Supporto di avvio - ripristino manuale

Install and maintain

NetApp
February 13, 2026

Sommario

Supporto di avvio - ripristino manuale

Flusso di lavoro per il ripristino manuale dei supporti di avvio - AFF A70 e AFF A90

Il ripristino manuale dell'immagine di avvio prevede l'utilizzo di un'unità USB per reinstallare ONTAP sul supporto di avvio sostitutivo del sistema AFF A70 o AFF A90 . È necessario scaricare l'immagine di ripristino ONTAP appropriata dal sito di supporto NetApp e copiarla su un'unità USB. Questa unità USB preparata viene quindi utilizzata per eseguire il ripristino e ripristinare il sistema allo stato operativo.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare"procedura di ripristino automatico dell'avvio" . Se il sistema esegue una versione precedente di ONTAP, utilizzare la procedura di ripristino manuale all'avvio.

Per iniziare, rivedere i requisiti di ripristino, spegnere il controller, sostituire il supporto di avvio, utilizzare l'unità USB per ripristinare l'immagine e riapplicare le impostazioni di crittografia, se necessario.

"Esaminare i requisiti per sostituire il supporto di avvio"

Esaminare i requisiti per la sostituzione dei supporti di avvio.

"Controllare il supporto e lo stato della chiave di crittografia"

Determinare se il sistema dispone di un gestore delle chiavi di sicurezza abilitato o di dischi crittografati.

"Spegnere il controller"

Spegnere il controller quando è necessario sostituire il supporto di avvio.

"Sostituire il supporto di avvio"

Rimuovere il supporto di avvio non riuscito dal modulo di gestione del sistema e installare il supporto di avvio sostitutivo, quindi trasferire un'immagine ONTAP utilizzando un'unità flash USB.

"Avviare l'immagine di ripristino"

Avviare l'immagine ONTAP dall'unità USB, ripristinare il file system e verificare le variabili ambientali.

"Ripristino della crittografia"

Ripristinare la configurazione del gestore chiavi integrato o del gestore chiavi esterno dal menu di avvio ONTAP .

7 **"Restituire la parte guasta a NetApp"**

Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Requisiti per il ripristino manuale dei supporti di avvio - AFF A70 e AFF A90

Prima di sostituire il supporto di avvio nel sistema AFF A70 o AFF A90, assicurarsi di soddisfare i requisiti necessari per una sostituzione corretta. È necessario assicurarsi di disporre di un'unità flash USB con la quantità di spazio di archiviazione appropriata e verificare di disporre della periferica di avvio sostitutiva corretta.

Se il sistema è in esecuzione in ONTAP 9.17.1 e versioni successive, utilizzare "procedura di ripristino automatico dell'avvio" .

Chiavetta USB

- Assicurati di avere una chiavetta USB formattata in FAT32.
- La chiavetta USB deve avere una capacità di archiviazione sufficiente per contenere il `image_xxx.tgz` file.

Preparazione del file

Copia il `image_xxx.tgz` file sull'unità flash USB. Questo file verrà utilizzato quando si trasferisce l'immagine ONTAP tramite l'unità flash USB.

Sostituzione dei componenti

Sostituire il componente guasto con il componente sostitutivo fornito da NetApp.

Identificazione del controllore

Quando si sostituisce il supporto di avvio danneggiato, è fondamentale applicare i comandi al controller corretto:

- Il *controller non funzionante* è il controller su cui si sta eseguendo la manutenzione.
- Il *controllore sano* è il partner HA del controllore compromesso.

Quali sono le prossime novità?

Dopo aver esaminato i requisiti per sostituire il supporto di avvio, è necessario "controllare il supporto e lo stato della chiave di crittografia sul supporto di avvio".

Controllare il supporto di crittografia per il ripristino manuale dei supporti di avvio - AFF A70 e AFF A90

Per garantire la sicurezza dei dati sul sistema di storage AFF A70 o AFF A90, è necessario verificare il supporto e lo stato della chiave di crittografia sul supporto di avvio. Verifica se la versione di ONTAP supporta la crittografia dei volumi di NetApp (NVE) e prima di arrestare il controller verifica se il gestore delle chiavi è attivo.

Se il sistema è in esecuzione in ONTAP 9.17.1 e versioni successive, utilizzare "procedura di ripristino

automatico dell'avvio" .

