Supporto di boot

Install and maintain

NetApp
April 19, 2024

Sommario

Supporto di boot

Panoramica della sostituzione dei supporti di avvio - AFF A700

Il supporto di avvio principale memorizza l'immagine di avvio ONTAP utilizzata dal sistema all'avvio. È possibile ripristinare l'immagine principale del supporto di avvio utilizzando l'immagine ONTAP sul supporto di avvio secondario o, se necessario, utilizzando un'unità flash USB.

Se il supporto di avvio secondario non funziona o manca il file image.tgz, è necessario ripristinare il supporto di avvio primario utilizzando un'unità flash USB. Il disco deve essere formattato in FAT32 e disporre della quantità di storage appropriata per contenere il file image_xxx.tgz.

- Il processo di sostituzione ripristina il file system var dal supporto di avvio secondario o dall'unità flash USB al supporto di avvio primario.
- È necessario sostituire il componente guasto con un componente FRU sostitutivo ricevuto dal provider.
- È importante applicare i comandi descritti di seguito al controller corretto:
  - Il controller *alterato* è il controller su cui si esegue la manutenzione.
  - Il controller *healthy* è il partner ha del controller compromesso.

Controllare le chiavi di crittografia integrate - AFF A700s

Prima di spegnere il controller compromesso e controllare lo stato delle chiavi di crittografia integrate, è necessario controllare lo stato del controller compromesso, disattivare il giveback automatico e verificare quale versione di ONTAP è in esecuzione sul sistema.

Se si dispone di un cluster con più di due nodi, questo deve trovarsi in quorum. Se il cluster non si trova 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. Controllare lo stato del controller compromesso:
   - Se il controller non utilizzato viene visualizzato al prompt di login, accedere come `admin`.
   - Se il controller compromesso è al prompt DEL CARICATORE e fa parte della configurazione ha, accedere come `admin` sul controller integro.
   - Se il controller compromesso si trova in una configurazione standalone e al prompt DEL CARICATORE, contattare "mysupport.netapp.com".
2. 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`

3. Verificare la versione di ONTAP in esecuzione sul controller compromesso se attivato o sul controller partner se il controller non funzionante è attivo, utilizzando `version -v` comando:
   - Se nell'output del comando viene visualizzato <lno-DARE> o <1Ono-DARE>, il sistema non supporta NVE, spegnere il controller.
   - Se <lno-DARE> non viene visualizzato nell'output del comando e il sistema esegue ONTAP 9.5, passare a. Opzione 1: Selezionare NVE o NSE nei sistemi che eseguono ONTAP 9.5 e versioni precedenti.
   - Se <lno-DARE> non viene visualizzato nell'output del comando e sul sistema è in esecuzione ONTAP 9.6 o versione successiva, passare a. Opzione 2: Selezionare NVE o NSE nei sistemi che eseguono ONTAP 9.6 e versioni successive.
4. Se il controller compromesso fa parte di una configurazione ha, disattivare il giveback automatico dal controller integro: `storage failover modify -node local -auto-giveback false` oppure `storage failover modify -node local -auto-giveback-after-panic false`

Opzione 1: Selezionare NVE o NSE nei sistemi che eseguono ONTAP 9.5 e versioni precedenti

Prima di spegnere il controller compromesso, è necessario verificare se il sistema ha abilitato NetApp Volume Encryption (NVE) o NetApp Storage Encryption (NSE). In tal caso, è necessario verificare la configurazione.

Fasi

1. Collegare il cavo della console al controller compromesso.
2. Controllare se NVE è configurato per qualsiasi volume nel cluster: `volume show -is-encrypted true`

   Se nell'output sono elencati volumi, NVE viene configurato ed è necessario verificare la configurazione di NVE. Se nell'elenco non sono presenti volumi, verificare che NSE sia configurato.

3. Verificare se NSE è configurato: `storage encryption disk show`
   - Se l'output del comando elenca i dettagli del disco con le informazioni di modalità e ID chiave, NSE è configurato ed è necessario verificare la configurazione NSE.
   - Se NVE e NSE non sono configurati, è possibile spegnere il controller compromesso.

Verificare la configurazione NVE

Fasi

1. Visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi: `security key-manager query`
   - Se il `Restored` viene visualizzata la colonna `yes` vengono visualizzati tutti i principali manager `available`, è sicuro spegnere il controller compromesso.
   - Se il `Restored` la colonna visualizza un valore diverso da `yes`, o se viene visualizzato un gestore di chiavi `unavailable`, è necessario completare alcuni passaggi aggiuntivi.
   - Se viene visualizzato il messaggio questo comando non è supportato quando è attivata la gestione delle chiavi integrate, è necessario completare altri passaggi.
2. Se il `Restored` la colonna visualizzata non è diversa da `yes`, o se viene visualizzato un gestore di chiavi `unavailable`:

a. Recuperare e ripristinare tutte le chiavi di autenticazione e gli ID chiave associati: `security key-manager restore -address *`

   Se il comando non riesce, contattare il supporto NetApp.

"mysupport.netapp.com"

a. Verificare che il `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione e visualizzate da tutti i gestori delle chiavi `available`: `security key-manager query`

b. Spegnere il controller compromesso.

3. Se viene visualizzato il messaggio questo comando non è supportato quando è attivata la gestione delle chiavi integrate, visualizzare i tasti memorizzati nel gestore delle chiavi integrato: `security key-manager key show -detail`

   a. Se il `Restored` viene visualizzata la colonna `yes` eseguire manualmente il backup delle informazioni di gestione delle chiavi integrate:

      - Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
      - Immettere il comando per visualizzare le informazioni di backup OKM: `security key-manager backup show`
      - Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
      - Tornare alla modalità admin: `set -priv admin`
      - Spegnere il controller compromesso.

   b. Se il `Restored` la colonna visualizza un valore diverso da `yes`:

      - Eseguire la procedura guidata di configurazione del gestore delle chiavi: `security key-manager setup -node target/impaired node name`

        Inserire la passphrase di gestione della chiave integrata del cliente al prompt. Se non è possibile fornire la passphrase, contattare "mysupport.netapp.com"

      - Verificare che il `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione: `security key-manager key show -detail`
      - Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
      - Immettere il comando per visualizzare le informazioni di backup OKM: `security key-manager backup show`
      - Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
      - Tornare alla modalità admin: `set -priv admin`
      - È possibile arrestare il controller in modo sicuro.

Verificare la configurazione NSE

Fasi

1. Visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi: `security key-manager query`
   - Se il `Restored` viene visualizzata la colonna `yes` vengono visualizzati tutti i principali manager `available`, è sicuro spegnere il controller compromesso.
   - Se il `Restored` la colonna visualizza un valore diverso da `yes`, o se viene visualizzato un gestore di chiavi `unavailable`, è necessario completare alcuni passaggi aggiuntivi.
   - Se viene visualizzato il messaggio questo comando non è supportato quando è attivata la gestione delle chiavi integrate, è necessario completare altri passaggi
2. Se il `Restored` la colonna visualizzata non è diversa da `yes`, o se viene visualizzato un gestore di chiavi `unavailable`:

   a. Recuperare e ripristinare tutte le chiavi di autenticazione e gli ID chiave associati: `security key-manager restore -address *`

      Se il comando non riesce, contattare il supporto NetApp.

