



# **Supporto di boot**

## **Install and maintain**

NetApp  
September 20, 2024

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems/fas8200/bootmedia-replace-overview.html> on September 20, 2024. Always check docs.netapp.com for the latest.

# Sommario

- Supporto di boot ..... 1
  - Panoramica sulla sostituzione dei supporti di avvio - FAS8200 ..... 1
  - Controllare la crittografia integrata - FAS8200 ..... 1
  - Spegnere il controller compromesso - FAS8200 ..... 8
  - Sostituire il supporto di avvio - FAS8200 ..... 12
  - Avviare l'immagine di ripristino - FAS8200 ..... 15
  - Switch back aggregates in una configurazione MetroCluster a due nodi - FAS8200 ..... 18
  - Ripristinare OKM, NSE e NVE secondo necessità - FAS8200 ..... 19
  - Restituire il componente guasto a NetApp - FAS8200 ..... 25

# Supporto di boot

## Panoramica sulla sostituzione dei supporti di avvio - FAS8200

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. A seconda della configurazione di rete, è possibile eseguire una sostituzione senza interruzioni o senza interruzioni.

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

- 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 di questi passaggi al nodo corretto:
  - Il nodo *alterato* è il nodo su cui si esegue la manutenzione.
  - Il *nodo sano* è il partner ha del nodo compromesso.

## Controllare la crittografia integrata - FAS8200

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 la versione di ONTAP in esecuzione nel sistema.

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"](https://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 <Ino-DARE> o <1Ono-DARE>, il sistema non supporta NVE, spegnere il controller.
    - Se <Ino-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 <Ino-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"](https://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. Spegner 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`
- Spegner 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"](https://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"](https://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. Spegnerne 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`
      - Spegnerne 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"](https://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"](https://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"](https://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"](https://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"](https://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 compromesso - FAS8200

### Opzione 1: La maggior parte dei sistemi

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

Se il controller non utilizzato visualizza...	Quindi...
Prompt di sistema o prompt della password (inserire la password di sistema)	Assumere il controllo o arrestare il controller compromesso dal controller integro: <code>storage failover takeover -ofnode impaired_node_name</code>  Quando il controller non utilizzato visualizza <code>Waiting for giveback...</code> (in attesa di <code>giveback...</code> ), premere <code>Ctrl-C</code> e rispondere <code>y</code> .

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: Il controller è in una configurazione MetroCluster



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.

Se il controller non utilizzato visualizza...	Quindi...
In attesa di un giveback...	Premere Ctrl-C, quindi rispondere <i>y</i> 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: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code>  Quando il controller non utilizzato visualizza Waiting for giveback... (in attesa di giveback...), premere Ctrl-C e rispondere <i>y</i> .

### Opzione 3: Controller in un MetroCluster a due nodi

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

#### A proposito di questa attività

- Al termine di questa procedura, è necessario lasciare accesi gli alimentatori per alimentare il controller integro.

#### Fasi

- Controllare lo stato MetroCluster per determinare se il controller compromesso è passato automaticamente al controller integro: `metrocluster show`
- A seconda che si sia verificato uno switchover automatico, procedere come indicato nella seguente tabella:

Se il controller è compromesso...	Quindi...
Si è attivata automaticamente	Passare alla fase successiva.
Non si è attivato automaticamente	Eseguire un'operazione di switchover pianificata dal controller integro: <code>metrocluster switchover</code>
Non è stato attivato automaticamente, si è tentato di eseguire lo switchover con <code>metrocluster switchover</code> e lo switchover è stato vetoed	Esaminare i messaggi di veto e, se possibile, risolvere il problema e riprovare. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

- Risincronizzare gli aggregati di dati eseguendo `metrocluster heal -phase aggregates` dal cluster esistente.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

Se la riparazione è vetoed, si ha la possibilità di rimettere il `metrocluster heal` con il `-override -vetoed` parametro. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

4. Verificare che l'operazione sia stata completata utilizzando il comando `MetroCluster Operation show`.

```
controller_A_1::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: 7/25/2016 18:45:55
End Time: 7/25/2016 18:45:56
Errors: -
```

5. Controllare lo stato degli aggregati utilizzando `storage aggregate show` comando.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State    #Vols  Nodes      RAID
Status
-----
...
aggr_b2        227.1GB    227.1GB    0% online      0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Riparare gli aggregati root utilizzando `metrocluster heal -phase root-aggregates` comando.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

Se la riparazione è vetoed, si ha la possibilità di rimettere il `metrocluster heal` comando con il parametro `-override-vetoed`. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

7. Verificare che l'operazione di riparazione sia completa utilizzando `metrocluster operation show` sul cluster di destinazione:

```
mcc1A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: 7/29/2016 20:54:41
End Time: 7/29/2016 20:54:42
Errors: -
```

8. Sul modulo controller guasto, scollegare gli alimentatori.

# Sostituire il supporto di avvio - FAS8200

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.