Passaggio 1: verificare il supporto NVE e scaricare l'immagine ONTAP corretta

Determina se la tua versione ONTAP supporta NetApp Volume Encryption (NVE), in modo da poter scaricare l'immagine ONTAP corretta per la sostituzione del supporto di avvio.

Fasi

1. Controlla se la tua versione ONTAP supporta la crittografia:

   `version -v`

   Se l'output include `1Ono-DARE`, NVE non è supportato nella versione del cluster.

2. Scarica l'immagine ONTAP appropriata in base al supporto NVE:
   - Se NVE è supportato: scaricare l'immagine ONTAP con NetApp Volume Encryption
   - Se NVE non è supportato: scaricare l'immagine ONTAP senza NetApp Volume Encryption

   Scarica l'immagine ONTAP dal sito di supporto NetApp sul tuo server HTTP o FTP o in una cartella locale. Questo file immagine sarà necessario durante la procedura di sostituzione del supporto di avvio.

Passaggio 2: verificare lo stato del gestore delle chiavi ed eseguire il backup della configurazione

Prima di spegnere il controller danneggiato, verificare la configurazione del gestore delle chiavi ed eseguire il backup delle informazioni necessarie.

Fasi

1. Determinare quale gestore delle chiavi è abilitato sul proprio sistema:

Versione di ONTAP	Eseguire questo comando
ONTAP 9.14.1 o versione successiva	`security key-manager keystore show` • Se EKM è attivato, `EKM` viene elencato nell'output del comando. • Se OKM è attivato, `OKM` viene elencato nell'output del comando. • Se nessun gestore di chiavi è attivato, `No key manager keystores configured` viene elencato nell'output del comando.

Versione di ONTAP	Eseguire questo comando
ONTAP 9.13.1 o versioni precedenti	`security key-manager show-key-store` • Se EKM è attivato, `external` viene elencato nell'output del comando. • Se OKM è attivato, `onboard` viene elencato nell'output del comando. • Se nessun gestore di chiavi è attivato, `No key managers configured` viene elencato nell'output del comando.

2. A seconda che sul sistema sia configurato un gestore delle chiavi, procedere in uno dei seguenti modi:

   Se non è configurato alcun gestore chiavi:

   È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

   Se è configurato un gestore delle chiavi (EKM o OKM):

   a. Immettere il seguente comando di query per visualizzare lo stato delle chiavi di autenticazione nel gestore delle chiavi:

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

   b. Rivedere l'output e controllare il valore nel `Restored` colonna. Questa colonna indica se le chiavi di autenticazione per il gestore delle chiavi (EKM o OKM) sono state ripristinate correttamente.

3. Completare la procedura appropriata in base al tipo di responsabile delle chiavi:

Gestore chiavi esterno (EKM)

Completare questi passaggi in base al valore nel `Restored` colonna.

Se vengono visualizzate tutte le chiavi `true` nella colonna Ripristinato:

È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Se una qualsiasi delle chiavi mostra un valore diverso da `true` nella colonna Ripristinato:

a. Ripristinare le chiavi di autenticazione della gestione delle chiavi esterne su tutti i nodi del cluster:

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

   Se il comando non riesce, contattare l'assistenza NetApp .

b. Verificare che tutte le chiavi di autenticazione siano state ripristinate:

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

   Confermare che il `Restored` display a colonna `true` per tutte le chiavi di autenticazione.

c. Se tutte le chiavi vengono ripristinate, è possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Onboard Key Manager (OKM)

Completare questi passaggi in base al valore nel `Restored` colonna.

Se vengono visualizzate tutte le chiavi `true` nella colonna Ripristinato:

a. Eseguire il backup delle informazioni OKM:

   i. Passa alla modalità privilegio avanzata:

      ```
      set -priv advanced
      ```

   Entra `y` quando ti viene chiesto di continuare.

   i. Visualizza le informazioni di backup della gestione delle chiavi:

      ```
      security key-manager onboard show-backup
      ```

   ii. Copiare le informazioni di backup in un file separato o nel file di registro.

      Queste informazioni di backup saranno necessarie se sarà necessario ripristinare manualmente OKM durante la procedura di sostituzione.

   iii. Torna alla modalità amministratore:

      ```
      set -priv admin
      ```

b. È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Se una qualsiasi delle chiavi mostra un valore diverso da `true` nella colonna Ripristinato:

a. Sincronizzare il gestore delle chiavi integrato:

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

Quando richiesto, immettere la passphrase alfanumerica di 32 caratteri per la gestione delle chiavi integrate.

