Configurare il volume NetApp e la crittografia aggregata

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Configurare il volume NetApp e la crittografia aggregata

Scopri di più sulla crittografia di volumi e aggregati ONTAP NetApp

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, sono crittografati sia i metadati che i dati (incluse le snapshot). 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 9.17.1, è possibile utilizzare Barbican KMS per proteggere le chiavi NVE solo per le SVM di dati.
  - 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.

> I provider di Cloud KMS come Azure Key Vault e AWS KMS non supportano KMIP. Di conseguenza, non sono elencati su 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 Cloud Volumes 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	MetroCluster è supportato a partire da ONTAP 9.8. A partire da ONTAP 9.6, NVE supporta l'ambito SVM solo per la gestione delle chiavi esterne, non per Onboard Key Manager.
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. La crittografia configurata sull'origine non verrà replicata sulla destinazione. La crittografia deve essere configurata manualmente sull'origine e sulla destinazione. Fare riferimento a Configurare NVE e Crittografare i dati del volume con NVE. • 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	SnapLock è supportato sia in modalità Compliance che Enterprise, solo per i nuovi volumi. Non è possibile attivare la crittografia su un volume SnapLock esistente.
Volumi FlexGroup	Sono supportati i volumi FlexGroup . 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.

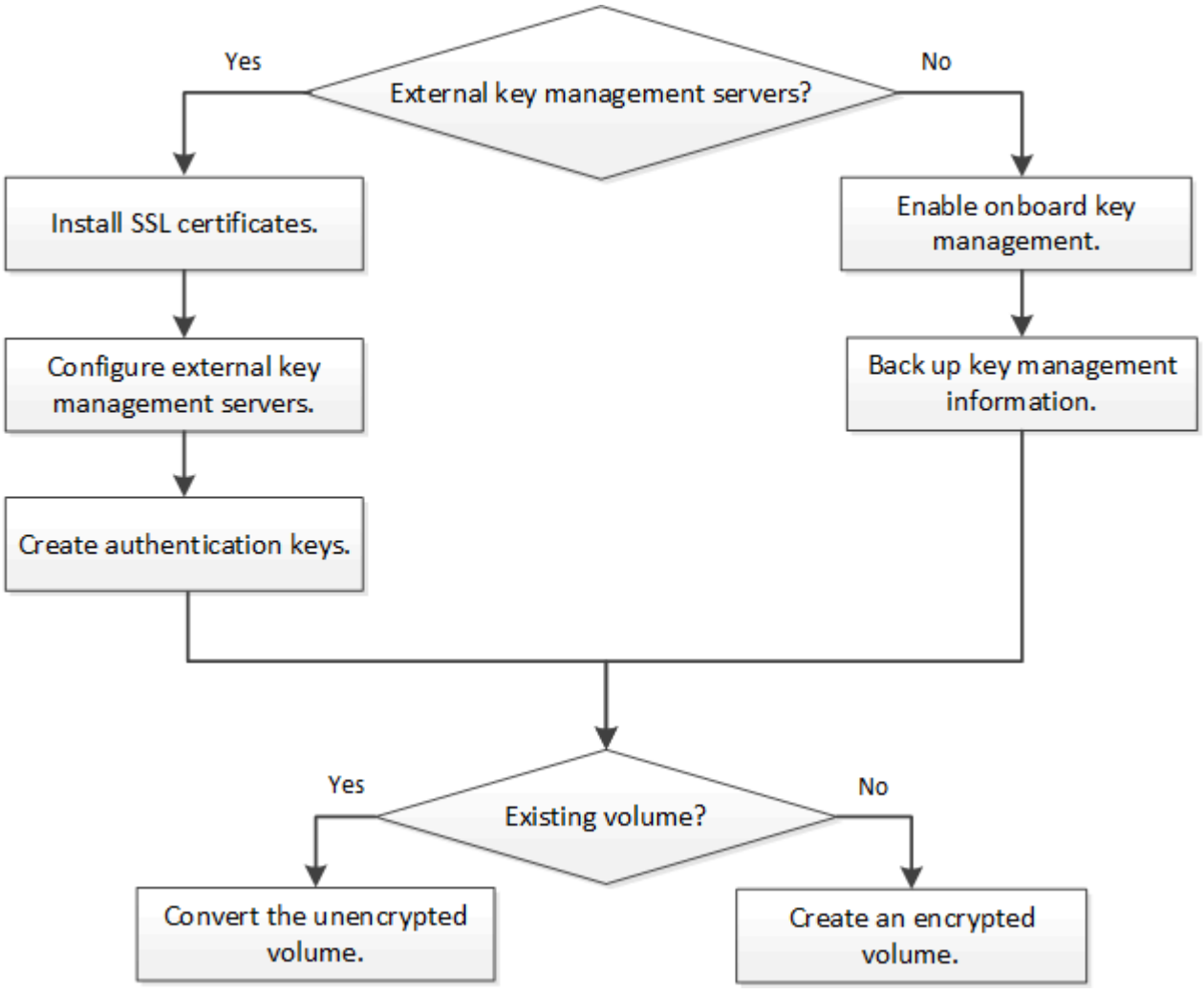
Transizione 7-Mode	A partire da 7-Mode Transition Tool 3.3, è possibile utilizzare 7-Mode Transition Tool CLI per eseguire una transizione basata su copia a volumi di destinazione abilitati per NVE sul sistema in cluster.

