# Supporto di boot

## Install and maintain

NetApp
September 20, 2024

# Sommario

# Supporto di boot

## Panoramica sulla sostituzione dei supporti di avvio - AFF C250

Il supporto di avvio memorizza un set primario e secondario di file di sistema (immagine di avvio) che il sistema utilizza al momento dell'avvio.

**Prima di iniziare**

- È necessario disporre di un'unità flash USB, formattata in MBR/FAT32, con la quantità di storage appropriata per contenere `image_xxx.tgz` file.
- È inoltre necessario copiare il `image_xxx.tgz` Sul disco flash USB per utilizzarlo successivamente in questa procedura.

**A proposito di questa attività**

- I metodi senza interruzioni e senza interruzioni per la sostituzione di un supporto di avvio richiedono entrambi il ripristino di `var` file system:
  - Per la sostituzione senza interruzioni, la coppia ha deve essere connessa a una rete per ripristinare `var` file system.
  - Per la sostituzione delle interruzioni, non è necessaria una connessione di rete per ripristinare `var` file system, ma il processo richiede due riavvii.
- 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 nodo *alterato* è il controller su cui si esegue la manutenzione.
  - Il nodo *healthy* è il partner ha del controller compromesso.

## Controllare le chiavi di crittografia integrate - AFF C250

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 sul sistema è in esecuzione ONTAP 9.6 o versione successiva, passare alla sezione successiva.
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`

## Controllare 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 C250

## Opzione 1: La maggior parte dei sistemi

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`<br><br>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.

## Opzione 2: Sistemi in un MetroCluster

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

Non utilizzare questa procedura se il sistema si trova in una configurazione MetroCluster a due nodi.

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".
- Se si dispone di una configurazione MetroCluster, è necessario confermare 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. Disattivare il giveback automatico dalla console del controller integro: `storage failover modify -node local -auto-giveback false`
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. |
| 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`*<br><br>Quando il controller non utilizzato visualizza Waiting for giveback… (in attesa di giveback…), premere Ctrl-C e rispondere `y`. |

# Sostituire il supporto di avvio - AFF C250

Per sostituire il supporto di avvio, è necessario rimuovere il modulo controller compromesso, installare il supporto di avvio sostitutivo e trasferire l'immagine di avvio su un'unità flash USB.

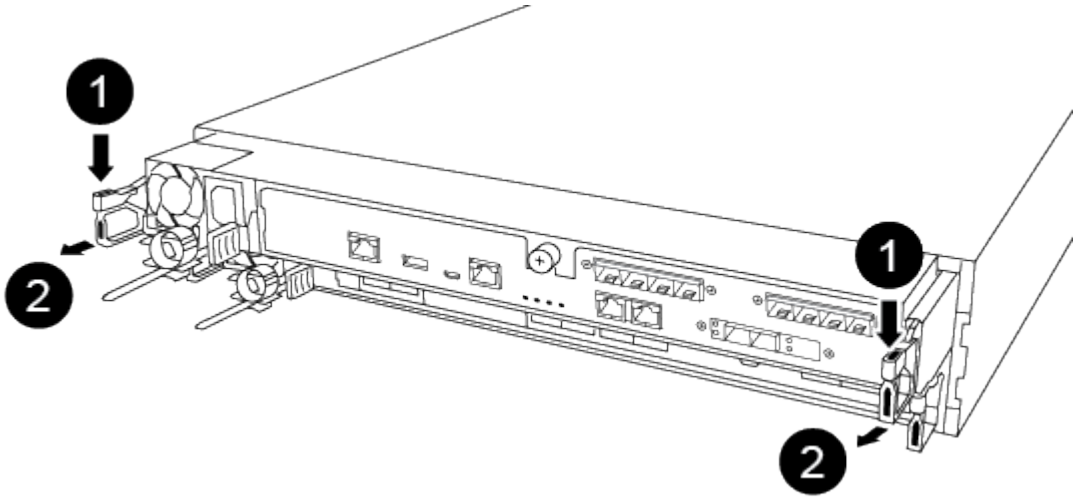
## Fase 1: Rimuovere il modulo controller

Per accedere ai componenti all'interno del modulo controller, rimuovere prima il modulo controller dal sistema, quindi rimuovere il coperchio sul modulo controller.