> Questa è la passphrase per l'intero cluster creata durante la configurazione iniziale di Onboard Key Manager. Se non si dispone di questa passphrase, contattare l'assistenza NetApp .

b. Verificare che tutte le chiavi di autenticazione siano state ripristinate:

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

Confermare che il `Restored` display a colonna `true` per tutte le chiavi di autenticazione e `Key Manager` tipo spettacoli `onboard` .

c. Eseguire il backup delle informazioni OKM:

i. Passa alla modalità privilegio avanzata:

```
set -priv advanced
```

Entra `y` quando ti viene chiesto di continuare.

i. Visualizza le informazioni di backup della gestione delle chiavi:

```
security key-manager onboard show-backup
```

ii. Copiare le informazioni di backup in un file separato o nel file di registro.

Queste informazioni di backup saranno necessarie se sarà necessario ripristinare manualmente OKM durante la procedura di sostituzione.

iii. Torna alla modalità amministratore:

```
set -priv admin
```

d. È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Quali sono le prossime novità?

Dopo aver verificato il supporto e lo stato della chiave di crittografia sul supporto di avvio, è necessario "spegnere il controller".

Arrestare il controller per il ripristino manuale del supporto di avvio - AFF A70 e AFF A90

Arrestare il controller danneggiato nel sistema di archiviazione AFF A70 o AFF A90 per evitare la perdita di dati e mantenere la stabilità del sistema durante il processo di ripristino automatico del supporto di avvio.

Opzione 1: La maggior parte dei sistemi

Per spegnere il controller compromesso, è necessario determinare lo stato del controller e, se necessario, assumere il controllo del controller in modo che il controller integro continui a servire i dati provenienti dallo storage del controller compromesso.

A proposito di questa attività

- Se si dispone di un sistema SAN, è necessario aver controllato i messaggi di evento `cluster kernel-service show`) per il blade SCSI del controller danneggiato. Il `cluster kernel-service show` comando (dalla modalità avanzata precedente) visualizza il nome del nodo, "stato quorum" di quel nodo, lo stato di disponibilità di quel nodo e lo stato operativo di quel nodo.

  Ogni processo SCSI-blade deve essere in quorum con gli altri nodi del cluster. Eventuali problemi devono essere risolti prima di procedere con la sostituzione.

- Se si dispone di un cluster con più di due nodi, questo deve trovarsi in quorum. Se il cluster non è in quorum o un controller integro mostra false per idoneità e salute, è necessario correggere il problema prima di spegnere il controller compromesso; vedere "Sincronizzare un nodo con il cluster".

Fasi

1. Se AutoSupport è attivato, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=<# of hours>h`

   Il seguente messaggio AutoSupport elimina la creazione automatica del caso per due ore:

   ```
   cluster1:> system node autosupport invoke -node * -type all -message
   MAINT=2h
   ```

2. Disattiva la restituzione automatica:
   a. Immettere il seguente comando dalla console del controller funzionante:

      `storage failover modify -node impaired_node_name -auto-giveback false`

   b. Entra `y` quando vedi il messaggio *Vuoi disattivare la restituzione automatica?*
3. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza…	Quindi…
Il prompt DEL CARICATORE	Passare alla fase successiva.
In attesa di un giveback…	Premere Ctrl-C, quindi rispondere `y` quando richiesto.

Se il controller non utilizzato visualizza…	Quindi…
Prompt di sistema o prompt della password	Assumere il controllo o arrestare il controller compromesso dal controller integro: `storage failover takeover -ofnode impaired_node_name -halt true` Il parametro *-halt true* consente di visualizzare il prompt di Loader.

Opzione 2: Controller in un MetroCluster

Per spegnere il controller compromesso, è necessario determinare lo stato del controller e, se necessario, assumere il controllo del controller in modo che il controller integro continui a servire i dati provenienti dallo storage del controller compromesso.

- Se si dispone di un cluster con più di due nodi, questo deve trovarsi in quorum. Se il cluster non è in quorum o un controller integro mostra false per idoneità e salute, è necessario correggere il problema prima di spegnere il controller compromesso; vedere "Sincronizzare un nodo con il cluster".
- È necessario aver confermato che lo stato di configurazione MetroCluster è configurato e che i nodi sono in uno stato abilitato e normale:

  `metrocluster node show`

Fasi

1. Se AutoSupport è attivato, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   Il seguente messaggio AutoSupport elimina la creazione automatica del caso per due ore:

   ```
   cluster1:*> system node autosupport invoke -node * -type all -message
   MAINT=2h
   ```

2. Disattiva la restituzione automatica:
   a. Immettere il seguente comando dalla console del controller funzionante:

      `storage failover modify -node local -auto-giveback false`

   b. Entra `y` quando vedi il messaggio *Vuoi disattivare la restituzione automatica?*
3. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza…	Quindi…
Il prompt DEL CARICATORE	Passare alla sezione successiva.