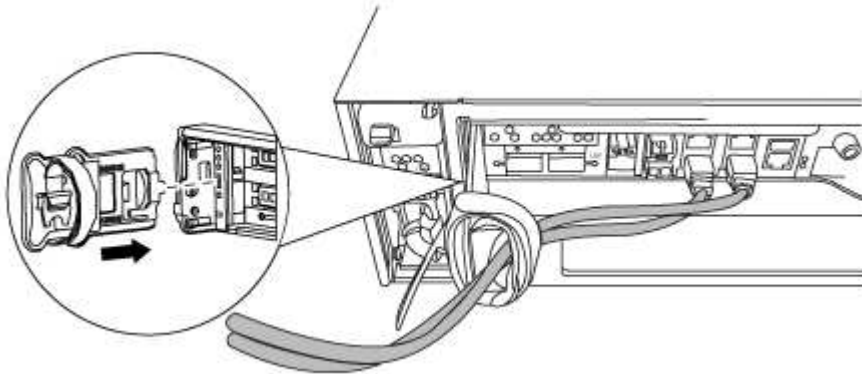
## Fase 1: Rimuovere il controller

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

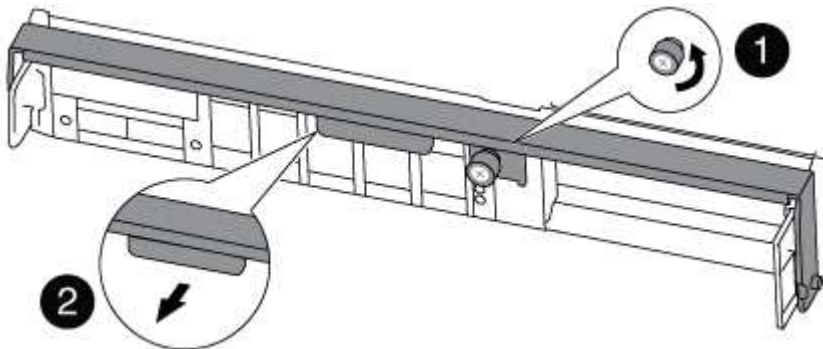
1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Allentare il gancio e la fascetta che fissano i cavi al dispositivo di gestione dei cavi, quindi scollegare i cavi di sistema e gli SFP (se necessario) dal modulo controller, tenendo traccia del punto in cui sono stati collegati i cavi.

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. Rimuovere e mettere da parte i dispositivi di gestione dei cavi dai lati sinistro e destro del modulo controller.



4. Allentare la vite a testa zigrinata sulla maniglia della camma sul modulo controller.



1

Vite a testa zigrinata

2

Maniglia CAM

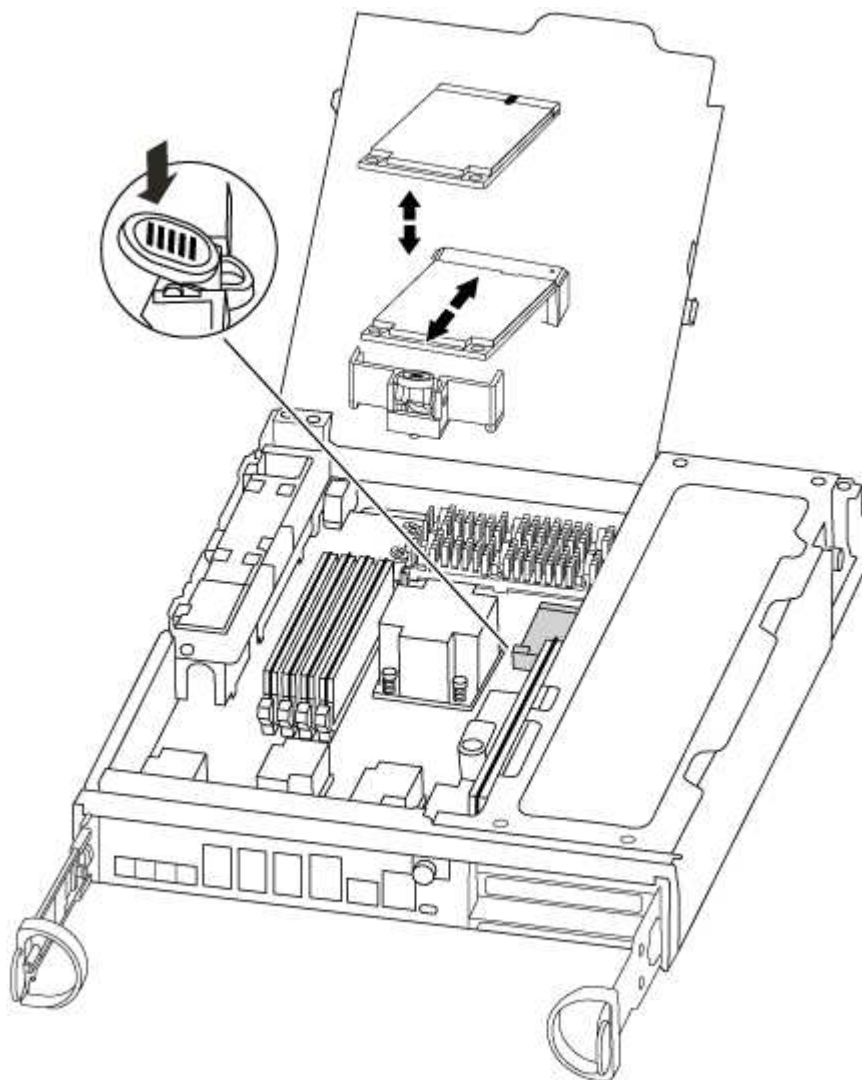
5. Tirare la maniglia della camma verso il basso e iniziare a far scorrere il modulo controller fuori dallo chassis.

