Fase 6. Completare l'aggiornamento

Upgrade controllers

NetApp
March 11, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap-systems-upgrade/upgrade-arl-manual/manage_authentication_kmip.html on March 11, 2026. Always check docs.netapp.com for the latest.

Sommario

Fase 6. Completare l’aggiornamento . . . 1
Gestire l’autenticazione utilizzando i server KMIP . . . 1
Verificare che i nuovi controller siano impostati correttamente . . . 1
Impostare Storage Encryption sul nuovo modulo controller . . . 4
Impostare NetApp Volume o aggregate Encryption sul nuovo modulo controller . . . 5
Decommissionare il vecchio sistema . . . 6
Riprendere le operazioni di SnapMirror . . . 7

Fase 6. Completare l’aggiornamento

Gestire l’autenticazione utilizzando i server KMIP

Con ONTAP 9.5 e versioni successive, è possibile utilizzare i server KMIP (Key Management Interoperability Protocol) per gestire le chiavi di autenticazione.

Fasi

1. Aggiungere un nuovo controller:

   ```
   security key-manager setup -node new_controller_name
   ```

2. Aggiungere il gestore delle chiavi:

   ```
   security key-manager -add key_management_server_ip_address
   ```

3. Verificare che i server di gestione delle chiavi siano configurati e disponibili per tutti i nodi del cluster:

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

4. Ripristinare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati al nuovo nodo:

   ```
   security key-manager restore -node new_controller_name
   ```

Verificare che i nuovi controller siano impostati correttamente

Per confermare la corretta configurazione, attivare la coppia ha. Inoltre, è possibile verificare che node3 e node4 possano accedere reciprocamente allo storage e che nessuno dei due possieda le LIF dei dati appartenenti ad altri nodi del cluster. Inoltre, confermi che node3 possiede gli aggregati di node1 e che node4 possiede gli aggregati di node2 e che i volumi per entrambi i nodi sono online.

Fasi

1. Abilitare il failover dello storage immettendo il seguente comando su uno dei nodi:

   ```
   storage failover modify -enabled true -node <node3>
   ```

2. Verificare che il failover dello storage sia attivato:

   ```
   storage failover show
   ```

   L’esempio seguente mostra l’output del comando quando è attivato il failover dello storage:

```
cluster::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- ------------------
node3          node4          true     Connected to node4
node4          node3          true     Connected to node3
```

3. Eseguire una delle seguenti operazioni:

Se il cluster è un…	Descrizione
Cluster a due nodi	Abilitare la disponibilità elevata del cluster immettendo il seguente comando su uno dei nodi: `cluster ha modify -configured true`
Cluster con più di due nodi	Passare a. Fase 4.

4. verificare che node3 e node4 appartengano allo stesso cluster immettendo il seguente comando ed esaminando l'output:

   `cluster show`

5. Verificare che node3 e node4 possano accedere reciprocamente allo storage immettendo il seguente comando ed esaminando l'output:

   `storage failover show -fields local-missing-disks,partner-missing-disks`

6. Verificare che né node3 né node4 detengano le LIF dei dati di proprietà di altri nodi del cluster immettendo il seguente comando ed esaminando l'output:

   `network interface show`

   Se il nodo 3 o il nodo 4 possiede le LIF dei dati di proprietà di altri nodi del cluster, utilizzare il `network interface revert` Comando per ripristinare le LIF dei dati al proprietario di casa.

7. Verificare che node3 possieda gli aggregati dal node1 e che node4 possieda gli aggregati dal node2:

   ```
   storage aggregate show -owner-name <node3>
   storage aggregate show -owner-name <node4>
   ```

8. Determinare se i volumi sono offline:

   ```
   volume show -node <node3> -state offline
   volume show -node <node4> -state offline
   ```

9. Se alcuni volumi non sono in linea, confrontarli con l'elenco dei volumi non in linea in cui sono stati acquisiti "Fase 19 (d)" In *preparare i nodi per l'aggiornamento* e portare online qualsiasi volume offline, come richiesto, immettendo il seguente comando, una volta per ogni volume:

   `volume online -vserver <vserver_name> -volume <volume_name>`

10. Installare nuove licenze per i nuovi nodi immettendo il seguente comando per ciascun nodo:

    ```
    system license add -license-code <license_code,license_code,license_code…>
    ```

    Il parametro License-code accetta un elenco di 28 chiavi alfabetiche maiuscole. È possibile aggiungere una licenza alla volta oppure più licenze contemporaneamente, ciascuna chiave di licenza separata da una virgola.