Se il controller non utilizzato visualizza…	Quindi…
In attesa di un giveback…	Premere Ctrl-C, quindi rispondere `y` quando richiesto.
Prompt di sistema o prompt della password (inserire la password di sistema)	Assumere il controllo o arrestare il controller compromesso dal controller integro: `storage failover takeover -ofnode` *`impaired_node_name`* `-halt` *`true`* Il parametro *-halt true* consente di visualizzare il prompt di Loader.

Quali sono le prossime novità?

Dopo aver spento il controller, è necessario "sostituire il supporto di avvio".

Sostituisci il supporto di avvio e preparati per il ripristino manuale dell'avvio - AFF A70 e AFF A90

Il supporto di avvio del sistema AFF A70 o AFF A90 memorizza i dati essenziali del firmware e della configurazione. La procedura di sostituzione prevede la rimozione del modulo di gestione del sistema, la rimozione del supporto di avvio danneggiato, l'installazione del supporto di avvio sostitutivo e il trasferimento manuale dell'immagine ONTAP sul supporto di avvio sostitutivo tramite un'unità flash USB.

Fase 1: Sostituire il supporto di avvio

Il supporto di avvio si trova all'interno del modulo di gestione del sistema ed è accessibile rimuovendo il modulo dal sistema.

Fasi

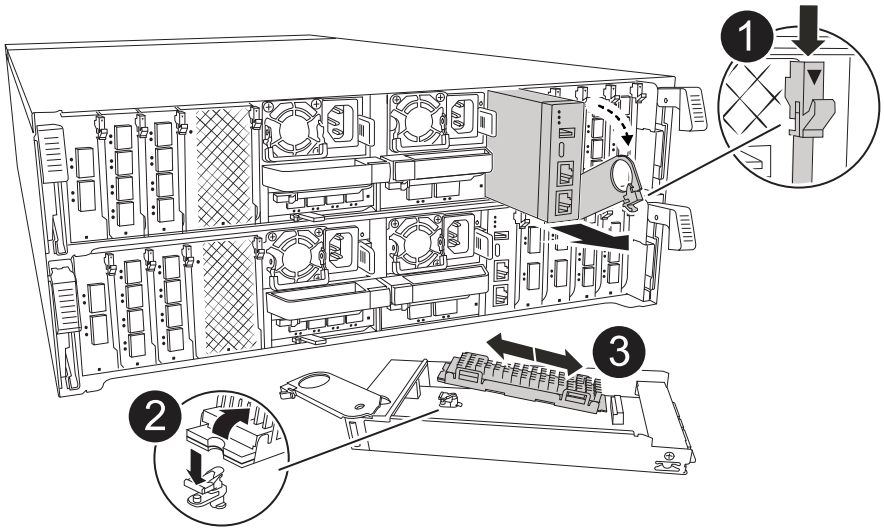
1. Andare sul retro del telaio. Se non si è già collegati a terra, mettere a terra l'utente.
2. Scollegare gli alimentatori del controller.

> Se il sistema è alimentato a corrente continua, scollegare il blocco di alimentazione dalle PSU.

   a. Rimuovere tutti i cavi collegati al modulo di gestione del sistema. Assicurarsi di etichettare il punto in cui sono stati collegati i cavi, in modo da poterli collegare alle porte corrette quando si reinstalla il modulo.
   b. Ruotare il vassoio di gestione dei cavi verso il basso tirando i pulsanti su entrambi i lati all'interno del vassoio di gestione dei cavi, quindi ruotare il vassoio verso il basso.
   c. Premere il pulsante della camma di gestione del sistema. La leva della camma si allontana dal telaio.
   d. Ruotare la leva della camma completamente verso il basso e rimuovere il modulo di gestione del sistema dal modulo controller.

e. Posizionare il modulo di gestione del sistema su un tappetino antistatico, in modo che il supporto di avvio sia accessibile.