Informazioni correlate

- "FAQ - NetApp Volume Encryption e NetApp aggregate Encryption"
- "creazione di aggregati di archiviazione"

Flusso di lavoro di crittografia del volume ONTAP NetApp

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

Determina se la versione del cluster ONTAP 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.

Fasi

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 sta utilizzando una piattaforma non elencata in "Dettagli del supporto".

Installare la licenza di crittografia del volume su un cluster ONTAP

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 necessario, i clienti esistenti possono scegliere di "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

Scopri come configurare la gestione delle chiavi esterne con ONTAP NetApp Volume Encryption

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 presente nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol). Oltre a Onboard Key Manager, ONTAP supporta diversi server di gestione delle chiavi esterni.

A partire da ONTAP 9.10.1, è possibile utilizzare Azure Key Vault o servizio Google Cloud Key Manager per proteggere le chiavi NVE per le SVM di dati. A partire da ONTAP 9.11.1, è possibile configurare più gestori di chiavi esterni in un cluster. VedereConfigurare server chiave in cluster . A partire da ONTAP 9.12.0, è possibile utilizzare "KMS DI AWS" per proteggere le chiavi NVE per le SVM di dati. A partire da ONTAP 9.17.1, è possibile utilizzare OpenStack Barbican KMS per proteggere le chiavi NVE per le SVM di dati.

Gestire i responsabili delle chiavi esterne con ONTAP 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 **crittografia**, 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 **crittografia** in **protezione**, selezionare .

2. Per aggiungere un server delle chiavi principale, selezionare + Add e completare i campi **Indirizzo IP o Nome host** e **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 associare 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 associare 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 **crittografia**, selezionare , quindi selezionare **Modifica gestore chiavi esterno**.
Storage VM Scope External Key Manager	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **crittografia** in **protezione**, selezionare , quindi selezionare **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 **crittografia**, selezionare ⋮, quindi selezionare **Elimina gestore chiavi esterno**.
Storage VM Scope External Key Manager	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **crittografia** in **protezione**, selezionare ⋮, quindi selezionare **Elimina gestore chiavi esterno**.

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 ONTAP

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

A proposito di questa attività

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

Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.

- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.

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

Fasi

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

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

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

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

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

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

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

Informazioni correlate

- "installazione del certificato di sicurezza"

Abilita la gestione delle chiavi esterne per NVE in ONTAP 9.6 e versioni successive

Utilizzare i 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 una 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 connettere fino a quattro server KMIP a un cluster o SVM. Utilizzare almeno due server per la ridondanza e il ripristino in caso di emergenza.

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>`

  Ulteriori informazioni su `system license add` nella "Riferimento al comando ONTAP".

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.