   "mysupport.netapp.com"

   a. Verificare che il `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione e visualizzate da tutti i gestori delle chiavi `available`: `security key-manager query`

   b. Spegnere il controller compromesso.
3. Se viene visualizzato il messaggio questo comando non è supportato quando è attivata la gestione delle chiavi integrate, visualizzare i tasti memorizzati nel gestore delle chiavi integrato: `security key-manager key show -detail`

   a. Se il `Restored` viene visualizzata la colonna `yes`, eseguire manualmente il backup delle informazioni di gestione delle chiavi integrate:
      - Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
      - Immettere il comando per visualizzare le informazioni di backup OKM: `security key-manager backup show`
      - Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
      - Tornare alla modalità admin: `set -priv admin`
      - Spegnere il controller compromesso.

   b. Se il `Restored` la colonna visualizza un valore diverso da `yes`:
      - Eseguire la procedura guidata di configurazione del gestore delle chiavi: `security key-manager setup -node target/impaired node name`

      > Inserire la passphrase OKM del cliente quando richiesto. Se non è possibile fornire la passphrase, contattare "mysupport.netapp.com"

- Verificare che il `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione: `security key-manager key show -detail`
- Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
- Immettere il comando per eseguire il backup delle informazioni OKM: `security key-manager backup show`

> Assicurarsi che le informazioni OKM siano salvate nel file di log. Queste informazioni saranno necessarie in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.

- Copiare il contenuto delle informazioni di backup in un file separato o nel registro. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
- Tornare alla modalità admin: `set -priv admin`
- È possibile spegnere il controller in modo sicuro.

Opzione 2: Selezionare NVE o NSE nei sistemi che eseguono ONTAP 9.6 e versioni successive

Prima di spegnere il controller compromesso, è necessario verificare se il sistema ha abilitato NetApp Volume Encryption (NVE) o NetApp Storage Encryption (NSE). In tal caso, è necessario verificare la configurazione.

1. Verificare se NVE è in uso per qualsiasi volume nel cluster: `volume show -is-encrypted true`

   Se nell'output sono elencati volumi, NVE viene configurato ed è necessario verificare la configurazione di NVE. Se nell'elenco non sono presenti volumi, verificare che NSE sia configurato e in uso.

2. Verificare se NSE è configurato e in uso: `storage encryption disk show`
   - Se l'output del comando elenca i dettagli del disco con le informazioni di modalità e ID chiave, NSE è configurato ed è necessario verificare la configurazione NSE e in uso.
   - Se non viene visualizzato alcun disco, NSE non è configurato.
   - Se NVE e NSE non sono configurati, nessun disco è protetto con chiavi NSE, è sicuro spegnere il controller compromesso.

Verificare la configurazione NVE

1. Visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi: `security key-manager key query`

   > Dopo la release di ONTAP 9.6, potrebbero essere disponibili altri tipi di gestore delle chiavi. I tipi sono `KMIP`, `AKV`, e. `GCP`. La procedura per la conferma di questi tipi è la stessa di quella per la conferma `external` oppure `onboard` tipi di gestore delle chiavi.

   - Se il `Key Manager` display dei tipi `external` e a. `Restored` viene visualizzata la colonna `yes`, è sicuro spegnere il controller compromesso.
   - Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, è necessario completare alcuni passaggi aggiuntivi.

- Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.
- Se il `Key Manager` display dei tipi `onboard` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.

2. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, Eseguire manualmente il backup delle informazioni OKM:
   a. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
   b. Immettere il comando per visualizzare le informazioni di gestione delle chiavi: `security key-manager onboard show-backup`
   c. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
   d. Tornare alla modalità admin: `set -priv admin`
   e. Spegnere il controller compromesso.
3. Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`:
   a. Ripristinare le chiavi di autenticazione per la gestione delle chiavi esterne in tutti i nodi del cluster: `security key-manager external restore`

      Se il comando non riesce, contattare il supporto NetApp.

   "mysupport.netapp.com"

   a. Verificare che il `Restored` colonna uguale a. `yes` per tutte le chiavi di autenticazione: `security key-manager key query`
   b. Spegnere il controller compromesso.
4. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` la colonna visualizza un valore diverso da `yes`:
   a. Immettere il comando di sincronizzazione del gestore delle chiavi di sicurezza integrato: `security key-manager onboard sync`

      > Immettere la passphrase di gestione della chiave alfanumerica integrata a 32 caratteri del cliente al prompt. Se non è possibile fornire la passphrase, contattare il supporto NetApp. "mysupport.netapp.com"

   b. Verificare `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione: `security key-manager key query`
   c. Verificare che il `Key Manager` viene visualizzato il tipo `onboard`, Quindi eseguire manualmente il backup delle informazioni OKM.
   d. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
   e. Immettere il comando per visualizzare le informazioni di backup per la gestione delle chiavi: `security key-manager onboard show-backup`

f. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.

g. Tornare alla modalità admin: `set -priv admin`

h. È possibile spegnere il controller in modo sicuro.

Verificare la configurazione NSE

1. Visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi: `security key-manager key query -key-type NSE-AK`

> Dopo la release di ONTAP 9.6, potrebbero essere disponibili altri tipi di gestore delle chiavi. I tipi sono `KMIP`, `AKV`, e. `GCP`. La procedura per la conferma di questi tipi è la stessa di quella per la conferma `external` oppure `onboard` tipi di gestore delle chiavi.

   - Se il `Key Manager` display dei tipi `external` e a. `Restored` viene visualizzata la colonna `yes`, è sicuro spegnere il controller compromesso.
   - Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, è necessario completare alcuni passaggi aggiuntivi.
   - Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.
   - Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.

2. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, Eseguire manualmente il backup delle informazioni OKM:

   a. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`

   b. Immettere il comando per visualizzare le informazioni di gestione delle chiavi: `security key-manager onboard show-backup`

   c. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.

   d. Tornare alla modalità admin: `set -priv admin`

   e. È possibile spegnere il controller in modo sicuro.

3. Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`:

   a. Ripristinare le chiavi di autenticazione per la gestione delle chiavi esterne in tutti i nodi del cluster: `security key-manager external restore`

      Se il comando non riesce, contattare il supporto NetApp.

   "mysupport.netapp.com"

   a. Verificare che il `Restored` colonna uguale a. `yes` per tutte le chiavi di autenticazione: `security key-manager key query`

   b. È possibile spegnere il controller in modo sicuro.

4. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` la colonna visualizza un valore diverso da `yes`:

   a. Immettere il comando di sincronizzazione del gestore delle chiavi di sicurezza integrato: `security key-manager onboard sync`

      Immettere la passphrase di gestione della chiave alfanumerica integrata a 32 caratteri del cliente al prompt. Se non è possibile fornire la passphrase, contattare il supporto NetApp.

   "mysupport.netapp.com"

   a. Verificare `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione: `security key-manager key query`
   b. Verificare che il `Key Manager` viene visualizzato il tipo `onboard`, Quindi eseguire manualmente il backup delle informazioni OKM.
   c. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
   d. Immettere il comando per visualizzare le informazioni di backup per la gestione delle chiavi: `security key-manager onboard show-backup`
   e. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
   f. Tornare alla modalità admin: `set -priv admin`
   g. È possibile spegnere il controller in modo sicuro.