3. Rimuovere il supporto di avvio dal modulo di gestione:



1	Dispositivo di chiusura della camma del modulo di gestione del sistema
2	Pulsante di blocco dei supporti di avvio
3	Supporto di boot

a. Premere il pulsante di bloccaggio blu.

b. Ruotare il supporto di avvio verso l'alto, farlo scorrere fuori dallo zoccolo e metterlo da parte.

4. Installare il supporto di avvio sostitutivo nel modulo di gestione del sistema:

a. Allineare i bordi del supporto di avvio con l'alloggiamento dello zoccolo, quindi spingerlo delicatamente a squadra nello zoccolo.

b. Ruotare il supporto di avvio verso il basso verso il pulsante di bloccaggio.

c. Premere il pulsante di bloccaggio, ruotare completamente il supporto di avvio e rilasciare il pulsante di bloccaggio.

5. Reinstallare il modulo di gestione del sistema:

a. Ruotare il vassoio di gestione dei cavi verso l'alto fino alla posizione di chiusura.

b. Eseguire il richiamo del modulo Gestione del sistema.

Fase 2: Trasferire l'immagine di avvio sul supporto di avvio

Il supporto di avvio sostitutivo installato non è dotato di un'immagine ONTAP. È possibile trasferire l'immagine ONTAP sul supporto di avvio sostitutivo scaricando l'immagine di servizio ONTAP appropriata da "Sito di supporto NetApp" a un'unità flash USB e quindi al supporto di avvio sostitutivo.

Prima di iniziare

- È necessario disporre di un'unità flash USB, formattata con FAT32, con almeno 4 GB di capacità.

- Scaricare una copia della stessa versione dell'immagine di ONTAP del controller danneggiato in esecuzione. Puoi scaricare l'immagine appropriata dalla sezione Downloads del sito di supporto NetApp. USA il `version -v` comando per visualizzare se la tua versione di ONTAP supporta NVE. Se viene visualizzato il comando output `<10no- DARE>` , la versione di ONTAP non supporta NVE.
  - Se NVE è supportato dalla tua versione di ONTAP, scarica l'immagine con crittografia dei volumi di NetApp, come indicato nel pulsante di download.
  - Se NVE non è supportato, scaricare l'immagine senza crittografia dei volumi di NetApp, come indicato nel pulsante di download.
- Se il sistema è una coppia ha, è necessario disporre di una connessione di rete tra le porte di gestione dei nodi dei controller (in genere le interfacce e0M).

Fasi

1. Scaricare e copiare l'immagine di servizio appropriata da "Sito di supporto NetApp" nell'unità flash USB.

   a. Scaricare l'immagine del servizio dal collegamento Download nella pagina, nello spazio di lavoro del computer portatile.

   b. Decomprimere l'immagine del servizio.

   > Se si stanno estraendo i contenuti utilizzando Windows, non utilizzare WinZip per estrarre l'immagine netboot. Utilizzare un altro strumento di estrazione, ad esempio 7-zip o WinRAR.

   L'unità flash USB dovrebbe avere l'immagine ONTAP appropriata di ciò che il controller danneggiato è in esecuzione.

   a. Rimuovere l'unità flash USB dal computer portatile.

2. Inserire l'unità flash USB nella porta USB-A del modulo di gestione del sistema.

   Assicurarsi di installare l'unità flash USB nello slot contrassegnato per i dispositivi USB e non nella porta della console USB.

3. Collegare i cavi di alimentazione agli alimentatori. Il controller si riavvia non appena viene ripristinata l'alimentazione.

   > Se si dispone di alimentatori CC, ricollegare il blocco di alimentazione agli alimentatori.

4. Interrompere il processo di avvio premendo Ctrl-C per interrompere il PROCESSO al prompt DEL CARICATORE.

   Se non viene visualizzato questo messaggio, premere Ctrl-C, selezionare l'opzione per avviare la modalità di manutenzione, quindi arrestare il controller per avviare IL CARICATORE.

Quali sono le prossime novità?

Dopo aver sostituito il supporto di avvio, è necessario "avviare l'immagine di ripristino".

Ripristino manuale del supporto di avvio da un'unità USB - AFF A70 e AFF A90

Dopo aver installato il nuovo dispositivo di supporto di avvio nel sistema AFF A70 o AFF

A90 , è possibile avviare manualmente l'immagine di ripristino da un'unità USB per ripristinare la configurazione dal nodo partner.

