alle porte configurate con il ruolo di gestione dei nodi prima di poter utilizzare il gestore delle chiavi esterno.

La crittografia dei volumi NetApp (NVE) può essere implementata con Onboard Key Manager in ONTAP 9.1 e versioni successive. 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 Key Manager esterni in un cluster. Vedere Configurare i server delle chiavi in cluster.

Raccogliere le informazioni di rete in ONTAP 9.2 e versioni precedenti

Se si utilizza ONTAP 9.2 o versioni precedenti, compilare il foglio di lavoro per la configurazione di rete prima di attivare la gestione esterna delle chiavi.

A partire da ONTAP 9.3, il sistema rileva automaticamente tutte le informazioni di rete necessarie.

Elemento	Note	Valore
Nome dell'interfaccia di rete per la gestione delle chiavi		
Indirizzo IP dell'interfaccia di rete per la gestione delle chiavi	Indirizzo IP della LIF di gestione dei nodi, in formato IPv4 o IPv6	
Gestione delle chiavi interfaccia di rete IPv6 lunghezza prefisso di rete	Se si utilizza IPv6, la lunghezza del prefisso di rete IPv6	
Subnet mask dell'interfaccia di rete per la gestione delle chiavi		
Gestione delle chiavi Indirizzo IP del gateway dell'interfaccia di rete		
Indirizzo IPv6 per l'interfaccia di rete del cluster	Obbligatorio solo se si utilizza IPv6 per l'interfaccia di rete per la gestione delle chiavi	
Numero di porta per ciascun server KMIP	Opzionale. Il numero di porta deve essere lo stesso per tutti i server KMIP. Se non si specifica un numero di porta, per impostazione predefinita viene impostata la porta 5696, che corrisponde alla porta assegnata dall'autorità IANA (Internet Assigned Numbers Authority) per KMIP.	
Nome tag chiave	Opzionale. Il nome del tag della chiave viene utilizzato per identificare tutte le chiavi appartenenti a un nodo. Il nome predefinito del tag della chiave è il nome del nodo.	

Informazioni correlate

"Report tecnico di NetApp 3954: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per IBM Tivoli Lifetime Key Manager"

"Report tecnico di NetApp 4074: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per SafeNet KeySecure"

Installare i certificati SSL sul cluster

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
   ```

Gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (basato su hardware)

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 di chiavi secondari per ogni server di chiavi primario per creare un server di 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.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il 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` il comando sostituisce `security key-manager setup` comando. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne. Per la sintassi completa dei comandi, vedere le pagine man.
   > - 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:

   ```
   clusterl::> 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` il comando sostituisce `security key-manager show -status` comando. Per la sintassi completa dei comandi, vedere la pagina man.

```
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.
```

Abilitare la gestione esterna delle chiavi 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 il 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.

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 la sintassi completa dei comandi, vedere la pagina man.

```
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 di chiavi esterne in cluster

A partire da ONTAP 9.11.1, è possibile configurare la connettività ai server di gestione delle chiavi esterni in cluster su una SVM. Con i key server in cluster, è possibile designare i key server primari e secondari su una SVM. Durante la registrazione delle chiavi, ONTAP tenta innanzitutto di accedere a un server principale prima di tentare di accedere in sequenza ai server secondari fino al completamento dell'operazione, evitando la duplicazione delle chiavi.

I Key server esterni possono essere utilizzati per le chiavi NSE, NVE, NAE e SED. Una SVM può supportare fino a quattro server KMIP esterni primari. Ciascun server primario può supportare fino a tre server secondari per le chiavi.

Prima di iniziare

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

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

1. Verificare che non sia stata attivata alcuna gestione delle chiavi per il cluster:
   `security key-manager external show -vserver` *`svm_name`*
   Se SVM ha già attivato un massimo di quattro server principali, è necessario rimuovere uno dei server principali esistenti prima di aggiungerne uno nuovo.
2. Attivare il gestore delle chiavi primario:
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter 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`*

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

1. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter 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`*
   Per ulteriori informazioni sui server di chiavi secondari, vedere [mod-secondary].

Modificare i server delle chiavi in cluster

È possibile modificare i cluster di Key Server esterni modificando lo stato (primario o secondario) di determinati Key Server, aggiungendo e rimuovendo i Key Server secondari o modificando l'ordine di accesso dei Key Server secondari.

Convertire i server chiavi primari e secondari

Per convertire un server di chiavi primario in un server di chiavi secondario, è necessario prima rimuoverlo

dalla SVM con `security key-manager external remove-servers` comando.

Per convertire un server chiavi secondario in un server chiavi primario, è necessario prima rimuovere il server chiavi secondario dal server chiavi primario esistente. Vedere [mod-secondary]. Se si converte un server chiavi secondario in un server primario durante la rimozione di una chiave esistente, il tentativo di aggiungere un nuovo server prima di completare la rimozione e la conversione può comportare la duplicazione delle chiavi.

Modificare i server chiavi secondari

I server di chiavi secondari vengono gestiti con `-secondary-key-servers` del parametro `security key-manager external modify-server` comando. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole. L'ordine specificato dei server di chiavi secondari nell'elenco determina la sequenza di accesso per i server di chiavi secondari. L'ordine di accesso può essere modificato eseguendo il comando `security key-manager external modify-server` con i server di chiavi secondari inseriti in una sequenza diversa.

Per rimuovere un server di chiavi secondario, la `-secondary-key-servers` gli argomenti devono includere i server chiave che si desidera conservare mentre si omette quello da rimuovere. Per rimuovere tutti i server di chiavi secondari, utilizzare l'argomento `-`, non significa nessuno.

Per ulteriori informazioni, fare riferimento a. `security key-manager external` nella "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 `security key-manager key delete` per eliminare le chiavi inutilizzate. Il `security key-manager key delete` Il comando non riesce se la chiave è attualmente in uso da ONTAP. Per utilizzare questo comando, è necessario disporre di privilegi superiori a "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
   ```