11. se nella configurazione vengono utilizzati dischi con crittografia automatica ed è stato impostato `kmip.init.maxwait` variabile a. `off` (ad esempio, in "Fase 16" Of *Install and boot node3*), devi disimpostare la variabile:

    ```
    set diag; systemshell -node node_name -command sudo kenv -u -p
    kmip.init.maxwait
    ```

12. Per rimuovere tutte le vecchie licenze dai nodi originali, immettere uno dei seguenti comandi:

    ```
    system license clean-up -unused -expired
    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - Per eliminare tutte le licenze scadute, immettere:

      ```
      system license clean-up -expired
      ```

    - Per eliminare tutte le licenze inutilizzate, immettere:

      ```
      system license clean-up -unused
      ```

    - Per eliminare una licenza specifica da un cluster, immettere i seguenti comandi sui nodi:

      ```
      system license delete -serial-number <node1_serial_number> -package *
      system license delete -serial-number <node2_serial_number> -package *
      ```

      Viene visualizzato il seguente output:

    ```
    Warning: The following licenses will be removed:
    <list of each installed package>
    Do you want to continue? {y|n}: y
    ```

    +
    Invio `y` per rimuovere tutti i pacchetti.

13. Verificare che le licenze siano installate correttamente immettendo il seguente comando ed esaminandone l'output:

    ```
    system license show
    ```

    Puoi confrontare l'output con l'output che hai catturato in"Fase 29" di *Preparare i nodi per l'aggiornamento*.

14. Configurare gli SP eseguendo il seguente comando su entrambi i nodi:

```
system service-processor network modify -node <node_name>
```

Vai a "Riferimenti" per collegarti al *System Administration Reference* per informazioni sugli SP e all'*ONTAP 9 Command reference* per informazioni dettagliate sul comando `system service- processor network modify`.

15. Se si desidera configurare un cluster senza switch sui nuovi nodi, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi al *sito di supporto di rete* e seguire le istruzioni in *passaggio a un cluster senza switch a due nodi*.

Al termine

Se Storage Encryption è attivato su node3 e node4, completare la procedura descritta in "Impostare Storage Encryption sul nuovo modulo controller". In caso contrario, completare la procedura descritta in "Decommissionare il vecchio sistema".

Impostare Storage Encryption sul nuovo modulo controller

Se il controller sostituito o il partner ha del nuovo controller utilizza Storage Encryption, è necessario configurare il nuovo modulo controller per Storage Encryption, inclusa l'installazione dei certificati SSL e la configurazione dei server di gestione delle chiavi.

A proposito di questa attività

Questa procedura include i passaggi che vengono eseguiti sul nuovo modulo controller. Immettere il comando sul nodo corretto.

Fasi

1. Verificare che i server di gestione delle chiavi siano ancora disponibili, che il loro stato e le relative informazioni sulla chiave di autenticazione:

   ```
   security key-manager show -status

   security key-manager query
   ```

2. Aggiungere i server di gestione delle chiavi elencati nel passaggio precedente all'elenco dei server di gestione delle chiavi nel nuovo controller.
   a. Aggiungere il server di gestione delle chiavi:

      ```
      security key-manager -add key_management_server_ip_address
      ```

   b. Ripetere il passaggio precedente per ciascun server di gestione delle chiavi elencato.

      È possibile collegare fino a quattro server di gestione delle chiavi.

   c. Verificare che i server di gestione delle chiavi siano stati aggiunti correttamente:

      ```
      security key-manager show
      ```

3. Sul nuovo modulo controller, eseguire la configurazione guidata della gestione delle chiavi per configurare e installare i server di gestione delle chiavi.

   È necessario installare gli stessi server di gestione delle chiavi installati sul modulo controller esistente.

a. Avviare la configurazione guidata del server di gestione delle chiavi sul nuovo nodo:

```
security key-manager setup -node new_controller_name
```

b. Completare la procedura guidata per configurare i server di gestione delle chiavi.