Se il sistema è in esecuzione in ONTAP 9.17.1 e versioni successive, utilizzare "procedura di ripristino automatico dell'avvio" .

Prima di iniziare

- Assicurati che la tua console sia collegata al controller non compatibile.
- Verifica di avere un'unità flash USB con l'immagine di ripristino.
- Determina se il tuo sistema utilizza la crittografia. Sarà necessario selezionare l'opzione appropriata nel passaggio 3 a seconda che la crittografia sia abilitata o meno.

Fasi

1. Dal prompt LOADER sul controller danneggiato, avviare l'immagine di ripristino dall'unità flash USB:

   ```
   boot_recovery
   ```

   L'immagine di ripristino viene scaricata dall'unità flash USB.

2. Quando richiesto, immettere il nome dell'immagine o premere **Invio** per accettare l'immagine predefinita visualizzata tra parentesi.
3. Ripristinare il file system var utilizzando la procedura per la versione ONTAP in uso:

ONTAP 9.16.0 o versioni precedenti

Completare i seguenti passaggi sul controller non funzionante e sul controller partner:

a. **Sul controller non compatibile:** Premere `Y` quando vedi `Do you want to restore the backup configuration now?`

b. **Sul controller non compatibile:** Se richiesto, premere `Y` per sovrascrivere */etc/ssh/ssh_host_ecdsa_key*.

c. **Sul controller partner:** Imposta il controller non autorizzato al livello di privilegio avanzato:

```
set -privilege advanced
```

d. **Sul controller partner:** eseguire il comando di ripristino del backup:

```
system node restore-backup -node local -target-address impaired_node_IP_address
```

> Se viene visualizzato un messaggio diverso da quello di ripristino riuscito, contattare l'assistenza NetApp .

e. **Sul controller partner:** Torna al livello amministratore:

```
set -privilege admin
```

f. **Sul controller non compatibile:** Premere `Y` quando vedi `Was the restore backup procedure successful?`

g. **Sul controller non compatibile:** Premere `Y` quando vedi `...would you like to use this restored copy now?`

h. **Sul controller non compatibile:** Premere `Y` quando viene richiesto di riavviare, quindi premere `Ctrl-C` quando vedi il menu di avvio.

i. **Sul controller con disabilità:** Eseguire una delle seguenti operazioni:

- Se il sistema non utilizza la crittografia, selezionare *Opzione 1 Avvio normale* dal menu di avvio.
- Se il sistema utilizza la crittografia, vai a"Ripristino della crittografia" .

ONTAP 9.16.1 o successivo

Completare i seguenti passaggi sul controller non funzionante:

a. Premere `Y` quando viene richiesto di ripristinare la configurazione di backup.

   Una volta completata correttamente la procedura di ripristino, viene visualizzato il seguente messaggio: `syncflash_partner: Restore from partner complete`

b. Premere `Y` quando viene richiesto di confermare che il backup di ripristino è stato eseguito correttamente.

c. Premere `Y` quando viene richiesto di utilizzare la configurazione ripristinata.

d. Premere `Y` quando viene richiesto di riavviare il nodo.

e. Premere `Y` quando viene richiesto di riavviare nuovamente, quindi premere `Ctrl-C` quando vedi il menu di avvio.

f. Effettuare una delle seguenti operazioni:

- Se il sistema non utilizza la crittografia, selezionare *Opzione 1 Avvio normale* dal menu di avvio.
- Se il sistema utilizza la crittografia, vai a"Ripristino della crittografia" .

4. Collegare il cavo della console al controller partner.
5. Riportare il controller al funzionamento normale restituendo lo storage:

```
storage failover giveback -fromnode local
```

6. Se hai disattivato la restituzione automatica, riattivala:

```
storage failover modify -node local -auto-giveback true
```

7. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Quali sono le prossime novità?

Dopo aver avviato l'immagine di ripristino, è necessario "ripristinare la crittografia sul supporto di avvio".

Ripristinare le chiavi di crittografia dopo il ripristino manuale dell'avvio - AFF A70 e AFF A90

Ripristinare la crittografia sul supporto di avvio sostitutivo nel sistema AFF A70 o AFF A90 per garantire una protezione continua dei dati. Il processo di sostituzione prevede la verifica della disponibilità delle chiavi, la riapplicazione delle impostazioni di crittografia e la conferma dell'accesso sicuro ai dati.

Se il sistema è in esecuzione in ONTAP 9.17.1 e versioni successive, utilizzare "procedura di ripristino automatico dell'avvio" .