**Fasi**

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Scollegare gli alimentatori del modulo controller dalla fonte di alimentazione.
3. Rilasciare i fermi dei cavi di alimentazione, quindi scollegare i cavi dagli alimentatori.
4. Inserire l'indice nel meccanismo di blocco su entrambi i lati del modulo controller, premere la leva con il pollice ed estrarre delicatamente il controller dal telaio.

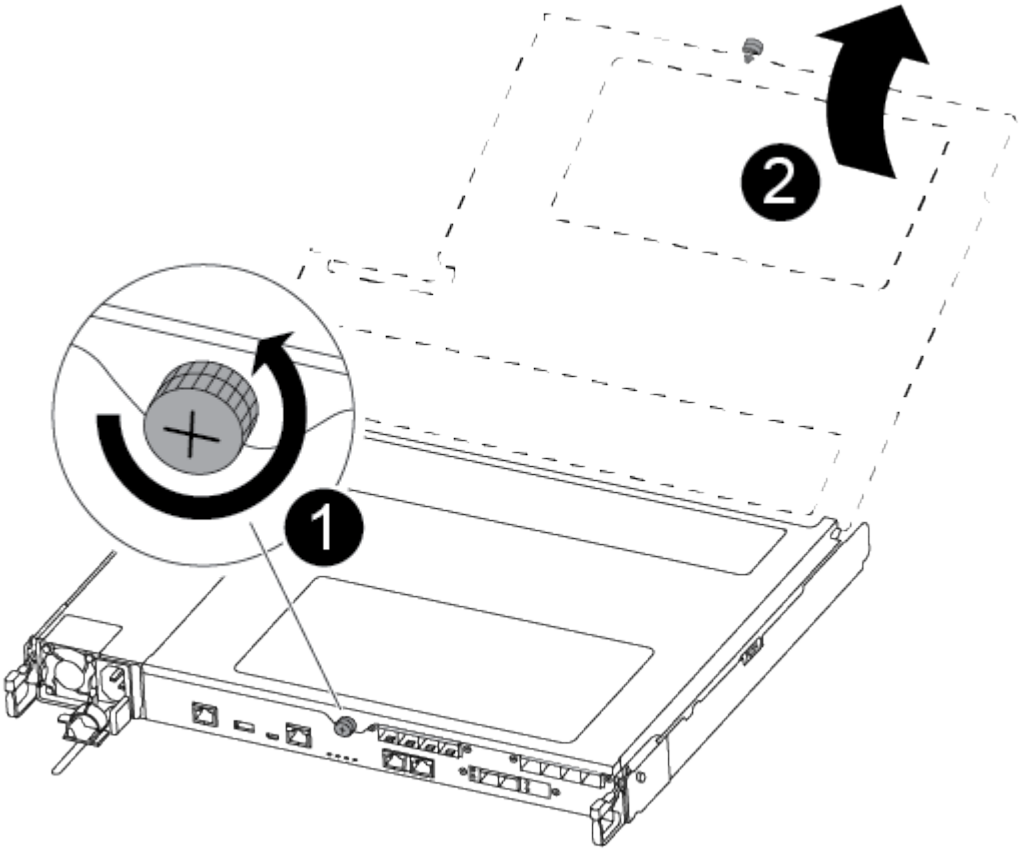
> In caso di difficoltà nella rimozione del modulo controller, posizionare le dita di riferimento attraverso i fori all'interno (incrociando le braccia).