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

Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Il server KMIP deve essere raggiungibile dal LIF di gestione dei nodi di ciascun nodo.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- In un ambiente MetroCluster :
  - MetroCluster deve essere completamente configurato prima di abilitare la gestione delle chiavi esterne.
  - È necessario installare lo stesso certificato SSL KMIP su entrambi i cluster.
  - Su entrambi i cluster deve essere configurato un gestore delle chiavi esterno.

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 il `security key-manager setup` comando. Se si esegue il comando al prompt di accesso al cluster, *`admin_SVM`* per impostazione predefinita è l'SVM di amministrazione del cluster corrente. Puoi eseguire il `security key-manager external modify` comando per modificare la configurazione della gestione delle chiavi esterne.

   Il seguente comando abilita la gestione esterna delle chiavi per `cluster1` con tre key server esterni. Il primo server chiavi viene specificato utilizzando il nome host e la porta, il secondo viene specificato utilizzando un indirizzo IP e la porta predefinita, mentre il terzo viene specificato utilizzando un indirizzo IPv6 e una porta:

```
cluster1::> security key-manager external enable -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 è l'SVM corrente. Puoi eseguire il `security key-manager external modify` comando per modificare la configurazione della 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.

   Inoltre, è possibile utilizzare il `security key-manager external add-servers` comando per configurare SVM aggiuntive. Il `security key-manager external add-servers` comando sostituisce il `security key-manager add` comando. Ulteriori informazioni su `security key-manager external add-servers` nella "Riferimento al comando ONTAP".

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

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

Node  Vserver  Key Server                                       Status
----  -------  -----------------------------------------
-------------
node1
      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.

Informazioni correlate

- Configurare i server di chiavi esterne in cluster
- "aggiunta licenza di sistema"
- "migrazione delle chiavi del gestore delle chiavi di sicurezza"
- "server aggiuntivi esterni del gestore delle chiavi di sicurezza"
- "gestore chiavi di sicurezza esterno mostra stato"

Abilita la gestione delle chiavi esterne per NVE in ONTAP 9.5 e versioni precedenti

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

A proposito di questa attività

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

Prima di iniziare

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

Fasi

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

   `security key-manager setup`

   Viene avviata la configurazione di Key Manager.

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

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

   `security key-manager add -address key_management_server_ipaddress`

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

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

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

   `security key-manager add -address key_management_server_ipaddress`

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

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

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

   `security key-manager show -status`

   Per saperne di più sui comandi descritti in questa procedura, consultare"Riferimento al comando ONTAP" .

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

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

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

   `volume encryption conversion start`

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

Gestire le chiavi NVE per le SVM dei dati ONTAP con un provider cloud

A partire da ONTAP 9.10.1, puoi utilizzare "Azure Key Vault (AKV)" e "Servizio di gestione delle chiavi di Google Cloud Platform (Cloud KMS)"proteggere le chiavi di crittografia ONTAP in un'applicazione ospitata su 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 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 in "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`*

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

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. È possibile verificarlo con il comando `cluster show`. Ulteriori informazioni su `cluster show` nella "Riferimento al comando ONTAP".
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.

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

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. È possibile verificarlo con il comando `cluster show`. Ulteriori

informazioni su `cluster show` nella "Riferimento al comando ONTAP".

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` 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 dati SVM LIF.

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

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"
- "gestore di chiavi di sicurezza esterno"

Gestisci le chiavi ONTAP con Barbican KMS