4. Ripristinare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati al nuovo nodo:

```
security key-manager restore -node new_controller_name
```

Impostare NetApp Volume o aggregate Encryption sul nuovo modulo controller

Se il controller sostituito o il partner ad alta disponibilità (ha) del nuovo controller utilizza NetApp Volume Encryption (NVE) o NetApp aggregate Encryption (NAE), è necessario configurare il nuovo modulo controller per NVE o NAE.

A proposito di questa attività

Questa procedura include i passaggi che vengono eseguiti sul nuovo modulo controller. Immettere il comando sul nodo corretto.

Fasi

1. Verificare che i server di gestione delle chiavi siano ancora disponibili, che il loro stato e le relative informazioni sulla chiave di autenticazione:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 o 9.7	`security key-manager key query -node node`
ONTAP 9.5 o versioni precedenti	`security key-manager key show`

2. Aggiungere i server di gestione delle chiavi elencati nel passaggio precedente all'elenco dei server di gestione delle chiavi nel nuovo controller:

a. Aggiungere il server di gestione delle chiavi utilizzando il seguente comando:

```
security key-manager -add key_management_server_ip_address
```

b. Ripetere il passaggio precedente per ciascun server di gestione delle chiavi elencato. È possibile collegare fino a quattro server di gestione delle chiavi.

c. Verificare che i server di gestione delle chiavi siano stati aggiunti correttamente utilizzando il seguente comando:

```
security key-manager show
```

3. Sul nuovo modulo controller, eseguire la configurazione guidata della gestione delle chiavi per configurare e installare i server di gestione delle chiavi.

È necessario installare gli stessi server di gestione delle chiavi installati sul modulo controller esistente.

a. Avviare la configurazione guidata del server di gestione delle chiavi sul nuovo nodo utilizzando il seguente comando:

```
security key-manager setup -node new_controller_name
```

b. Completare la procedura guidata per configurare i server di gestione delle chiavi.

4. Ripristinare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati al nuovo nodo.

   ◦ Ripristinare l'autenticazione per il gestore delle chiavi esterno:

   ```
   security key-manager external restore
   ```

   Questo comando richiede la passphrase di Onboard Key Manager (OKM)

   Per ulteriori informazioni, consultare l'articolo della Knowledge base "Come ripristinare la configurazione del server di gestione delle chiavi esterne dal menu di avvio di ONTAP".

   ◦ Ripristinare l'autenticazione per OKM:

Per questa versione di ONTAP…	Utilizzare questo comando…
Tutte le altre versioni di ONTAP	`security key-manager onboard sync`
ONTAP 9.5	`security key-manager setup -node node_name`

Al termine

Controllare se i volumi sono stati portati offline perché le chiavi di autenticazione non erano disponibili o non è stato possibile raggiungere i server di gestione delle chiavi esterne. Riportare online quei volumi utilizzando `volume online` comando.

Decommissionare il vecchio sistema

Dopo l'aggiornamento, è possibile decommissionare il vecchio sistema tramite il NetApp Support Site. La disattivazione del sistema indica a NetApp che il sistema non è più in funzione e lo rimuove dai database di supporto.

Fasi

1. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* ed effettuare l'accesso.
2. Selezionare **prodotti > prodotti** dal menu.
3. Nella pagina **Visualizza sistemi installati**, scegliere i **criteri di selezione** da utilizzare per visualizzare le informazioni sul sistema.

   È possibile scegliere una delle seguenti opzioni per individuare il sistema:

   ◦ Numero di serie (situato sul retro dell'unità)

   ◦ Numeri di serie per la mia posizione

4. Selezionare **Go!**

   Una tabella visualizza le informazioni sul cluster, inclusi i numeri di serie.

5. Individuare il cluster nella tabella e selezionare **Decommissionare questo sistema** dal menu a discesa Product Tool Set (Set strumenti prodotto).

Riprendere le operazioni di SnapMirror

È possibile riprendere i trasferimenti di SnapMirror che sono stati disattivati prima dell'aggiornamento e riprendere le relazioni di SnapMirror. Gli aggiornamenti sono programmati una volta completato l'aggiornamento.

Fasi

1. Verificare lo stato di SnapMirror sulla destinazione:

   ```
   snapmirror show
   ```

2. Riprendere la relazione di SnapMirror:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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