| | |
|---|---|
| 1 | |
| Leva | |
| 2 | |
| Meccanismo di blocco | |

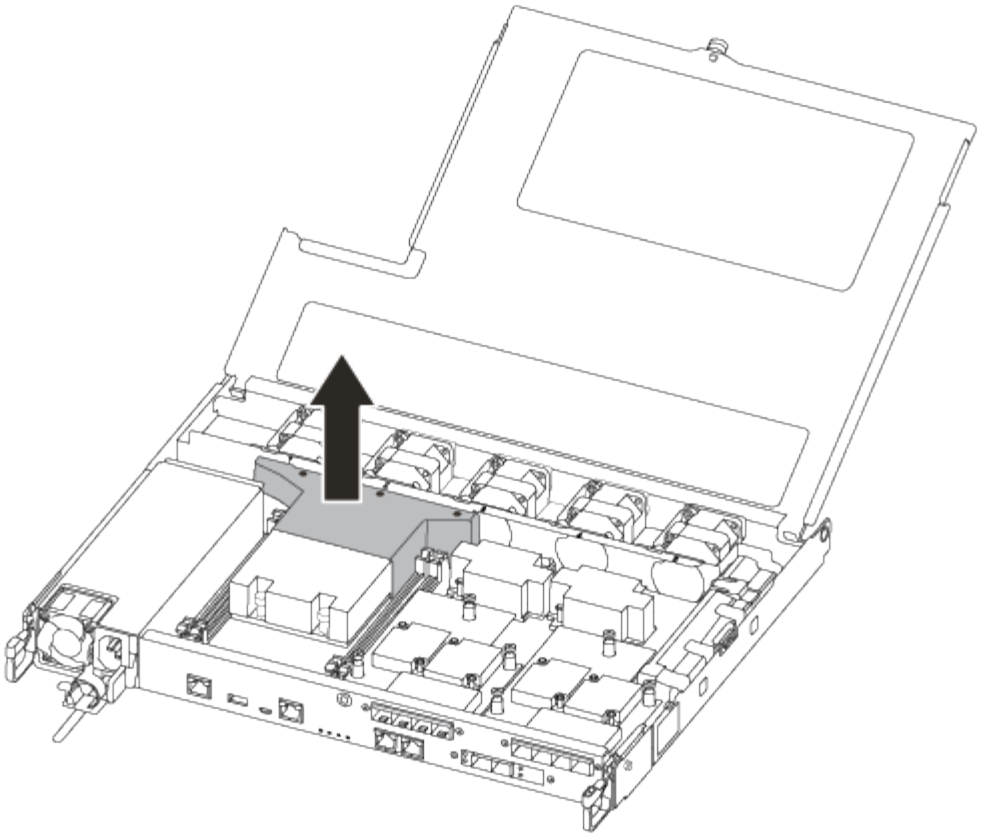
5. Con entrambe le mani, afferrare i lati del modulo controller ed estrarlo delicatamente dallo chassis e posizionare il modulo su una superficie piana e stabile.

6. Ruotare la vite a testa zigrinata sulla parte anteriore del modulo controller in senso antiorario e aprire il coperchio del modulo controller.




| | |
|---|---|
| 1 | |
| Vite a testa zigrinata | |
| 2 | |
| Coperchio del modulo controller. | |

7. Estrarre il coperchio del condotto dell'aria.



## Fase 2: Sostituire il supporto di avvio

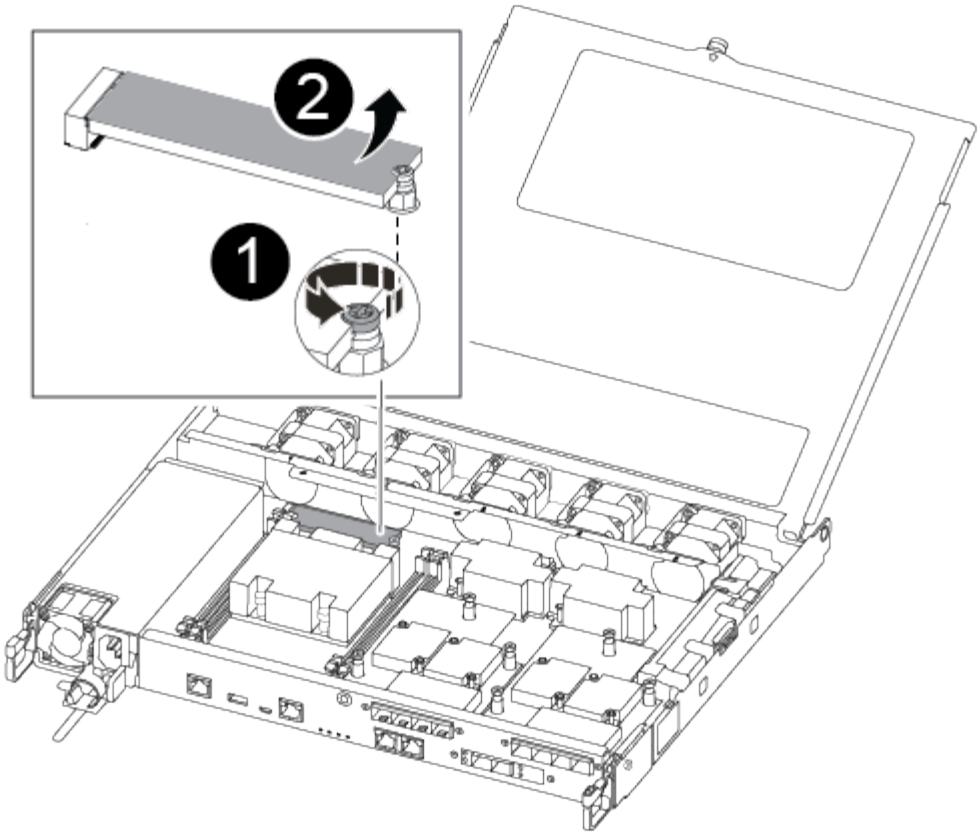
Individuare il supporto di avvio guasto nel modulo controller rimuovendo il condotto dell'aria sul modulo controller prima di sostituire il supporto di avvio.