   > Impostazione `prompt-for-key=true` fa in modo che il sistema richieda all'amministratore del cluster la passphrase da utilizzare per l'autenticazione dei dischi crittografati. In caso contrario, il sistema genera automaticamente una passphrase da 32 byte. Il `security key-manager key create` il comando sostituisce `security key-manager create-key` comando. Per la sintassi completa dei comandi, vedere la pagina man.

   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:
   000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

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

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

   > Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina man. 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:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

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`

   Per la sintassi completa dei comandi, vedere la pagina man del 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 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: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   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`

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

   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:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


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

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

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

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
```

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

> 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
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

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
```

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
[...]
```

Configurare la gestione delle chiavi integrata

Attiva la gestione delle chiavi integrata in ONTAP 9.6 e versioni successive

È possibile utilizzare Onboard Key Manager per autenticare i nodi del cluster su un disco FIPS o SED. Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati. Onboard Key Manager è conforme a FIPS-140-2 livello 1.

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager onboard enable` ogni volta che si aggiunge un nodo al cluster. Nelle configurazioni MetroCluster, è necessario eseguire `security key-manager onboard`

`enable` sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. Ad eccezione di MetroCluster, è possibile utilizzare `cc-mode-enabled=yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

> Quando Onboard Key Manager è attivato in modalità Common Criteria (Criteri comuni) (`cc-mode-enabled=yes`), il comportamento del sistema viene modificato nei seguenti modi:
>
> - Il sistema monitora i tentativi consecutivi di passphrase del cluster non riusciti quando si opera in modalità Common Criteria.
>
> Se NetApp Storage Encryption (NSE) è attivato e non si riesce a inserire la passphrase del cluster corretta all'avvio, il sistema non può autenticare i propri dischi e si riavvia automaticamente. Per risolvere il problema, al prompt di boot occorre inserire la passphrase del cluster corretta. Una volta avviato, il sistema consente fino a 5 tentativi consecutivi di inserire correttamente la passphrase del cluster in un periodo di 24 ore per qualsiasi comando che richieda la passphrase del cluster come parametro. Se il limite viene raggiunto (ad esempio, non è stato possibile inserire correttamente la passphrase del cluster 5 volte di seguito), è necessario attendere che il periodo di timeout di 24 ore sia trascorso oppure riavviare il nodo per ripristinare il limite.
>
> - Gli aggiornamenti delle immagini di sistema utilizzano il certificato di firma del codice NetApp RSA-3072 insieme ai digest con firma del codice SHA-384 per controllare l'integrità dell'immagine invece del certificato di firma del codice NetApp RSA-2048 e dei digest con firma del codice SHA-256.
>
> Il comando upgrade verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida ha esito positivo, il processo di aggiornamento dell'immagine passa alla fase successiva; in caso contrario, l'aggiornamento dell'immagine non riesce. Per informazioni sugli aggiornamenti di sistema, consultare la pagina man "cluster image".

> Onboard Key Manager memorizza le chiavi nella memoria volatile. I contenuti della memoria volatile vengono cancellati quando il sistema viene riavviato o arrestato. In condizioni operative normali, il contenuto della memoria volatile viene cancellato entro 30 secondi quando il sistema viene arrestato.

Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

  "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare il comando di configurazione del gestore delle chiavi:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

> Impostare `cc-mode-enabled=yes` per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Il `- cc-mode-enabled` L'opzione non è supportata nelle configurazioni MetroCluster. Il `security key-manager onboard enable` il comando sostituisce `security key-manager setup` comando.

Nell'esempio seguente viene avviato il comando di configurazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

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

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

2. Al prompt della 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.

3. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
4. Verificare che le chiavi di autenticazione siano state create:

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

> Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina man.

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

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

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

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 per utilizzarle in caso di disastro.

Abilitare la gestione delle chiavi integrata in ONTAP 9.5 e versioni precedenti

