Fase 7. Completare l'aggiornamento

Upgrade controllers

NetApp
February 22, 2024

Sommario

Fase 7. Completare l'aggiornamento

Panoramica

Durante la fase 7, confermi che i nuovi nodi sono impostati correttamente e, se i nuovi nodi sono abilitati per la crittografia, configuri e configuri Storage Encryption o NetApp Volume Encryption. È inoltre necessario decommissionare i vecchi nodi e riprendere le operazioni di SnapMirror.

Fasi

1. "Gestire l'autenticazione utilizzando i server KMIP"
2. "Verificare che i nuovi controller siano impostati correttamente"
3. "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"

Gestire l'autenticazione utilizzando i server KMIP

A partire da ONTAP 9.10.1, 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 external enable
   ```

2. Aggiungere il gestore delle chiavi:

   ```
   security key-manager external add-servers -key-servers
   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 external show-status
   ```

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

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

Verificare che i nuovi controller siano impostati correttamente

Per confermare la corretta configurazione, verificare che la coppia ha sia attivata. Inoltre, è possibile verificare che node1 e node2 possano accedere reciprocamente allo storage e che nessuno dei due possieda le LIF dei dati appartenenti ad altri nodi del cluster.

Inoltre, è possibile verificare che tutti gli aggregati di dati si trovino sui nodi principali corretti e che i volumi di entrambi i nodi siano online. Se uno dei nuovi nodi dispone di un adattatore di destinazione unificato, è necessario ripristinare le configurazioni delle porte e modificare l'utilizzo dell'adattatore.

Fasi

1. Dopo i controlli post-node2, vengono attivate la coppia di ha cluster e failover dello storage per il cluster node2. Al termine dell'operazione, entrambi i nodi vengono visualizzati come completati e il sistema esegue alcune operazioni di pulizia.
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
   ----------  -----------   ------------  ------------------
   node1       node2         true          Connected to node2
   node2       node1         true          Connected to node1
   ```

3. Verificare che node1 e node2 appartengano allo stesso cluster utilizzando il seguente comando ed esaminando l'output:

   ```
   cluster show
   ```

4. Verificare che node1 e node2 possano accedere reciprocamente allo storage utilizzando il seguente comando ed esaminando l'output:

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

5. Verificare che né node1 né node2 detengano le LIF dei dati di proprietà di altri nodi del cluster utilizzando il seguente comando ed esaminando l'output:

   ```
   network interface show
   ```

   Se nessuno dei nodi 1 o node2 possiede le LIF dei dati di proprietà di altri nodi del cluster, ripristinare le LIF dei dati al proprietario di casa:

   ```
   network interface revert
   ```

6. Verificare che gli aggregati siano di proprietà dei rispettivi nodi principali.

   ```
   storage aggregate show -owner-name node1
   ```

   ```
   storage aggregate show -owner-name node2
   ```

7. Determinare se i volumi sono offline:

```
volume show -node node1 -state offline

volume show -node node2 -state offline
```

8. Se alcuni volumi non sono in linea, confrontarli con l'elenco dei volumi non in linea acquisito nella sezione "Preparare i nodi per l'aggiornamento"e portare online uno qualsiasi dei volumi offline, come richiesto, utilizzando il seguente comando, una volta per ciascun volume:

   ```
   volume online -vserver vserver_name -volume volume_name
   ```

9. Installare nuove licenze per i nuovi nodi utilizzando 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, separando ciascuna chiave di licenza con una virgola.

10. Rimuovere tutte le vecchie licenze dai nodi originali utilizzando uno dei seguenti comandi:

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

    system license delete -serial-number node_serial_number -package
    licensable_package
    ```

    - Eliminare tutte le licenze scadute:

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

    - Eliminare tutte le licenze inutilizzate:

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

    - Eliminare una licenza specifica da un cluster utilizzando 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.

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

    ```
    system license show
    ```

È possibile confrontare l'output con quello acquisito in "Preparare i nodi per l'aggiornamento" sezione.

12. se nella configurazione vengono utilizzate unità con crittografia automatica ed è stato impostato `kmip.init.maxwait` variabile a. `off` (Ad esempio, in *Boot node2 with the replacement system modules*, "Fase 1"), è necessario annullare l'impostazione della variabile:

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

13. Configurare gli SP utilizzando il seguente comando su entrambi i nodi:

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

    Fare riferimento a. "Riferimenti" Per informazioni dettagliate sul sistema, consultare il documento *riferimento amministrazione sistema* e i comandi di *ONTAP 9: Riferimento pagina manuale* `service-processor network modify` comando.

14. Se si desidera configurare un cluster senza switch sui nuovi nodi, fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e seguire le istruzioni in *passaggio a un cluster senza switch a due nodi*.

Al termine

Se Storage Encryption è attivato su node1 e node2, completare la sezione "Impostare Storage Encryption sul nuovo modulo controller". In caso contrario, completare la sezione "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 external show-status

   security key-manager onboard show-backup
   ```

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 external add-servers -key-servers
      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 external 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 external enable
   ```

   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 external 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.

Gestione delle chiavi integrata

Configurare NVE o NAE utilizzando Onboard Key Manager.

Fasi

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

   ```
   security key-manager onboard sync
   ```

Gestione esterna delle chiavi

Configurare NVE o NAE utilizzando External Key Management.

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 key query -node node
   ```

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 external add-servers -key-servers
      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 external 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 external enable
      ```

   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 external restore
   ```

   Questo comando richiede la passphrase 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".

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 EKM. Ripristinare i volumi online utilizzando `volume online` comando.

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 i volumi online 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
   ```