Per rimuovere la vite che tiene in posizione il supporto di avvio, è necessario un cacciavite a croce magnetico n. 1. A causa dei limiti di spazio all'interno del modulo controller, è necessario disporre anche di un magnete per trasferire la vite in modo da non perderla.

Per sostituire il supporto di avvio, è possibile utilizzare il seguente video o la procedura tabulare:

Animazione - sostituire il supporto di avvio

1. Individuare e sostituire i supporti di avvio non adatti dal modulo controller.



| | |
|---|---|
| 1 | Rimuovere la vite che fissa il supporto di avvio alla scheda madre nel modulo controller. |
| 2 | Estrarre il supporto di avvio dal modulo controller. |

2. Utilizzando il cacciavite magnetico n. 1, rimuovere la vite dal supporto di avvio compromesso e metterla da parte in modo sicuro sul magnete.
3. Sollevare delicatamente il supporto di avvio compromesso direttamente dalla presa e metterlo da parte.
4. Rimuovere il supporto di avvio sostitutivo dalla confezione antistatica e allinearlo in posizione sul modulo controller.
5. Utilizzando il cacciavite magnetico n. 1, inserire e serrare la vite sul supporto di avvio.

> Non esercitare forza durante il serraggio della vite sul supporto di avvio, poiché potrebbe rompersi.

## Fase 3: Trasferire l'immagine di avvio sul supporto di avvio

Il supporto di avvio sostitutivo installato non dispone di un'immagine di avvio, pertanto è necessario trasferire un'immagine di avvio utilizzando un'unità flash USB.

- È necessario disporre di un'unità flash USB, formattata in MBR/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.

a. Scaricare e copiare l'immagine del servizio appropriata dal sito del supporto NetApp sull'unità flash USB.
b. Scarica l'immagine del servizio nel tuo spazio di lavoro sul laptop.
c. 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.

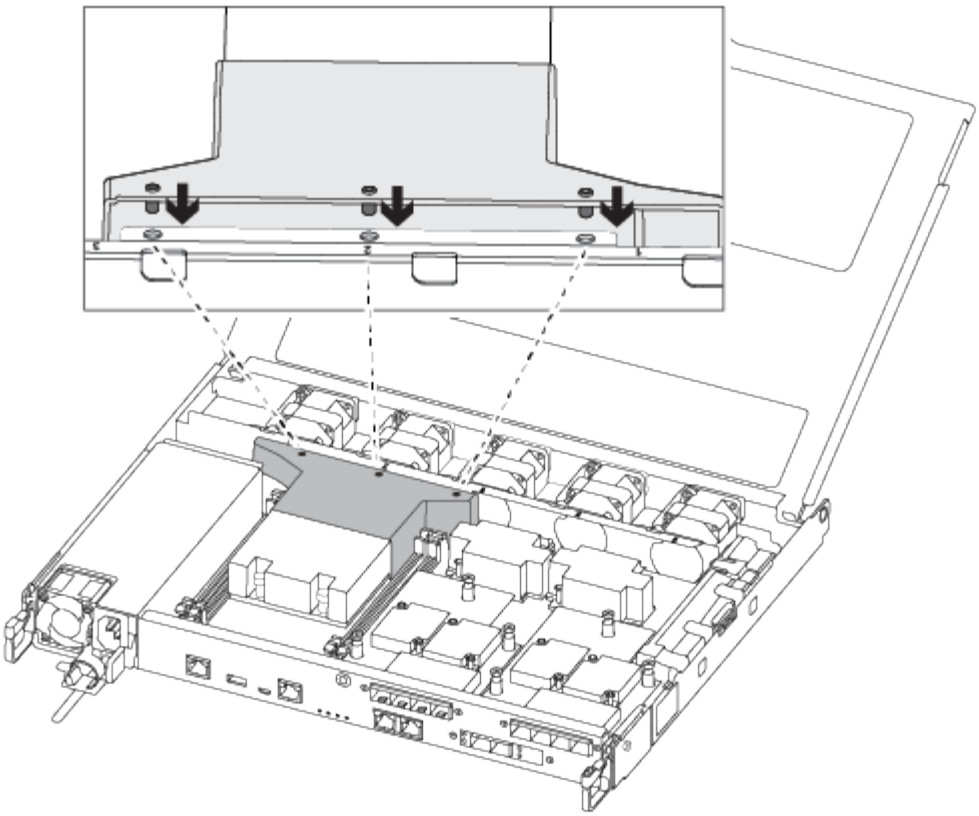
Il file di immagine del servizio decompresso contiene due cartelle:

    - avviare
    - efi

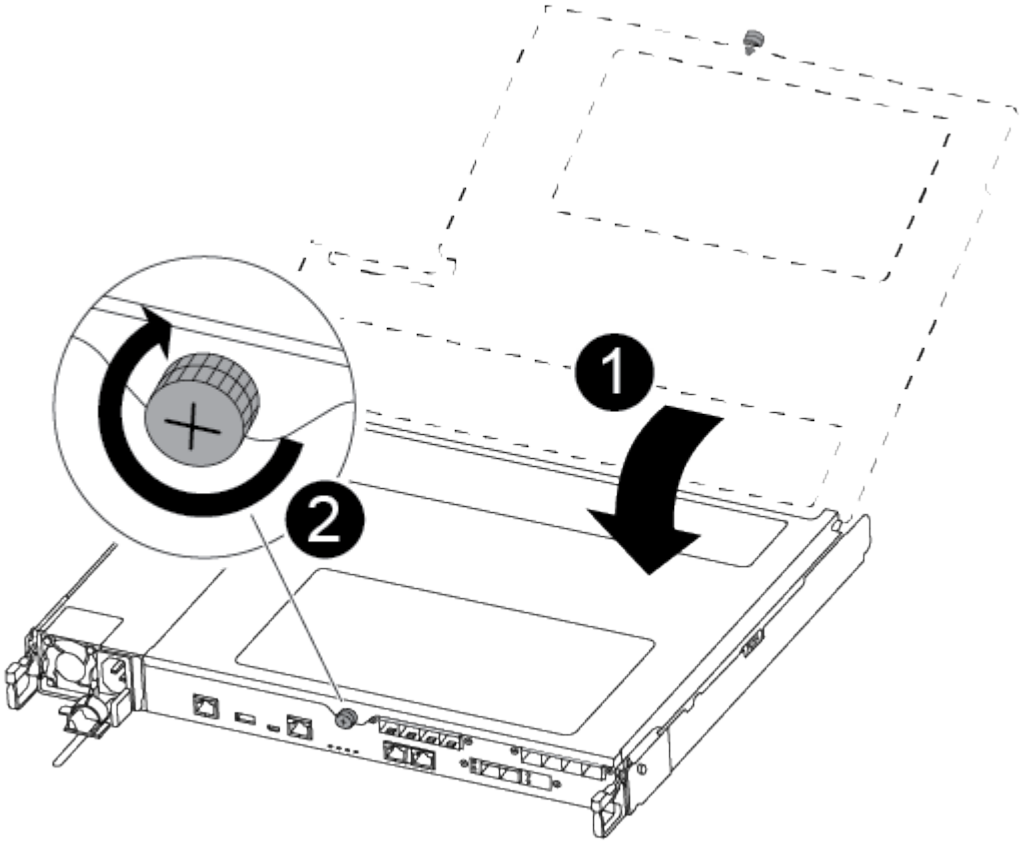
d. Copiare la cartella efi nella directory principale dell'unità flash USB.

L'unità flash USB deve disporre della cartella efi e della stessa versione del BIOS (Service Image) del controller non funzionante.

e. Rimuovere l'unità flash USB dal computer portatile.
f. Se non è già stato fatto, installare il condotto dell'aria.



g. Chiudere il coperchio del modulo controller e serrare la vite a testa zigrinata.



| | |
|---|---|
| ❶ | Coperchio del modulo controller |
| ❷ | Vite a testa zigrinata |

h. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

i. Collegare il cavo di alimentazione all'alimentatore e reinstallare il fermo del cavo di alimentazione.

j. 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.

k. Inserire completamente il modulo controller nello chassis:

l. Posizionare le dita di riferimento attraverso i fori per le dita dall'interno del meccanismo di blocco.

m. Premere i pollici verso il basso sulle linguette arancioni sulla parte superiore del meccanismo di blocco e spingere delicatamente il modulo controller oltre il fermo.

n. Rilasciare i pollici dalla parte superiore dei meccanismi di blocco e continuare a spingere fino a quando i meccanismi di blocco non scattano in posizione.

