Configurare la crittografia basata su hardware NetApp

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/it-it/ontap/encryption-at-rest/support-storage-encryption-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommario

Configurare la crittografia basata su hardware NetApp

Configurazione della panoramica della crittografia basata su hardware NetApp

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

Comprendere la crittografia basata su hardware NetApp

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

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol). Si consiglia di configurare i server di gestione delle chiavi esterni su un sistema storage diverso dai dati.
- Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati.

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

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

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

Tipi di dischi con crittografia automatica supportati

Sono supportati due tipi di dischi con crittografia automatica:

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

firmware del disco per ottenere una chiave di crittografia).

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

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

Quando utilizzare la gestione esterna delle chiavi

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

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

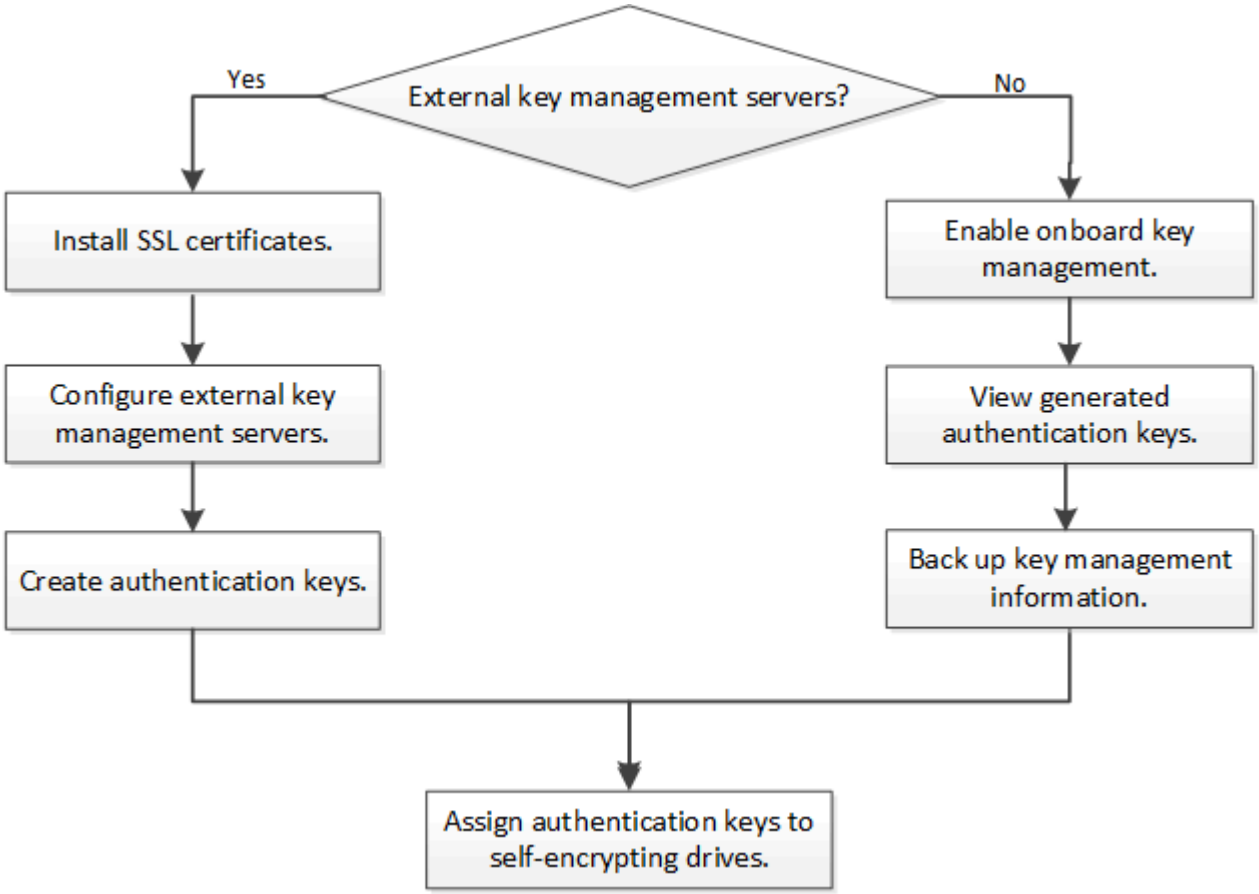
Dettagli del supporto

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

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

Workflow di crittografia basato su hardware

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



Informazioni correlate

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

Configurare la gestione esterna delle chiavi

Configurare una panoramica sulla gestione esterna delle chiavi

È possibile utilizzare uno o più server di gestione delle chiavi esterni per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. Un server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