A partire da ONTAP 9.17.1, è possibile utilizzare OpenStack "Barbican KMS" per proteggere le chiavi di crittografia ONTAP . Barbican KMS è un servizio per l'archiviazione e l'accesso sicuro alle chiavi. Barbican KMS può essere utilizzato per proteggere le chiavi NetApp Volume Encryption (NVE) per le SVM di dati. Barbican si basa su "OpenStack Keystone" , servizio di identità di OpenStack, per l'autenticazione.

A proposito di questa attività

È possibile configurare la gestione delle chiavi con Barbican KMS tramite la CLI o l'API REST ONTAP . Con la versione 9.17.1, il supporto di Barbican KMS presenta le seguenti limitazioni:

- Barbican KMS non è supportato per NetApp Storage Encryption (NSE) e NetApp Aggregate Encryption (NAE). In alternativa, è possibile utilizzare "KMIP esterni" o il "Gestore delle chiavi di bordo (OKM)" per le chiavi NSE e NVE.
- Barbican KMS non è supportato per le configurazioni MetroCluster .
- Barbican KMS può essere configurato solo per una SVM dati. Non è disponibile per la SVM amministrativa.

Salvo diversa indicazione, gli amministratori dell' `admin` livello di privilegio può eseguire le seguenti procedure.

Prima di iniziare

- Barbican KMS e OpenStack Keystone devono essere configurati. La SVM utilizzata con Barbican deve avere accesso di rete ai server Barbican e OpenStack Keystone .

- Se si utilizza un'autorità di certificazione (CA) personalizzata per i server Barbican e OpenStack Keystone , è necessario installare il certificato CA con `security certificate install -type server-ca -vserver <admin_svm>` .

Crea e attiva una configurazione Barbican KMS

È possibile creare una nuova configurazione Barbican KMS per una SVM e attivarla. Una SVM può avere più configurazioni Barbican KMS inattive, ma solo una può essere attiva alla volta.

Fasi

1. Crea una nuova configurazione Barbican KMS inattiva per una SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` è l'identificatore della chiave di crittografia a chiave Barbican (KEK). Inserisci un URL completo, incluso `https://` .

     Alcuni URL includono il carattere punto interrogativo (?). Il punto interrogativo attiva la guida attiva della riga di comando ONTAP . Per inserire un URL con un punto interrogativo, è necessario prima disattivare la guida attiva con il comando `set -active-help false` . L'aiuto attivo può essere successivamente riattivato con il comando `set -active-help true` . Scopri di più nel "Riferimento al comando ONTAP" .

   - `-keystone-url` è l'URL dell'host di autorizzazione OpenStack Keystone . Inserisci un URL completo, incluso `https://` .
   - `-application-cred-id` è l'ID delle credenziali dell'applicazione.

     Dopo aver inserito questo comando, ti verrà richiesta la chiave segreta delle credenziali dell'applicazione. Questo comando crea una configurazione Barbican KMS inattiva.

     L'esempio seguente crea una nuova configurazione Barbican KMS inattiva denominata `config1` per l'SVM `svm1` :

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Attiva la nuova configurazione Barbican KMS:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

È possibile utilizzare questo comando per passare da una configurazione Barbican KMS all'altra. Se è già presente una configurazione Barbican KMS attiva sulla SVM, questa verrà disattivata e la nuova configurazione verrà attivata.

3. Verificare che la nuova configurazione Barbican KMS sia attiva:

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

Questo comando fornirà lo stato della configurazione Barbican KMS attiva sull'SVM o sul nodo. Ad esempio, se l'SVM `svm1` sul nodo `node1` ha una configurazione Barbican KMS attiva, il seguente comando restituirà lo stato di tale configurazione:

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Aggiornare le credenziali e le impostazioni di una configurazione Barbican KMS

È possibile visualizzare e aggiornare le impostazioni correnti di una configurazione Barbican KMS attiva o inattiva.

Fasi

1. Visualizza le attuali configurazioni Barbican KMS per una SVM:

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

Per ogni configurazione Barbican KMS sull'SVM vengono visualizzati l'ID chiave, l'URL OpenStack Keystone e l'ID delle credenziali dell'applicazione.

2. Aggiornare le impostazioni di una configurazione Barbican KMS:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

Questo comando aggiorna le impostazioni di timeout e verifica della configurazione Barbican KMS specificata. `timeout` determina il tempo in secondi che ONTAP attenderà che Barbican risponda prima che la connessione fallisca. L'impostazione predefinita `timeout` è di dieci secondi. `verify` E `verify-host` Determina se l'identità e il nome host dell'host Barbican debbano essere verificati prima della connessione. Per impostazione predefinita, questi parametri sono impostati su `true` . IL `vserver` E `config-name` I parametri sono obbligatori. Gli altri parametri sono facoltativi.

3. Se necessario, aggiorna le credenziali di una configurazione Barbican KMS attiva o inattiva:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

Dopo aver immesso questo comando, ti verrà richiesta la chiave segreta delle nuove credenziali dell'applicazione.

4. Se necessario, ripristinare una chiave di crittografia della chiave SVM (KEK) mancante per una configurazione Barbican KMS attiva:
   a. Ripristinare un SVM KEK mancante con `security key-manager external barbican restore` :