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

## Fase 2: Sostituire il supporto di avvio

Individuare il supporto di avvio nel controller e seguire le istruzioni per sostituirlo.

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Individuare il supporto di avvio utilizzando la seguente illustrazione o la mappa FRU sul modulo controller:



3. Premere il pulsante blu sull'alloggiamento del supporto di avvio per rilasciare il supporto di avvio dall'alloggiamento, quindi estrarlo delicatamente dalla presa del supporto di avvio.



Non attorcigliare o tirare il supporto di avvio verso l'alto, in quanto potrebbe danneggiare la presa o il supporto di avvio.

4. Allineare i bordi del supporto di avvio sostitutivo con lo zoccolo del supporto di avvio, quindi spingerlo delicatamente nello zoccolo.
5. Verificare che il supporto di avvio sia inserito correttamente e completamente nella presa.

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

6. Premere il supporto di avvio verso il basso per inserire il pulsante di blocco sull'alloggiamento del supporto di avvio.
7. Chiudere il coperchio del modulo controller.

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

È possibile installare l'immagine di sistema sul supporto di avvio sostitutivo utilizzando un'unità flash USB su cui è installata l'immagine. Tuttavia, è necessario ripristinare il file system var durante questa procedura.

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



Il file tar.gz deve essere collocato in una partizione formattata con FAT32 di almeno 4 GB. Mentre le partizioni FAT32 possono essere grandi fino a 2 TB, i tool integrati di Windows (ad esempio diskpart) non possono formattare partizioni FAT32 di dimensioni superiori a 32 GB.

- 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. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
  - b. 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.
  - c. 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.
  - d. Inserire completamente il modulo controller nel sistema, assicurandosi che la maniglia della camma si allontani dall'unità flash USB, spingere con decisione la maniglia della camma per terminare l'inserimento del modulo controller, spingere la maniglia della camma in posizione chiusa, quindi serrare la vite a testa zigrinata.



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

- e. 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.

- f. 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.

- g. 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.

- h. Se il controller si trova in un MetroCluster esteso o collegato al fabric, è necessario ripristinare la configurazione dell'adattatore FC:

- i. Avvio in modalità di manutenzione: `boot_ontap maint`
- ii. Impostare le porte MetroCluster come iniziatori: `ucadmin modify -m fc -t initiator adapter_name`
- iii. Halt per tornare alla modalità di manutenzione: `halt`

Le modifiche verranno implementate all'avvio del sistema.

## Avviare l'immagine di ripristino - FAS8200

La procedura per avviare il controller compromesso dall'immagine di ripristino dipende dalla configurazione MetroCluster a due nodi del sistema.

## Opzione 1: La maggior parte dei sistemi

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

Questa procedura si applica ai sistemi che non si trovano in una configurazione MetroCluster a due nodi.