È possibile utilizzare Onboard Key Manager per autenticare i nodi del cluster su un disco FIPS o SED. Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati. Onboard Key Manager è conforme a FIPS-140-2 livello 1.

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati

crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e. `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

> Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

  "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare la configurazione di Key Manager:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente.

   Nell'esempio seguente viene avviata l'impostazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Invio `yes` quando viene richiesto di configurare la gestione delle chiavi integrata.
3. Al prompt della 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.

4. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
5. Verificare che le chiavi siano configurate per tutti i nodi:

   `security key-manager key show`

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

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Al termine

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere "Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate".

Assegnazione di una chiave di autenticazione dei dati a un'unità FIPS o SED (onboard key management)

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 accedere ai dati 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.

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`*

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   00000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4

   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`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Assegnare una chiave di autenticazione FIPS 140-2 a un disco FIPS

È possibile utilizzare `storage encryption disk modify` con il `-fips-key-id` Opzione per assegnare una chiave di autenticazione FIPS 140-2 a un disco FIPS. I nodi del cluster utilizzano questa chiave per operazioni di guida diverse dall'accesso ai dati, come la prevenzione di attacchi di tipo Denial-of-service sul disco.

A proposito di questa attività

La configurazione della sicurezza potrebbe richiedere l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

Questa procedura non comporta interruzioni.

Prima di iniziare

Il firmware del disco deve supportare la conformità FIPS 140-2. Il "Tool di matrice di interoperabilità NetApp" contiene informazioni sulle versioni del firmware del disco supportate.

Fasi

1. Assicurarsi di aver assegnato una chiave di autenticazione dei dati. Questa operazione può essere eseguita utilizzando un gestore delle chiavi esterno o un gestore delle chiavi integrato. Verificare che il tasto sia assegnato con il comando `storage encryption disk show`.
2. Assegnare una chiave di autenticazione FIPS 140-2 ai SED:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   6A1E21D8000000000100000000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

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

3. Verificare che la chiave di autenticazione sia stata assegnata:

   ```
   storage encryption disk show -fips
   ```

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

   ```
   cluster1::> storage encryption disk show -fips
   Disk    Mode FIPS-Compliance Key ID
   ------  ----
   ------------------------------------------------------------------
   2.10.0  full
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
   2.10.1  full
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
   [...]
   ```

Abilitare la modalità compatibile con FIPS a livello di cluster per le connessioni al server KMIP

È possibile utilizzare `security config modify` con il `-is-fips-enabled` Opzione per abilitare la modalità compatibile con FIPS a livello di cluster per i dati in volo. In questo modo, il cluster utilizza OpenSSL in modalità FIPS durante la connessione ai server KMIP.

A proposito di questa attività

Quando si attiva la modalità compatibile con FIPS a livello di cluster, il cluster utilizza automaticamente solo le suite di crittografia convalidate da TLS1.2 e FIPS. La modalità compatibile con FIPS a livello di cluster è disattivata per impostazione predefinita.

È necessario riavviare manualmente i nodi del cluster dopo aver modificato la configurazione di sicurezza a livello di cluster.

Prima di iniziare

- Lo storage controller deve essere configurato in modalità conforme a FIPS.
- Tutti i server KMIP devono supportare TLSv1.2. Il sistema richiede TLSv1.2 per completare la connessione al server KMIP quando è attivata la modalità compatibile con FIPS a livello di cluster.

Fasi

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

   ```
   set -privilege advanced
   ```

2. Verificare che TLSv1.2 sia supportato:

   ```
   security config show -supported-protocols
   ```

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

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Abilitare la modalità compatibile con FIPS a livello di cluster:

   `security config modify -is-fips-enabled true -interface SSL`

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

4. Riavviare manualmente i nodi del cluster.
5. Verificare che la modalità compatibile con FIPS a livello di cluster sia attivata:

   `security config show`

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

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
     QAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAAAAACAAAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAAA
     KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAAwAAABgBAAAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------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:

   ```
   clusterl::> 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:

   ```
   svml::> 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
   ```