Spegnere il controller - AFF A700s

Dopo aver completato le attività NVE o NSE, è necessario completare l'arresto del controller compromesso.

Fasi

1. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza…	**Quindi…**
Il prompt DEL CARICATORE	Andare a Rimozione del modulo controller.
`Waiting for 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` Quando il controller non utilizzato visualizza Waiting for giveback… (in attesa di giveback…), premere Ctrl-C e rispondere `y`.

2. Dal prompt DEL CARICATORE, immettere: `printenv` per acquisire tutte le variabili ambientali di avvio.

Salvare l'output nel file di log.

> Questo comando potrebbe non funzionare se il dispositivo di boot è corrotto o non funzionante.

Sostituire il supporto di avvio - AFF A700s

È necessario rimuovere il modulo controller dal telaio, aprirlo e sostituire il supporto di avvio guasto.

Fase 1: Rimuovere il modulo controller

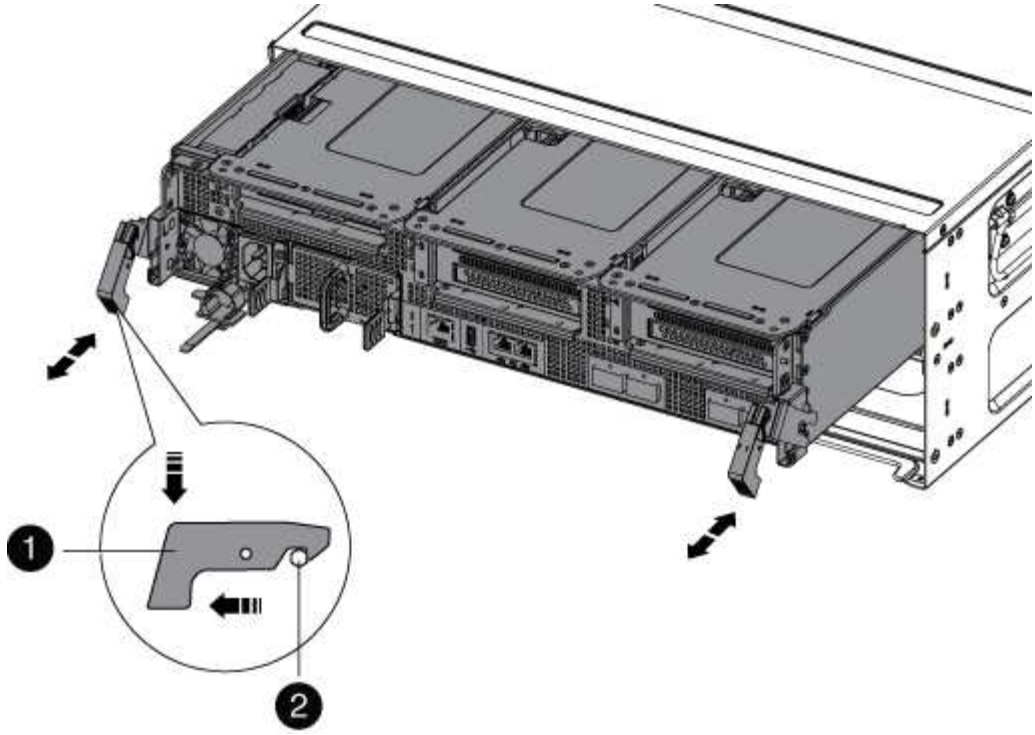
È necessario rimuovere il modulo controller dal telaio quando si sostituisce il modulo controller o un componente all'interno del modulo controller.

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Allentare il gancio e la fascetta che fissano i cavi al dispositivo di gestione dei cavi, quindi scollegare i cavi di sistema e gli SFP (se necessario) dal modulo controller, tenendo traccia del punto in cui sono stati collegati i cavi.

   Lasciare i cavi nel dispositivo di gestione dei cavi in modo che quando si reinstalla il dispositivo di gestione dei cavi, i cavi siano organizzati.

3. Scollegare l'alimentatore del modulo controller dalla fonte di alimentazione, quindi scollegare il cavo dall'alimentatore.
4. Rimuovere il dispositivo di gestione dei cavi dal modulo controller e metterlo da parte.
5. Premere verso il basso entrambi i fermi di bloccaggio, quindi ruotare entrambi i fermi verso il basso contemporaneamente.

   Il modulo controller si sposta leggermente fuori dallo chassis.

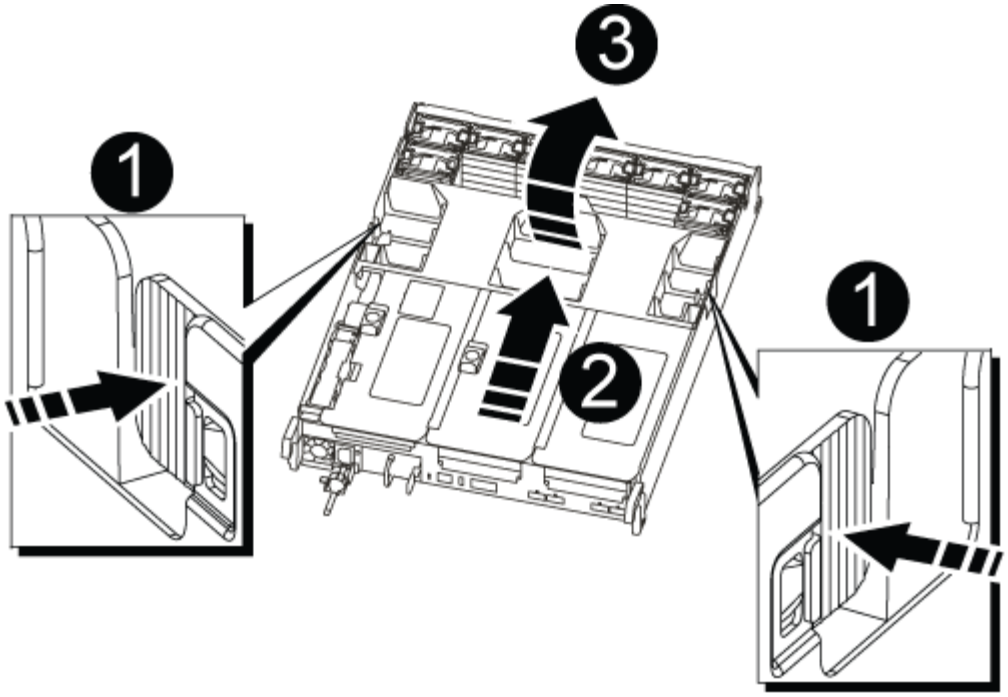


1	
Fermo di bloccaggio	
2	
Perno di bloccaggio	

1. Estrarre il modulo controller dal telaio.

   Assicurarsi di sostenere la parte inferiore del modulo controller mentre lo si sposta fuori dallo chassis.

2. Posizionare il modulo controller su una superficie piana e stabile, quindi aprire il condotto dell'aria:
   a. Premere verso l'interno le linguette di bloccaggio sui lati del condotto dell'aria verso il centro del modulo controller.
   b. Far scorrere il condotto dell'aria verso i moduli delle ventole, quindi ruotarlo verso l'alto fino a portarlo in posizione completamente aperta.