Completare i passaggi appropriati per ripristinare la crittografia sul sistema in base al tipo di gestore delle chiavi. Se non sei sicuro del gestore chiavi utilizzato dal tuo sistema, controlla le impostazioni acquisite all'inizio della procedura di sostituzione del supporto di avvio.

Onboard Key Manager (OKM)

Ripristinare la configurazione di Onboard Key Manager (OKM) dal menu di avvio di ONTAP.

Prima di iniziare

Assicurati di avere a disposizione le seguenti informazioni:

- Passphrase a livello di cluster inserita durante "abilitazione della gestione delle chiavi di bordo"
- "Informazioni di backup per il Key Manager integrato"
- Verifica di avere la passphrase corretta e i dati di backup utilizzando "Come verificare il backup della gestione delle chiavi integrata e la passphrase a livello del cluster" procedura

Fasi

Sul controller non autorizzato:

1. Collegare il cavo della console al controller non funzionante.
2. Dal menu di avvio ONTAP , selezionare l'opzione appropriata:

Versione di ONTAP	Selezionare questa opzione

ONTAP 9.8 o versione successiva	Selezionare l'opzione 10.
	
	Mostra un esempio di menu di avvio
	
	`Please choose one of the following:`
	
	`(1) Normal Boot.`
	`(2) Boot without /etc/rc.`
	`(3) Change password.`
	`(4) Clean configuration and initialize all disks.`
	`(5) Maintenance mode boot.`
	`(6) Update flash from backup config.`
	`(7) Install new software first.`
	`(8) Reboot node.`
	`(9) Configure Advanced Drive Partitioning.`
	`(10) Set Onboard Key Manager recovery secrets.`
	`(11) Configure node for external key management.`
	`Selection (1-11)? 10`

Versione di ONTAP	Selezionare questa opzione
ONTAP 9.7 e versioni precedenti	Selezionare l'opzione nascosta `recover_onboard_keymanager` **Mostra un esempio di menu di avvio** ``` Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager ```

3. Quando richiesto, conferma di voler continuare il processo di ripristino:

   Mostra prompt di esempio

   ```
   This option must be used only in disaster recovery procedures. Are you
   sure? (y or n):
   ```

4. Inserire due volte la passphrase a livello di cluster.

   Durante l'inserimento della passphrase, la console non mostra alcun input.

   Mostra prompt di esempio

   ```
   Enter the passphrase for onboard key management:

   Enter the passphrase again to confirm:
   ```

5. Inserisci le informazioni di backup:

   a. Incollare l'intero contenuto dalla riga BEGIN BACKUP alla riga END BACKUP, inclusi i trattini.

Mostra prompt di esempio

```
Enter the backup data:

--------------------------BEGIN
BACKUP--------------------------
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
34567890123456789012345678901234567890123456789012345678901234
56
45678901234567890123456789012345678901234567890123456789012345
67
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA

---------------------------END
BACKUP---------------------------
```

b. Premere Invio due volte alla fine dell'input.

   Il processo di ripristino viene completato e viene visualizzato il seguente messaggio:

   ```
   Successfully recovered keymanager secrets.
   ```

Mostra prompt di esempio

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*******************************************************************
******************
* Select option "(1) Normal Boot." to complete recovery process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*******************************************************************
******************
```

+

> Non procedere se l'output visualizzato è diverso da `Successfully recovered keymanager secrets` . Eseguire la risoluzione dei problemi per correggere l'errore.

6. Seleziona l'opzione `1` dal menu di avvio per continuare l'avvio in ONTAP.

Mostra prompt di esempio

```
**********************************************************************
******************
* Select option "(1) Normal Boot." to complete the recovery
process.
*
**********************************************************************
******************


(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

7. Verificare che la console del controller visualizzi il seguente messaggio:

   `Waiting for giveback…(Press Ctrl-C to abort wait)`

   Sul controller del partner:

8. Restituire il controller non funzionante:

   `storage failover giveback -fromnode local -only-cfo-aggregates true`

   Sul controller non autorizzato:

9. Dopo aver avviato solo con l'aggregato CFO, sincronizzare il gestore delle chiavi:

   `security key-manager onboard sync`

10. Quando richiesto, immettere la passphrase dell'intero cluster per Onboard Key Manager.

Mostra prompt di esempio

```
Enter the cluster-wide passphrase for the Onboard Key Manager:

All offline encrypted volumes will be brought online and the
corresponding volume encryption keys (VEKs) will be restored
automatically within 10 minutes. If any offline encrypted
volumes are not brought online automatically, they can be
brought online manually using the "volume online -vserver
<vserver> -volume <volume_name>" command.
```

Se la sincronizzazione ha esito positivo, viene restituito il prompt del cluster senza messaggi aggiuntivi. Se la sincronizzazione fallisce, viene visualizzato un messaggio di errore prima di tornare al prompt del cluster. Non continuare finché l'errore non sarà stato corretto e la sincronizzazione non sarà stata eseguita correttamente.