```
security key-manager external barbican restore -vserver <svm_name>
```

Questo comando ripristinerà l'SVM KEK per la configurazione Barbican KMS attiva comunicando con il server Barbican.

5. Se necessario, ricodificare la SVM KEK per una configurazione Barbican KMS:
   a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

   b. Ripristinare la chiave SVM KEK con `security key-manager external barbican rekey-internal` :

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

Questo comando genera una nuova SVM KEK per la SVM specificata e riesegui il wrapping delle chiavi di crittografia del volume con la nuova SVM KEK. La nuova SVM KEK sarà protetta dalla

configurazione Barbican KMS attiva.

Migrazione delle chiavi tra Barbican KMS e Onboard Key Manager

È possibile migrare le chiavi da Barbican KMS a Onboard Key Manager (OKM) e viceversa. Per ulteriori informazioni su OKM, consultare "Attiva la gestione delle chiavi integrata in ONTAP 9.6 e versioni successive" .

Fasi

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

```
set -privilege advanced
```

2. Se necessario, migrare le chiavi da Barbican KMS a OKM:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` è il nome dell'SVM con la configurazione Barbican KMS.

3. Se necessario, migrare le chiavi dall'OKM al Barbican KMS:

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Disabilitare ed eliminare una configurazione Barbican KMS

È possibile disattivare una configurazione Barbican KMS attiva senza volumi crittografati ed eliminare una configurazione Barbican KMS inattiva.

Fasi

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

```
set -privilege advanced
```

2. Disabilitare una configurazione Barbican KMS attiva:

```
security key-manager keystore disable -vserver <svm_name>
```

Se sull'SVM sono presenti volumi crittografati NVE, è necessario decrittografarli o migrare le chiavi prima di disabilitare la configurazione di Barbican KMS. L'attivazione di una nuova configurazione di Barbican KMS non richiede la decrittografia dei volumi NVE o la migrazione delle chiavi e disabiliterà la configurazione di Barbican KMS attualmente attiva.

3. Elimina una configurazione Barbican KMS inattiva:

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Abilita la gestione delle chiavi integrate per NVE in ONTAP 9.6 e versioni successive

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.

Scopri di più su `security key-manager onboard enable` E `security key-manager onboard sync` nel"Riferimento al comando ONTAP" .

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 Commercial Solutions for Classified (CSfC) è necessario utilizzare NSE con NVE e assicurarsi che Onboard Key Manager sia abilitato in modalità Common Criteria. Vedere"CSFC Solution Brief" .

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 immettere la passphrase del cluster per 5 volte, attendere 24 ore o riavviare il nodo per reimpostare 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 di aggiornamento verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida riesce, il sistema procede alla fase successiva del processo di aggiornamento dell'immagine; in caso contrario, l'aggiornamento dell'immagine non riesce. Scopri di più su `cluster image` nel"Riferimento al comando ONTAP" .

Onboard Key Manager memorizza le chiavi nella memoria volatile. Il contenuto della memoria volatile viene cancellato quando il sistema viene riavviato o arrestato. Quando il sistema viene arrestato, cancella la memoria volatile entro 30 secondi.

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.

2. Inserisci 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` comando sostituisce il `security key-manager query key` comando.

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

5. Facoltativamente, è possibile convertire i 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.

Dopo aver configurato la passphrase di Onboard Key Manager, eseguire manualmente il backup delle informazioni in una posizione sicura all'esterno del sistema di archiviazione. Vedere"Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate" .

Informazioni correlate

- "comandi dell'immagine del cluster"
- "abilitazione esterna del gestore delle chiavi di sicurezza"
- "query chiave del gestore delle chiavi di sicurezza"
- "abilitazione integrata del gestore delle chiavi di sicurezza"

Abilita la gestione delle chiavi integrate per NVE in ONTAP 9.5 e versioni precedenti

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 di gestione delle chiavi esterno (KMIP), 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.
- Configurare l'ambiente MetroCluster prima di configurare Onboard Key Manager.

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 show-key-store`

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

   Node: node1
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK

   Node: node2
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK
   ```