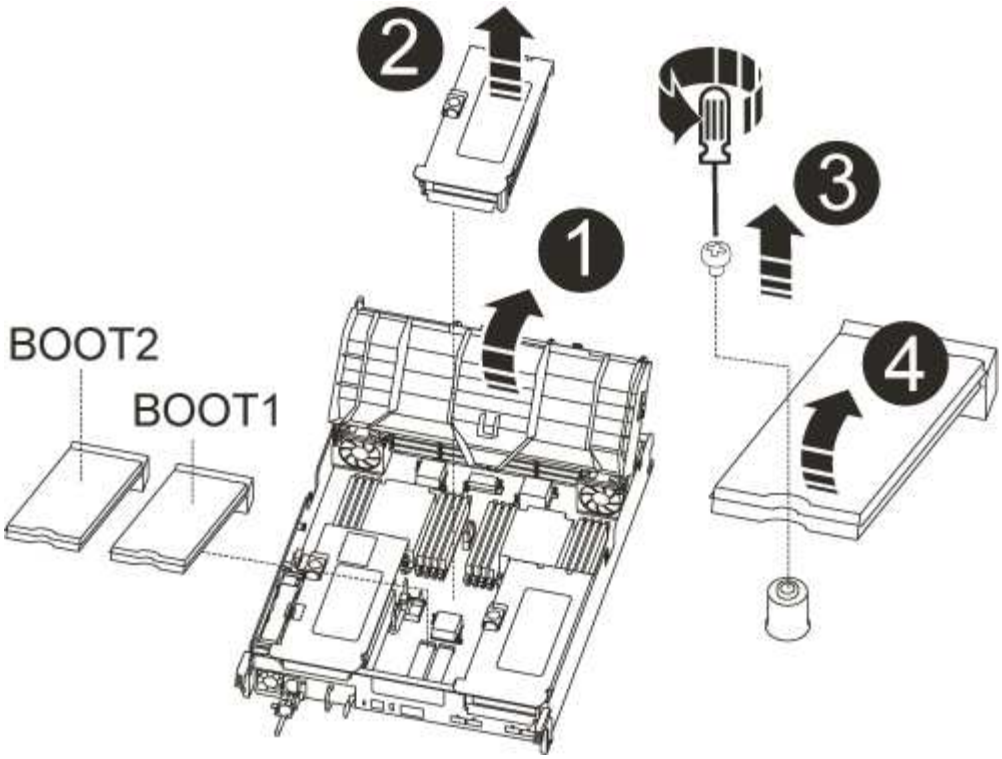
1	
Linguette di bloccaggio del condotto dell’aria	
2	
Riser	
3	
Condotto dell’aria	

Fase 2: Sostituire il supporto di avvio - AFF A700s

Individuare il supporto di avvio guasto nel modulo controller rimuovendo il modulo PCIe centrale sul modulo controller, individuando il supporto di avvio guasto e sostituendo il supporto di avvio.

Per rimuovere la vite che tiene in posizione il supporto di avvio, è necessario un cacciavite a stella.

1. Se non si è già collegati a terra, mettere a terra l’utente.
2. Individuare il supporto di avvio:
    a. Aprire il condotto dell’aria, se necessario.
    b. Se necessario, rimuovere il riser 2, il modulo PCIe centrale, sbloccando il fermo di blocco e rimuovendo il riser dal modulo controller.



1	
Condotto dell'aria	
2	
Riser 2 (modulo PCIe centrale)	
3	
Vite del supporto di avvio	
4	
Supporto di boot	

3. Individuare il supporto di avvio guasto.
4. Rimuovere il supporto di avvio dal modulo controller:
   a. Utilizzando un cacciavite Phillips n. 1, rimuovere la vite che fissa il supporto di avvio e mettere da parte la vite in un luogo sicuro.
   b. Afferrare i lati del supporto di avvio, ruotare delicatamente il supporto di avvio verso l'alto, quindi estrarre il supporto di avvio dalla presa e metterlo da parte.
5. Allineare i bordi del supporto di avvio sostitutivo con lo zoccolo del supporto di avvio, quindi spingerlo

delicatamente nello zoccolo.

6. Verificare che il supporto di avvio sia inserito correttamente e completamente nella presa.

   Se necessario, rimuovere il supporto di avvio e reinserirlo nella presa.

7. Ruotare il supporto di avvio verso il basso fino a quando non è a filo con la scheda madre.
8. Fissare il supporto di avvio in posizione utilizzando la vite.

   > Non serrare eccessivamente la vite. In questo modo, la scheda del supporto di avvio potrebbe rompersi.

9. Reinstallare il riser nel modulo controller.
10. Chiudere il condotto dell'aria:
    a. Ruotare il condotto dell'aria verso il basso.
    b. Far scorrere il condotto dell'aria verso i montanti fino a farlo scattare in posizione.

Trasferire l'immagine di boot sul supporto di boot - AFF A700s

È possibile installare l'immagine di sistema sul supporto di avvio sostitutivo utilizzando l'immagine sul secondo supporto di avvio installato nel modulo controller, il metodo principale per ripristinare l'immagine di sistema, Oppure trasferendo l'immagine di avvio sul supporto di avvio utilizzando un'unità flash USB quando il ripristino del supporto di avvio secondario non è riuscito o se il file image.tgz non viene trovato sul supporto di avvio secondario.

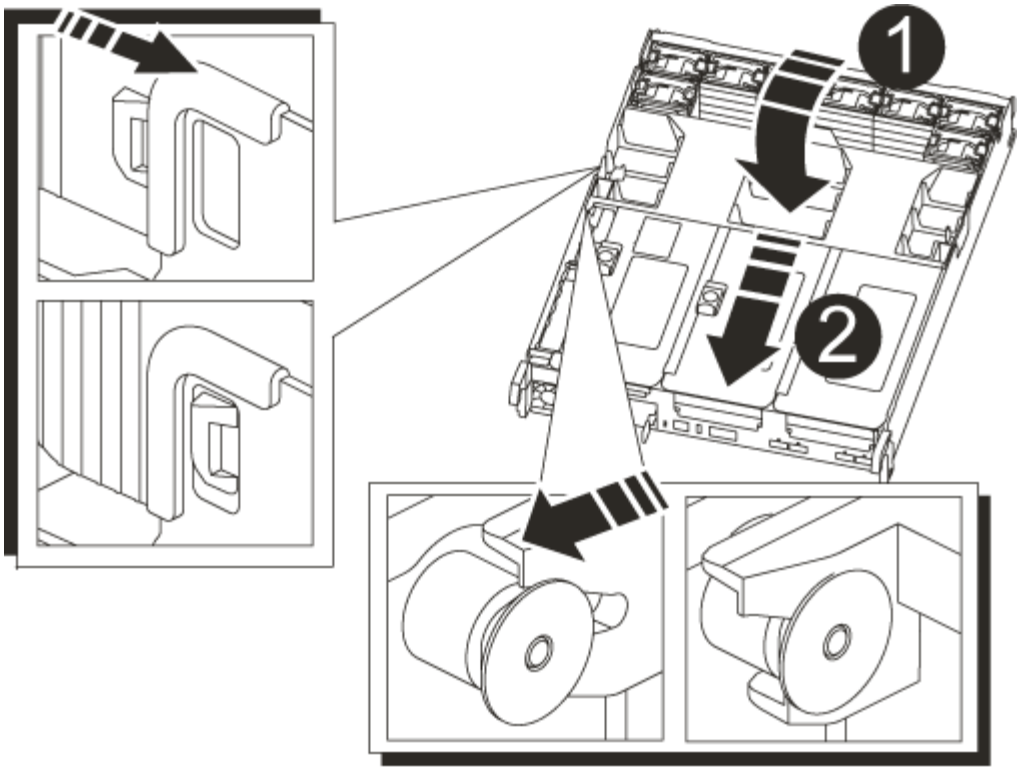
Opzione 1: Trasferimento dei file sul supporto di avvio utilizzando il backup recovery dal secondo supporto di avvio