11. Verificare che tutte le chiavi siano sincronizzate:

    ```
    security key-manager key query -restored false
    ```

    Il comando non dovrebbe restituire alcun risultato. Se vengono visualizzati dei risultati, ripetere il comando sync finché non vengono restituiti più risultati.

    Sul controller del partner:

12. Restituire il controller non funzionante:

    ```
    storage failover giveback -fromnode local
    ```

13. Ripristinare lo sconto automatico se è stato disattivato:

    ```
    storage failover modify -node local -auto-giveback true
    ```

14. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi:

    ```
    system node autosupport invoke -node * -type all -message MAINT=END
    ```

Gestore chiavi esterno (EKM)

Ripristinare la configurazione del gestore chiavi esterno dal menu di avvio di ONTAP.

Prima di iniziare

Raccogli i seguenti file da un altro nodo del cluster o dal tuo backup:

- `/cfcard/kmip/servers.cfg`file o l'indirizzo e la porta del server KMIP
- `/cfcard/kmip/certs/client.crt`file (certificato client)
- `/cfcard/kmip/certs/client.key`file (chiave client)
- `/cfcard/kmip/certs/CA.pem`file (certificati CA del server KMIP)

Fasi

Sul controller non autorizzato:

1. Collegare il cavo della console al controller non funzionante.
2. Seleziona l'opzione `11` dal menu di avvio di ONTAP .

   Mostra un esempio di menu di avvio

   ```
   (1)  Normal Boot.
   (2)  Boot without /etc/rc.
   (3)  Change password.
   (4)  Clean configuration and initialize all disks.
   (5)  Maintenance mode boot.
   (6)  Update flash from backup config.
   (7)  Install new software first.
   (8)  Reboot node.
   (9)  Configure Advanced Drive Partitioning.
   (10) Set Onboard Key Manager recovery secrets.
   (11) Configure node for external key management.
   Selection (1-11)? 11
   ```

3. Quando richiesto, conferma di aver raccolto le informazioni richieste:

   Mostra prompt di esempio

   ```
   Do you have a copy of the /cfcard/kmip/certs/client.crt file?
   {y/n}
   Do you have a copy of the /cfcard/kmip/certs/client.key file?
   {y/n}
   Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
   Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
   ```

4. Quando richiesto, immettere le informazioni sul client e sul server:

   a. Immettere il contenuto del file del certificato client (client.crt), comprese le righe BEGIN e END.
   b. Immettere il contenuto del file della chiave client (client.key), comprese le righe BEGIN e END.
   c. Immettere il contenuto del file CA(s) del server KMIP (CA.pem), comprese le righe BEGIN e END.
   d. Immettere l'indirizzo IP del server KMIP.
   e. Immettere la porta del server KMIP (premere Invio per utilizzare la porta predefinita 5696).

Mostra esempio

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

Il processo di ripristino viene completato e viene visualizzato il seguente messaggio:

```
Successfully recovered keymanager secrets.
```

Mostra esempio

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Seleziona l'opzione `1` dal menu di avvio per continuare l'avvio in ONTAP.

Mostra prompt di esempio

```
*****************************************************************
***********
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****************************************************************
***********

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

6. Ripristinare lo sconto automatico se è stato disattivato:

   ```
   storage failover modify -node local -auto-giveback true
   ```

7. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

Quali sono le prossime novità?

Dopo aver ripristinato la crittografia sul supporto di avvio, è necessario "Restituire la parte guasta a NetApp".

Restituire il componente guasto a NetApp - AFF A70 e AFF A90

Se un componente del sistema di storage AFF A70 o AFF A90 si guasta, restituire la parte guasta a NetApp. Vedere "Restituzione e sostituzione delle parti" pagina per ulteriori informazioni.

Informazioni sul copyright

Informazioni sul marchio commerciale