Configurare NVE

ONTAP 9

NetApp
April 24, 2024

Sommario

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.