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

La crittografia dei volumi NetApp (NVE) può essere implementata con Onboard Key Manager in ONTAP 9.1 e versioni successive. In ONTAP 9.3 e versioni successive, NVE può essere implementato con gestione delle chiavi esterna (KMIP) e Gestione delle chiavi integrata. A partire da ONTAP 9.11.1, è possibile configurare più

Key Manager esterni in un cluster. Vedere Configurare i server delle chiavi in cluster.

Raccogliere le informazioni di rete in ONTAP 9.2 e versioni precedenti

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

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

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

Informazioni correlate

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

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

Installare i certificati SSL sul cluster

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

A proposito di questa attività

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

Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.
- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.

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

Fasi

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

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

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

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

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

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

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

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

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

A partire da ONTAP 9.11.1, è possibile aggiungere fino a 3 server di chiavi secondari per ogni server di chiavi primario per creare un server di chiavi in cluster. Per ulteriori informazioni, vedere Configurare i server di chiavi esterne in cluster.

Prima di iniziare

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

Fasi

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

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

   - Il `security key-manager external enable` il comando sostituisce `security key-manager setup` comando. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne. Per la sintassi completa dei comandi, vedere le pagine man.
   - In un ambiente MetroCluster, se si sta configurando la gestione esterna delle chiavi per la SVM amministrativa, è necessario ripetere `security key-manager external enable` sul cluster partner.

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

   ```
   cluster1::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

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

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

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

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

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

6 entries were displayed.
```

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

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

A proposito di questa attività

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

Prima di iniziare

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

Fasi

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

   ```
   security key-manager setup
   ```

   Viene avviata la configurazione di Key Manager.

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

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

```
security key-manager add -address key_management_server_ipaddress
```

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

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

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

```
security key-manager add -address key_management_server_ipaddress
```

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

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

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

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

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

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

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

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

```
volume encryption conversion start
```

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

Configurare i server di chiavi esterne in cluster

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

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

Prima di iniziare

- "La gestione delle chiavi di KMIP deve essere abilitata per la SVM".
- Questo processo supporta solo i server chiave che utilizzano KMIP. Per un elenco dei server delle chiavi supportati, consultare "Tool di matrice di interoperabilità NetApp".
- Tutti i nodi del cluster devono eseguire ONTAP 9.11.1 o versione successiva.
- L'ordine dei server elenca gli argomenti in `-secondary-key-servers` Il parametro riflette l'ordine di accesso dei server KMIP (gestione delle chiavi esterne).

Creare un server di chiavi in cluster

La procedura di configurazione dipende dal fatto che sia stato configurato o meno un server di chiavi primario.

Aggiunta di server di chiavi primari e secondari a una SVM

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

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

1. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole di un massimo di tre server chiave.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Per ulteriori informazioni sui server di chiavi secondari, vedere [mod-secondary].

Modificare i server delle chiavi in cluster

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

Convertire i server chiavi primari e secondari

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

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

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

Modificare i server chiavi secondari

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

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

Per ulteriori informazioni, fare riferimento a. `security key-manager external` nella "Riferimento al comando ONTAP".

Creare chiavi di autenticazione in ONTAP 9.6 e versioni successive

È possibile utilizzare `security key-manager key create` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando Onboard Key Manager è attivato. Tuttavia, quando Onboard Key Manager è attivato, vengono create automaticamente due chiavi di autenticazione. I tasti possono essere visualizzati con il seguente comando:

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

- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.
- È possibile utilizzare `security key-manager key delete` per eliminare le chiavi inutilizzate. Il `security key-manager key delete` Il comando non riesce se la chiave è attualmente in uso da ONTAP. Per utilizzare questo comando, è necessario disporre di privilegi superiori a "admin".