È possibile installare l'immagine di sistema sul supporto di avvio sostitutivo utilizzando l'immagine sul secondo supporto di avvio installato nel modulo controller. Questo è il metodo principale per trasferire i file dei supporti di avvio sui supporti di avvio sostitutivi nei sistemi con due supporti di avvio nel modulo controller.

L'immagine sul supporto di avvio secondario deve contenere un `image.tgz` file e non devono riportare errori. Se il file image.tgz non è presente o il supporto di avvio segnala errori, non è possibile utilizzare questa procedura. È necessario trasferire l'immagine di avvio sul supporto di avvio sostitutivo utilizzando la procedura di sostituzione dell'unità flash USB.

Fasi

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. In caso contrario, chiudere il condotto dell'aria:
   a. Ruotare completamente il condotto dell'aria verso il basso fino al modulo controller.
   b. Far scorrere il condotto dell'aria verso i montanti fino a quando le linguette di bloccaggio non scattano in posizione.
   c. Ispezionare il condotto dell'aria per assicurarsi che sia posizionato correttamente e bloccato in posizione.



1	
Condotto dell’aria	
2	
Riser	

3. Allineare l’estremità del modulo controller con l’apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
4. Reinstallare il dispositivo di gestione dei cavi e rieseguire il sistema secondo necessità.

   Quando si esegue la modifica, ricordarsi di reinstallare i convertitori di supporti (SFP) se sono stati rimossi.

5. Ricollegare l’alimentatore, quindi collegarlo alla fonte di alimentazione.

   Assicurarsi di ricollegare il collare di bloccaggio del cavo di alimentazione al cavo di alimentazione.

6. Spingere delicatamente il modulo controller completamente nel sistema fino a quando i ganci di bloccaggio del modulo controller non iniziano a sollevarsi, spingere con decisione i ganci di bloccaggio per terminare l’alloggiamento del modulo controller, quindi ruotare i ganci di bloccaggio in posizione di blocco sui piedini del modulo controller.

   Il controller inizia ad avviarsi non appena viene installato completamente nello chassis.

7. 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.

8. Dal prompt DEL CARICATORE, avviare l'immagine di ripristino dal supporto di avvio secondario: `boot_recovery`

   L'immagine viene scaricata dal supporto di avvio secondario.

9. Quando richiesto, inserire il nome dell'immagine o accettare l'immagine predefinita visualizzata tra parentesi sullo schermo.
10. Una volta installata l'immagine, avviare il processo di ripristino:
    a. Registrare l'indirizzo IP del controller che ha subito problemi visualizzato sullo schermo.
    b. Premere `y` quando viene richiesto di ripristinare la configurazione di backup.
    c. Premere `y` quando viene richiesto di confermare che la procedura di backup è stata eseguita correttamente.
11. Dal controller partner nel livello di privilegio avanzato, avviare la sincronizzazione della configurazione utilizzando l'indirizzo IP registrato nel passaggio precedente: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`*
12. Una volta completata la sincronizzazione della configurazione senza errori, premere `y` quando viene richiesto di confermare che la procedura di backup è stata eseguita correttamente.
13. Premere `y` quando viene richiesto se si desidera utilizzare la copia ripristinata, quindi premere `y` quando viene richiesto di riavviare il controller.
14. Uscire dal livello di privilegio avanzato sul controller integro.

Opzione 2: Trasferire l'immagine di avvio sul supporto di avvio utilizzando un'unità flash USB

Questa procedura deve essere utilizzata solo se il ripristino del supporto di avvio secondario non è riuscito o se il file image.tgz non viene trovato sul supporto di avvio secondario.

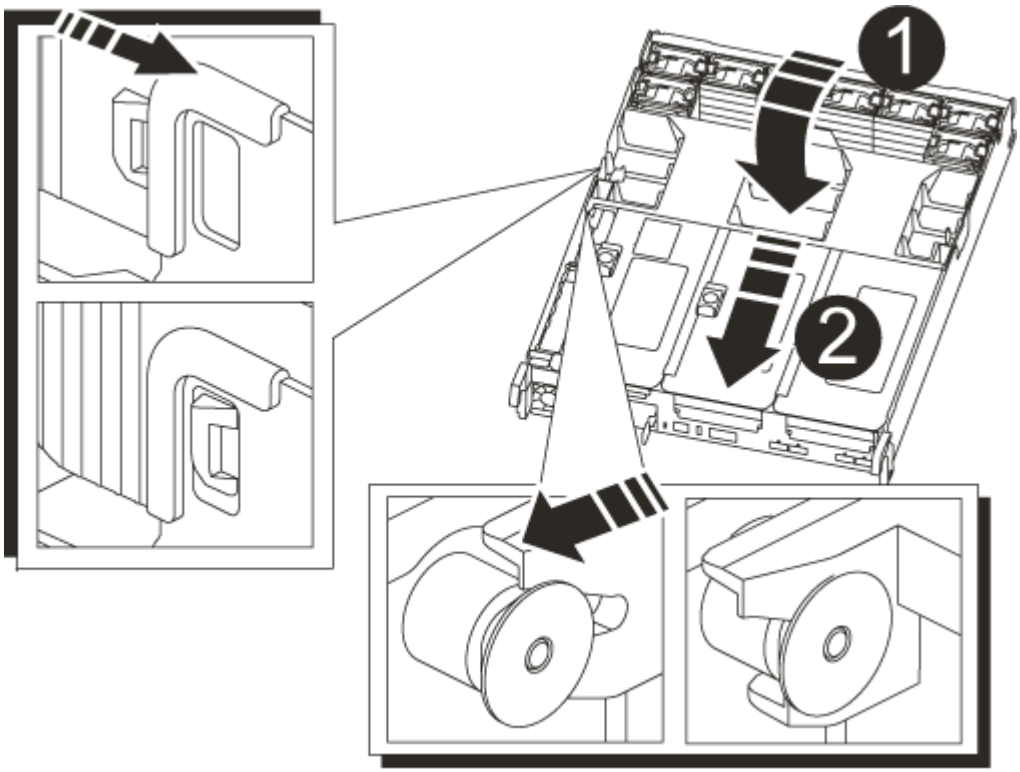
- È necessario disporre di un'unità flash USB, formattata con FAT32, con almeno 4 GB di capacità.
- Una copia della stessa versione dell'immagine di ONTAP utilizzata dal controller compromesso. È possibile scaricare l'immagine appropriata dalla sezione Download sul sito del supporto NetApp
  - Se NVE è attivato, scaricare l'immagine con NetApp Volume Encryption, come indicato nel pulsante download.
  - Se NVE non è attivato, scaricare l'immagine senza NetApp Volume Encryption, come indicato nel pulsante download.
- Se il sistema è una coppia ha, è necessario disporre di una connessione di rete.
- Se il sistema è autonomo, non è necessaria una connessione di rete, ma è necessario eseguire un ulteriore riavvio durante il ripristino del file system var.