   Scopri di più su `security key-manager show-key-store` nel"Riferimento al comando ONTAP" .

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

   `volume encryption conversion start`

   Configurare Onboard Key Manager prima di convertire i volumi. Negli ambienti MetroCluster , configurarlo su entrambi i siti.

Al termine

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

Quando si configura la passphrase di Onboard Key Manager, eseguire il backup delle informazioni in una posizione sicura all'esterno del sistema di archiviazione in caso di emergenza. Vedere"Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate" .

Informazioni correlate

- "Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate"
- "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"
- "gestore chiavi di sicurezza mostra archivio chiavi"

Abilita la gestione delle chiavi integrate nei nodi ONTAP 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 9.6 e versioni successive, è necessario eseguire `security key-manager onboard sync` comando ogni volta che aggiungi un nodo al cluster.
>
> Per ONTAP 9.5 e versioni precedenti, è necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.
>
> Se si aggiunge un nodo a un cluster con gestione delle chiavi integrata, 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.

  Ulteriori informazioni su `security key-manager onboard enable` e `security key-manager onboard sync` nella "Riferimento al comando ONTAP".

- 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`.

> Se il tentativo di inserimento della passphrase fallisce, riavviare il nodo. Dopo il riavvio, puoi provare a immettere nuovamente la passphrase.

Informazioni correlate

- "comandi dell'immagine del cluster"
- "abilitazione esterna del gestore delle chiavi di sicurezza"
- "abilitazione integrata del gestore delle chiavi di sicurezza"

Crittografare i dati del volume con NVE o NAE

Scopri come crittografare i dati del volume ONTAP con 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.

Abilita la crittografia a livello di aggregato con licenza VE in ONTAP

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

A proposito di questa attività

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

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

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

Prima di iniziare

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

Fasi

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

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

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

Scopri di più su `storage aggregate modify` nel "Riferimento al comando ONTAP" .

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
```

Ulteriori informazioni su `storage aggregate create` nella "Riferimento al comando ONTAP".

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

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

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.
```

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

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 in ONTAP

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.

Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "Riferimento al comando ONTAP".

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

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

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

Fasi

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

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

Ulteriori informazioni su `volume create` nella "Riferimento al comando ONTAP".

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

   `volume show -is-encrypted true`

   Ulteriori informazioni su `volume show` nella "Riferimento al comando ONTAP".

Risultato

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

Abilita NAE o NVE su un volume ONTAP 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

Puoi usare il `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 il comando `volume move start` comando.

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

Puoi usare il `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`

   Ulteriori informazioni su `volume encryption conversion start` nella "Riferimento al comando ONTAP".

   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`

   Ulteriori informazioni su `volume encryption conversion show` nella "Riferimento al comando ONTAP".

   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`

   Ulteriori informazioni su `volume show` nella "Riferimento al comando ONTAP".

   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

Puoi utilizzare `volume move start` il comando per attivare la crittografia spostando un volume esistente. 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`

Ulteriori informazioni su `volume move start` nella "Riferimento al comando ONTAP".

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.

   Ulteriori informazioni su `volume show` nella "Riferimento al comando ONTAP".

   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`

   Ulteriori informazioni su `volume show` nella "Riferimento al comando ONTAP".

   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 NVE su un volume radice ONTAP 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`

   Ulteriori informazioni su `volume move` nella "Riferimento al comando ONTAP".

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

System Manager

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

Configurare NVE su un volume radice del nodo ONTAP

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
```

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.