### Fasi

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	<ol style="list-style-type: none"><li>a. Premere <code>y</code> quando viene richiesto di ripristinare la configurazione di backup.</li><li>b. Impostare il controller integro su un livello di privilegio avanzato: <code>set -privilege advanced</code></li><li>c. Eseguire il comando di ripristino del backup: <code>system node restore-backup -node local -target-address impaired_node_IP_address</code></li><li>d. Riportare il controller al livello di amministrazione: <code>set -privilege admin</code></li><li>e. Premere <code>y</code> quando viene richiesto di utilizzare la configurazione ripristinata.</li><li>f. Premere <code>y</code> quando viene richiesto di riavviare il controller.</li></ol>
Nessuna connessione di rete	<ol style="list-style-type: none"><li>a. Premere <code>n</code> quando viene richiesto di ripristinare la configurazione di backup.</li><li>b. Riavviare il sistema quando richiesto dal sistema.</li><li>c. Selezionare l'opzione <b>Update flash from backup config</b> (Sync flash) dal menu visualizzato.</li></ol> <p>Se viene richiesto di continuare con l'aggiornamento, premere <code>y</code>.</p>

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.
In attesa di un giveback...	a. Accedere al controller partner. b. Verificare che il controller di destinazione sia pronto per il giveback con <code>storage failover show</code> 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.

## Opzione 2: Controller in un MetroCluster a due nodi

È necessario avviare l'immagine ONTAP dall'unità USB e verificare le variabili ambientali.

Questa procedura si applica ai sistemi in una configurazione MetroCluster a due nodi.

### Fasi

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. Una volta installata l'immagine, avviare il processo di ripristino:
  - a. Premere `n` quando viene richiesto di ripristinare la configurazione di backup.
  - b. Premere `y` quando viene richiesto di riavviare per iniziare a utilizzare il software appena installato.

Quando richiesto, si dovrebbe essere pronti ad interrompere il processo di avvio.
4. All'avvio del sistema, premere `Ctrl-C` dopo aver visualizzato `Press Ctrl-C for Boot Menu E`

quando viene visualizzato il menu di avvio, selezionare l'opzione 6.

5. Verificare che le variabili ambientali siano impostate come previsto.
  - a. Portare il nodo 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.
  - e. Riavviare il nodo.

## Switch back aggregates in una configurazione MetroCluster a due nodi - FAS8200

Una volta completata la sostituzione dell'unità FRU in una configurazione MetroCluster a due nodi, è possibile eseguire l'operazione di switchback dell'unità MetroCluster. In questo modo, la configurazione torna al suo normale stato operativo, con le macchine virtuali dello storage di origine sincronizzata (SVM) sul sito precedentemente compromesso ora attive e che forniscono i dati dai pool di dischi locali.

Questa attività si applica solo alle configurazioni MetroCluster a due nodi.

### Fasi

1. Verificare che tutti i nodi si trovino in `enabled` stato: `metrocluster node show`

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
      controller_A_1 configured      enabled      heal roots
completed
      cluster_B
      controller_B_1 configured      enabled      waiting for
switchback recovery
2 entries were displayed.
```

2. Verificare che la risincronizzazione sia completa su tutte le SVM: `metrocluster vserver show`
3. Verificare che tutte le migrazioni LIF automatiche eseguite dalle operazioni di riparazione siano state completate correttamente: `metrocluster check lif show`
4. Eseguire lo switchback utilizzando `metrocluster switchback` comando da qualsiasi nodo del cluster esistente.
5. Verificare che l'operazione di switchback sia stata completata: `metrocluster show`

L'operazione di switchback è ancora in esecuzione quando un cluster si trova in `waiting-for-switchback` stato:

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured      switchover
Remote: cluster_A configured      waiting-for-switchback
```

L'operazione di switchback è completa quando i cluster si trovano in `normal` stato:

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured      normal
Remote: cluster_A configured      normal
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando `metrocluster config-replication resync-status show` comando.

6. Ripristinare le configurazioni SnapMirror o SnapVault.

## Ripristinare OKM, NSE e NVE secondo necessità - FAS8200

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: <code>boot_ontap menu</code>
In attesa di un giveback...	<ol style="list-style-type: none"> <li>Invio <code>Ctrl-C</code> quando richiesto</li> <li>Quando viene visualizzato il messaggio: Arrestare il controller invece di attendere <code>[y/n]?</code> , inserire: <code>y</code></li> <li>Al prompt DEL CARICATORE, immettere <code>boot_ontap menu</code> comando.</li> </ol>

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:

[illegible]

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...	<ol style="list-style-type: none"><li>a. Accedere al controller partner.</li><li>b. Verificare che il controller di destinazione sia pronto per il giveback con <code>storage failover show</code> comando.</li></ol>

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.
In attesa di un giveback...	<ul style="list-style-type: none"> <li>a. Accedere al controller partner.</li> <li>b. Verificare che il controller di destinazione sia pronto per il giveback con <code>storage failover show</code> comando.</li> </ul>

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. Se AutoSupport è attivato, ripristinare/riattivare la creazione automatica dei casi utilizzando `system node autosupport invoke -node * -type all -message MAINT=END`

## Restituire il componente guasto a NetApp - FAS8200

Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit. Vedere ["Parti restituite sostituzioni"](#) per ulteriori informazioni.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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