Fasi

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. In caso contrario, chiudere il condotto dell'aria:
   a. Ruotare completamente il condotto dell'aria verso il basso fino al modulo controller.

b. Far scorrere il condotto dell'aria verso i montanti fino a quando le linguette di bloccaggio non scattano in posizione.

c. Ispezionare il condotto dell'aria per assicurarsi che sia posizionato correttamente e bloccato in posizione.



1	
Condotto dell'aria	
2	
Riser	

3. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
4. Reinstallare il dispositivo di gestione dei cavi e rieseguire il sistema secondo necessità.

   Quando si esegue la modifica, ricordarsi di reinstallare i convertitori di supporti (SFP) se sono stati rimossi.

5. Ricollegare l'alimentatore, quindi collegarlo alla fonte di alimentazione.

   Assicurarsi di ricollegare il collare di bloccaggio del cavo di alimentazione al cavo di alimentazione.

6. Inserire l'unità flash USB nello slot USB del modulo controller.

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

7. Spingere delicatamente il modulo controller completamente nel sistema fino a quando i ganci di bloccaggio del modulo controller non iniziano a sollevarsi, spingere con decisione i ganci di bloccaggio per terminare l'alloggiamento del modulo controller, quindi ruotare i ganci di bloccaggio in posizione di blocco sui piedini del modulo controller.

   Il controller inizia ad avviarsi non appena viene installato completamente nello chassis.

8. 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.

9. Sebbene le variabili d'ambiente e i bootargs siano conservati, è necessario verificare che tutte le variabili d'ambiente di boot e i bootargs necessari siano impostati correttamente per il tipo di sistema e per la configurazione utilizzando il `printenv bootarg name` e correggere eventuali errori utilizzando `setenv variable-name <value>` comando.

   a. Controllare le variabili di ambiente di boot:

      - `bootarg.init.boot_clustered`
      - `partner-sysid`
      - `bootarg.init.flash_optimized` Per AFF C190/AFF A220 (All Flash FAS)
      - `bootarg.init.san_optimized` Per array AFF A220 e SAN all-flash
      - `bootarg.init.switchless_cluster.enable`

   b. Se External Key Manager (Gestore chiavi esterne) è attivato, controllare i valori di boot, elencati in `kenv` Output ASUP:

      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `kmip.init.interface <value>`
      - `kmip.init.ipaddr <value>`
      - `kmip.init.netmask <value>`
      - `kmip.init.gateway <value>`

   c. Se Onboard Key Manager è attivato, controllare i valori di boot, elencati nella `kenv` Output ASUP:

      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `bootarg.onboard_keymanager <value>`

   d. Salvare le variabili di ambiente modificate con `savenv` comando

   e. Confermare le modifiche utilizzando `printenv *variable-name*` comando.

10. Dal prompt DEL CARICATORE, avviare l'immagine di ripristino dall'unità flash USB: `boot_recovery`

    L'immagine viene scaricata dall'unità flash USB.

11. Quando richiesto, inserire il nome dell'immagine o accettare l'immagine predefinita visualizzata tra

parentesi sullo schermo.

12. Una volta installata l'immagine, avviare il processo di ripristino:
    a. Registrare l'indirizzo IP del controller che ha subito problemi visualizzato sullo schermo.
    b. Premere `y` quando viene richiesto di ripristinare la configurazione di backup.
    c. Premere `y` quando viene richiesto di confermare che la procedura di backup è stata eseguita correttamente.
13. Premere `y` quando viene richiesto se si desidera utilizzare la copia ripristinata, quindi premere `y` quando viene richiesto di riavviare il controller.
14. Dal controller partner nel livello di privilegio avanzato, avviare la sincronizzazione della configurazione utilizzando l'indirizzo IP registrato nel passaggio precedente: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`*
15. Una volta completata la sincronizzazione della configurazione senza errori, premere `y` quando viene richiesto di confermare che la procedura di backup è stata eseguita correttamente.
16. Premere `y` quando viene richiesto se si desidera utilizzare la copia ripristinata, quindi premere `y` quando viene richiesto di riavviare il controller.
17. Verificare che le variabili ambientali siano impostate come previsto.
    a. Portare il controller al prompt DEL CARICATORE.

       Dal prompt di ONTAP, puoi eseguire il comando 'System node halt -skip-lif-migration-before-shutdown true -ignore-quorum-warnings true -inhibit-takeover true'.

    b. Controllare le impostazioni delle variabili di ambiente con `printenv` comando.
    c. Se una variabile di ambiente non è impostata come previsto, modificarla con `setenv` *`environment-variable-name changed-value`* comando.
    d. Salvare le modifiche utilizzando `savenv` comando.
    e. Riavviare il controller.
18. Con il controller riavviato per problemi che visualizza `Waiting for giveback…` eseguire un giveback dal controller integro:

Se il sistema è in…	Quindi…
Una coppia ha	Una volta visualizzato il `Waiting for giveback…` eseguire un giveback dal controller integro: a. Dal controller integro: `storage failover giveback -ofnode partner_node_name` Il controller compromesso recupera lo storage, termina l'avvio e poi si riavvia e viene nuovamente sostituito dal controller integro. Se il giveback viene vetoed, puoi prendere in considerazione la possibilità di ignorare i veti. "Gestione delle coppie HA" b. Monitorare l'avanzamento dell'operazione di giveback utilizzando `storage failover show-giveback` comando. c. Una volta completata l'operazione di giveback, verificare che la coppia ha sia in buone condizioni e che sia possibile effettuare il takeover utilizzando `storage failover show` comando. d. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify` comando.

19. Uscire dal livello di privilegio avanzato sul controller integro.

Avviare l'immagine di ripristino - AFF A700s

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

1. Dal prompt DEL CARICATORE, avviare l'immagine di ripristino dall'unità flash USB: `boot_recovery`

   L'immagine viene scaricata dall'unità flash USB.

2. Quando richiesto, inserire il nome dell'immagine o accettare l'immagine predefinita visualizzata tra parentesi sullo schermo.
3. Ripristinare il file system var:

Se il sistema dispone di…	Quindi…
Una connessione di rete	a. Premere `y` quando viene richiesto di ripristinare la configurazione di backup. b. Impostare il controller integro su un livello di privilegio avanzato: `set -privilege advanced` c. Eseguire il comando di ripristino del backup: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Riportare il controller al livello di amministrazione: `set -privilege admin` e. Premere `y` quando viene richiesto di utilizzare la configurazione ripristinata. f. Premere `y` quando viene richiesto di riavviare il controller.
Nessuna connessione di rete	a. Premere `n` quando viene richiesto di ripristinare la configurazione di backup. b. Riavviare il sistema quando richiesto dal sistema. c. Selezionare l'opzione **Update flash from backup config** (Sync flash) dal menu visualizzato. Se viene richiesto di continuare con l'aggiornamento, premere `y`.