> In un ambiente MetroCluster, prima di eliminare una chiave, è necessario assicurarsi che la chiave non sia in uso nel cluster partner. È possibile utilizzare i seguenti comandi sul cluster partner per verificare che la chiave non sia in uso:
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

Prima di iniziare

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

Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

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

   Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`, che genera automaticamente una passphrase da 32 byte:

   ```
   cluster1::> security key-manager key create
   Key ID:
   000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

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

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

   > Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina man. L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

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

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

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

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

Creare chiavi di autenticazione in ONTAP 9.5 e versioni precedenti

È possibile utilizzare `security key-manager create-key` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.
- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.

È possibile utilizzare il software del server di gestione delle chiavi per eliminare le chiavi inutilizzate, quindi eseguire nuovamente il comando.

Prima di iniziare

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

Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

   `security key-manager create-key`

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

   > L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

   Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

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

   `security key-manager query`

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

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

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

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


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

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

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

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per bloccare o sbloccare i dati crittografati sul disco.

A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

Questa procedura non comporta interruzioni.

Prima di iniziare

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

Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

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

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

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

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

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

```
storage encryption disk show
```

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

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

Configurare la gestione delle chiavi integrata

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

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

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

A proposito di questa attività

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

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

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

Quando Onboard Key Manager è attivato in modalità Common Criteria (Criteri comuni) (`cc-mode-enabled=yes`), il comportamento del sistema viene modificato nei seguenti modi:

- Il sistema monitora i tentativi consecutivi di passphrase del cluster non riusciti quando si opera in modalità Common Criteria.

  Se NetApp Storage Encryption (NSE) è attivato e non si riesce a inserire la passphrase del cluster corretta all'avvio, il sistema non può autenticare i propri dischi e si riavvia automaticamente. Per risolvere il problema, al prompt di boot occorre inserire la passphrase del cluster corretta. Una volta avviato, il sistema consente fino a 5 tentativi consecutivi di inserire correttamente la passphrase del cluster in un periodo di 24 ore per qualsiasi comando che richieda la passphrase del cluster come parametro. Se il limite viene raggiunto (ad esempio, non è stato possibile inserire correttamente la passphrase del cluster 5 volte di seguito), è necessario attendere che il periodo di timeout di 24 ore sia trascorso oppure riavviare il nodo per ripristinare il limite.

- Gli aggiornamenti delle immagini di sistema utilizzano il certificato di firma del codice NetApp RSA-3072 insieme ai digest con firma del codice SHA-384 per controllare l'integrità dell'immagine invece del certificato di firma del codice NetApp RSA-2048 e dei digest con firma del codice SHA-256.

  Il comando upgrade verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida ha esito positivo, il processo di aggiornamento dell'immagine passa alla fase successiva; in caso contrario, l'aggiornamento dell'immagine non riesce. Per informazioni sugli aggiornamenti di sistema, consultare la pagina man "cluster image".

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

Prima di iniziare

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

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

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

Fasi

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

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

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

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

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

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

2. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per "cc-mode", una passphrase compresa tra 64 e 256 caratteri.

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

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

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

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

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

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

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

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

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

Al termine

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

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

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

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

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

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

A proposito di questa attività

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

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

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

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

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

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

Prima di iniziare

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

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

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

Fasi

1. Avviare la configurazione di Key Manager:

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

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

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

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

...

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

2. Invio `yes` quando viene richiesto di configurare la gestione delle chiavi integrata.
3. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per “cc-mode”, una passphrase compresa tra 64 e 256 caratteri.

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

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

   `security key-manager key show`

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

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

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

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

Al termine

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

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

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

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per accedere ai dati sul disco.

A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

Prima di iniziare

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

Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

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

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

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

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

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

   `storage encryption disk show`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

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

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

A proposito di questa attività

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

Questa procedura non comporta interruzioni.

Prima di iniziare

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

Fasi

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

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

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

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

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

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

   `storage encryption disk show -fips`

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

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

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

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

A proposito di questa attività

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

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

Prima di iniziare

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

Fasi

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

   ```
   set -privilege advanced
   ```

2. Verificare che TLSv1.2 sia supportato:

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

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

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

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

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

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

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

   ```
   security config show
   ```

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

Informazioni sul copyright

Copyright © 2024 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.