   Il modulo controller inizia ad avviarsi non appena viene inserito completamente nello chassis. Prepararsi ad interrompere il processo di avvio.

   Il modulo controller deve essere inserito completamente e a filo con i bordi dello chassis.

o. Interrompere il processo di avvio per interrompere il CARICAMENTO premendo Ctrl-C quando viene visualizzato Avvio DI AUTOBOOT premere Ctrl-C per interrompere….

   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.

p. Per i sistemi con un controller nello chassis, ricollegare l'alimentazione e accendere gli alimentatori.

   Il sistema inizia ad avviarsi e si arresta al prompt DEL CARICATORE.

q. Impostare il tipo di connessione di rete al prompt DEL CARICATORE:

   - Se si sta configurando DHCP: `ifconfig e0a -auto`

     > La porta di destinazione configurata è la porta di destinazione utilizzata per comunicare con il controller compromesso dal controller integro durante il ripristino del file system var con una connessione di rete. È anche possibile utilizzare la porta e0M in questo comando.

   - Se si configurano connessioni manuali: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - `filer_addr` È l'indirizzo IP del sistema di storage.
     - `netmask` È la maschera di rete della rete di gestione connessa al partner ha.
     - `gateway` è il gateway per la rete.

- `dns_addr` È l'indirizzo IP di un name server sulla rete.
- `dns_domain` È il nome di dominio DNS (Domain Name System).

  Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot. È necessario solo il nome host del server.

> Potrebbero essere necessari altri parametri per l'interfaccia. È possibile immettere `help ifconfig` al prompt del firmware per ulteriori informazioni.

# Avviare l'immagine di ripristino - AFF C250

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 `var` file system:

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

| Se il sistema dispone di… | Quindi… |
| --- | --- |
| Nessuna connessione di rete e si trova in una configurazione MetroCluster IP | a. Premere `n` quando viene richiesto di ripristinare la configurazione di backup.<br>b. Riavviare il sistema quando richiesto dal sistema.<br>c. Attendere che le connessioni dello storage iSCSI si connettano.<br>È possibile procedere dopo aver visualizzato i seguenti messaggi:<br>`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`<br>`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`<br>`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`<br>`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`<br>d. Selezionare l'opzione **Update flash from backup config** (Sync flash) dal menu visualizzato.<br>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 `saveenv` 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. |
| In attesa di un giveback… | a. Accedere al controller partner.<br>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 C250

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.

1. Determinare la sezione da 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. Restore NVE or NSE (Ripristina NVE o NSE) quando Onboard Key Manager è attivato.
   - Se NSE o NVE sono abilitati per ONTAP 9.6, passare a. Ripristinare NSE/NVE nei sistemi che eseguono ONTAP 9.6 e versioni successive.

## 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<br>b. Quando viene visualizzato il messaggio: Interrompere questo nodo invece di attendere [y/n]? , inserire: `y`<br>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
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . .
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

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

   Il sistema si avvia in attesa di giveback… prompt.

8. Verificare che il controller di destinazione sia pronto per il giveback con `storage failover show` comando.
9. Giveback solo il CFO si aggrega con `storage failover giveback -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 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.

10. 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).

11. Spostare il cavo della console sul controller di destinazione.
    a. Se si utilizza ONTAP 9.6 o versione successiva, eseguire la sincronizzazione integrata del Security Key-Manager:
    b. Eseguire `security key-manager onboard sync` e inserire la passphrase quando richiesto.
    c. 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.

    d. Attendere 10 minuti per la sincronizzazione della chiave nel cluster.
12. Spostare il cavo della console sul controller partner.
13. Restituire il controller di destinazione utilizzando `storage failover giveback -fromnode local` comando.
14. 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.

15. 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.

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

## Ripristinare 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… | Allora… |
|---|---|
| Prompt di login | Passare alla fase 7. |
| In attesa di un giveback… | a. Accedere al controller partner.<br>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 `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 `security key-manager key query` per verificare che il `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.

# Restituire il componente guasto a NetApp - AFF C250

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