4. Assicurarsi che le variabili ambientali siano impostate come previsto:
   a. Portare il controller al prompt DEL CARICATORE.
   b. Controllare le impostazioni delle variabili di ambiente con `printenv` comando.
   c. Se una variabile di ambiente non è impostata come previsto, modificarla con `setenv` *`environment-variable-name changed-value`* comando.
   d. Salvare le modifiche utilizzando `savenv` comando.
5. Il successivo dipende dalla configurazione del sistema:
   - Se il sistema dispone di onboard keymanager, NSE o NVE configurati, visitare il sito Ripristinare OKM, NSE e NVE secondo necessità
   - Se il sistema non dispone di onboard keymanager, NSE o NVE configurati, completare la procedura descritta in questa sezione.
6. Dal prompt DEL CARICATORE, immettere `boot_ontap` comando.

Se viene visualizzato…	Quindi…
Prompt di login	Passare alla fase successiva.

Se viene visualizzato…	Quindi…
In attesa di un giveback…	a. Accedere al controller partner. b. Verificare che il controller di destinazione sia pronto per il giveback con `storage failover show` comando.

7. Collegare il cavo della console al controller partner.
8. Restituire il controller utilizzando `storage failover giveback -fromnode local` comando.
9. Al prompt del cluster, controllare le interfacce logiche con `net int -is-home false` comando.

   Se le interfacce sono elencate come "false", ripristinarle alla porta home utilizzando `net int revert` comando.

10. Spostare il cavo della console sul controller riparato ed eseguire `version -v` Per controllare le versioni di ONTAP.
11. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

Ripristinare OKM, NSE e NVE secondo necessità - AFF A700

Una volta controllate le variabili di ambiente, è necessario completare i passaggi specifici per i sistemi con Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) o NetApp Volume Encryption (NVE) abilitati.

Determinare quale sezione utilizzare per ripristinare le configurazioni OKM, NSE o NVE:

Se NSE o NVE sono attivati insieme a Onboard Key Manager, è necessario ripristinare le impostazioni acquisite all'inizio di questa procedura.

- Se NSE o NVE sono attivati e Onboard Key Manager è attivato, passare a. Opzione 1: Restore NVE or NSE (Ripristina NVE o NSE) quando Onboard Key Manager è attivato.
- Se NSE o NVE sono abilitati per ONATP 9.5, passare a. Opzione 2: Ripristino di NSE/NVE nei sistemi che eseguono ONTAP 9.5 e versioni precedenti.
- Se NSE o NVE sono abilitati per ONTAP 9.6, passare a. Opzione 3: Ripristino di NSE/NVE nei sistemi che eseguono ONTAP 9.6 e versioni successive.

Opzione 1: Restore NVE or NSE (Ripristina NVE o NSE) quando Onboard Key Manager è attivato

Fasi

1. Collegare il cavo della console al controller di destinazione.
2. Utilizzare `boot_ontap` Al prompt DEL CARICATORE per avviare il controller.
3. Controllare l'output della console:

Se la console visualizza…	Allora…
Il prompt DEL CARICATORE	Avviare il controller dal menu di avvio: `boot_ontap menu`
In attesa di un giveback…	a. Invio `Ctrl-C` quando richiesto b. Quando viene visualizzato il messaggio: Arrestare il controller invece di attendere [y/n]? , inserire: `y` c. Al prompt DEL CARICATORE, immettere `boot_ontap menu` comando.

4. Nel menu di avvio, immettere il comando nascosto, `recover_onboard_keymanager` e rispondere `y` quando richiesto.
5. Inserire la passphrase per il gestore delle chiavi integrato ottenuto dal cliente all'inizio di questa procedura.
6. Quando viene richiesto di inserire i dati di backup, incollare i dati di backup acquisiti all'inizio di questa procedura, quando richiesto. Incollare l'output di `security key-manager backup show` OPPURE `security key-manager onboard show-backup` comando.

   > I dati vengono generati da entrambi `security key-manager backup show` oppure `security key-manager onboard show-backup` comando.

   Esempio di dati di backup:

   ```
   ---------- INIZIA IL BACKUP----------
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . .
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

   ---------- FINE BACKUP----------
   ```

7. Nel menu di avvio, selezionare l'opzione Normal Boot (Avvio normale).

   Il sistema si avvia in `Waiting for giveback…` prompt.

8. Spostare il cavo della console sul controller partner e accedere come admin.
9. Verificare che il controller di destinazione sia pronto per il giveback con `storage failover show` comando.
10. Restituire solo gli aggregati CFO con il giveback di failover dello storage `-fromnode local -only-cfo -aggregates true` comando.
    - Se il comando non riesce a causa di un disco guasto, disinnestare fisicamente il disco guasto, ma lasciare il disco nello slot fino a quando non viene ricevuto un disco sostitutivo.
    - Se il comando non riesce a causa di una sessione CIFS aperta, verificare con il cliente come chiudere le sessioni CIFS.

> La chiusura di CIFS può causare la perdita di dati.

- Se il comando non riesce perché il partner è "non pronto", attendere 5 minuti per la sincronizzazione di NVMEM.
- Se il comando non riesce a causa di un processo NDMP, SnapMirror o SnapVault, disattivare il processo. Per ulteriori informazioni, consultare il centro di documentazione appropriato.

11. Una volta completato il giveback, controllare lo stato di failover e giveback con `storage failover show` e. `storage failover show`-giveback` comandi.

    Verranno mostrati solo gli aggregati CFO (aggregato root e aggregati di dati di stile CFO).

12. Spostare il cavo della console sul controller di destinazione.
13. Se si utilizza ONTAP 9.5 e versioni precedenti, eseguire l'installazione guidata del gestore delle chiavi:
    a. Avviare la procedura guidata utilizzando `security key-manager setup -nodenodename` e, quando richiesto, inserire la passphrase per la gestione della chiave integrata.
    b. Inserire il `key-manager key show -detail` per visualizzare una vista dettagliata di tutte le chiavi memorizzate nel gestore delle chiavi integrato e verificare che `Restored` colonna = `yes` per tutte le chiavi di autenticazione.

    > Se il `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes`, Contattare il supporto clienti.

    c. Attendere 10 minuti per la sincronizzazione della chiave nel cluster.
14. Se si utilizza ONTAP 9.6 o versione successiva:
    a. Eseguire `security key-manager onboard sync` e inserire la passphrase quando richiesto.
    b. Inserire il `security key-manager key query` per visualizzare una vista dettagliata di tutte le chiavi memorizzate nel gestore delle chiavi integrato e verificare che `Restored` colonna = `yes/true` per tutte le chiavi di autenticazione.

    > Se il `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes/true`, Contattare il supporto clienti.

    c. Attendere 10 minuti per la sincronizzazione della chiave nel cluster.
15. Spostare il cavo della console sul controller partner.
16. Restituire il controller di destinazione utilizzando `storage failover giveback -fromnode local` comando.
17. Controllare lo stato del giveback, 3 minuti dopo il completamento del report, utilizzando `storage failover show` comando.

    Se il giveback non viene completato dopo 20 minuti, contattare l'assistenza clienti.

18. Al prompt di clustershell, immettere `net int show -is-home false` comando per elencare le interfacce logiche che non si trovano sul proprio controller principale e sulla relativa porta.

    Se le interfacce sono elencate come `false`, ripristinare tali interfacce alla porta home utilizzando `net int revert -vserver Cluster -lif` *`nodename`* comando.

19. Spostare il cavo della console sul controller di destinazione ed eseguire `version -v` Per controllare le versioni di ONTAP.
20. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

Opzione 2: Ripristino di NSE/NVE nei sistemi che eseguono ONTAP 9.5 e versioni precedenti

Fasi

1. Collegare il cavo della console al controller di destinazione.
2. Utilizzare `boot_ontap` Al prompt DEL CARICATORE per avviare il controller.
3. Controllare l'output della console:

Se la console visualizza…	Allora…
Prompt di login	Passare alla fase 7.
In attesa di un giveback…	a. Accedere al controller partner. b. Verificare che il controller di destinazione sia pronto per il giveback con `storage failover show` comando.

4. Spostare il cavo della console sul controller partner e restituire lo storage del controller di destinazione utilizzando `storage failover giveback -fromnode local -only-cfo-aggregates true local` comando.
   - Se il comando non riesce a causa di un disco guasto, disinnestare fisicamente il disco guasto, ma lasciare il disco nello slot fino a quando non viene ricevuto un disco sostitutivo.
   - Se il comando non riesce a causa di sessioni CIFS aperte, verificare con il cliente come chiudere le sessioni CIFS.

     La chiusura di CIFS può causare la perdita di dati.

   - Se il comando non riesce perché il partner non è pronto, attendere 5 minuti per la sincronizzazione di NVMEM.
   - Se il comando non riesce a causa di un processo NDMP, SnapMirror o SnapVault, disattivare il processo. Per ulteriori informazioni, consultare il centro di documentazione appropriato.
5. Attendere 3 minuti e controllare lo stato di failover con `storage failover show` comando.
6. Al prompt di clustershell, immettere `net int show -is-home false` comando per elencare le interfacce logiche che non si trovano sul proprio controller principale e sulla relativa porta.

   Se le interfacce sono elencate come `false`, ripristinare tali interfacce alla porta home utilizzando `net int revert -vserver Cluster -lif` *`nodename`* comando.

7. Spostare il cavo della console sul controller di destinazione ed eseguire la versione `-v command` Per controllare le versioni di ONTAP.
8. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node`

`local -auto-giveback true` comando.

9. Utilizzare `storage encryption disk show` al prompt di clustershell, per rivedere l'output.

> Questo comando non funziona se è configurato NVE (NetApp Volume Encryption)

10. Utilizzare la query del gestore delle chiavi di protezione per visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi.
    - Se il `Restored` colonna = `yes` E tutti i responsabili chiave riportano lo stato disponibile, andare alla sezione *completamento del processo di sostituzione*.
    - Se il `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes`, e/o uno o più gestori di chiavi non sono disponibili, utilizzare `security key-manager restore -address` Comando per recuperare e ripristinare tutte le chiavi di autenticazione (AKS) e gli ID delle chiavi associati a tutti i nodi da tutti i server di gestione delle chiavi disponibili.

      Controllare nuovamente l'output della query del gestore delle chiavi di protezione per assicurarsi che il `Restored` colonna = `yes` e tutti i manager chiave riportano in uno stato disponibile

11. Se Onboard Key Management è attivato:
    a. Utilizzare `security key-manager key show -detail` per visualizzare una vista dettagliata di tutte le chiavi memorizzate nel gestore delle chiavi integrato.
    b. Utilizzare `security key-manager key show -detail` controllare e verificare che `Restored` colonna = `yes` per tutte le chiavi di autenticazione.

       Se il `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes`, utilizzare `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* Comando per ripristinare le impostazioni di Onboard Key Management. Rieseguire il `security key-manager key show -detail` comando da verificare `Restored` colonna = `yes` per tutte le chiavi di autenticazione.

12. Collegare il cavo della console al controller partner.
13. Restituire il controller utilizzando `storage failover giveback -fromnode local` comando.
14. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

Opzione 3: Ripristino di NSE/NVE nei sistemi che eseguono ONTAP 9.6 e versioni successive

Fasi

1. Collegare il cavo della console al controller di destinazione.
2. Utilizzare `boot_ontap` Al prompt DEL CARICATORE per avviare il controller.
3. Controllare l'output della console:

Se la console visualizza…	Quindi…
Prompt di login	Passare alla fase 7.

Se la console visualizza…	Quindi…
In attesa di un giveback…	a. Accedere al controller partner. b. Verificare che il controller di destinazione sia pronto per il giveback con `storage failover show` comando.

4. Spostare il cavo della console sul controller partner e restituire lo storage del controller di destinazione utilizzando `storage failover giveback -fromnode local -only-cfo-aggregates true local` comando.
   - Se il comando non riesce a causa di un disco guasto, disinnestare fisicamente il disco guasto, ma lasciare il disco nello slot fino a quando non viene ricevuto un disco sostitutivo.
   - Se il comando non riesce a causa di una sessione CIFS aperta, verificare con il cliente come chiudere le sessioni CIFS.

     La chiusura di CIFS può causare la perdita di dati.

   - Se il comando non riesce perché il partner è "non pronto", attendere 5 minuti per la sincronizzazione di NVMEM.
   - Se il comando non riesce a causa di un processo NDMP, SnapMirror o SnapVault, disattivare il processo. Per ulteriori informazioni, consultare il centro di documentazione appropriato.
5. Attendere 3 minuti e controllare lo stato di failover con `storage failover show` comando.
6. Al prompt di clustershell, immettere `net int show -is-home false` comando per elencare le interfacce logiche che non si trovano sul proprio controller principale e sulla relativa porta.

   Se le interfacce sono elencate come `false`, ripristinare tali interfacce alla porta home utilizzando `net int revert -vserver Cluster -lif` *`nodename`* comando.

7. Spostare il cavo della console sul controller di destinazione ed eseguire `version -v` Per controllare le versioni di ONTAP.
8. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.
9. Utilizzare `storage encryption disk show` al prompt di clustershell, per rivedere l'output.
10. Utilizzare `security key-manager key query` Per visualizzare gli ID delle chiavi di autenticazione memorizzate nei server di gestione delle chiavi.
    - Se il `Restored` colonna = `yes/true`, è possibile completare il processo di sostituzione.
    - Se il `Key Manager type` = `external` e a. `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes/true`, utilizzare `security key-manager external restore` Comando per ripristinare gli ID delle chiavi di autenticazione.

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

    - Se il `Key Manager type` = `onboard` e a. `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes/true`, utilizzare `security key-manager onboard sync` Comando per risync il tipo di Key Manager.

Utilizzare la query della chiave di gestione delle chiavi di protezione per verificare che `Restored` colonna = `yes/true` per tutte le chiavi di autenticazione.

11. Collegare il cavo della console al controller partner.
12. Restituire il controller utilizzando `storage failover giveback -fromnode local` comando.
13. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.
14. Ripristinare AutoSupport se è stato disattivato utilizzando `system node autosupport invoke -node * -type all -message MAINT=END`

Restituire il componente guasto a NetApp - AFF A700

Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit. Vedere "Parti restituita sostituzioni" per ulteriori informazioni.