



Supporto di boot

Install and maintain

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems/a320/bootmedia-replace-overview.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Sommario

- Supporto di boot 1
 - Panoramica della sostituzione dei supporti di avvio - AFF A320 1
 - Controllare le chiavi di crittografia integrate - AFF A320 1
 - Spegnere il nodo - AFF A320 5
 - Sostituire il supporto di avvio - AFF A320 7
 - Avviare l'immagine di ripristino - AFF A320 11
 - Ripristinare OKM, NSE e NVE secondo necessità - AFF A320 14
 - Restituire il componente guasto a NetApp - AFF A320 18

Supporto di boot

Panoramica della sostituzione dei supporti di avvio - AFF A320

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 le chiavi di crittografia integrate - AFF A320

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

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. Spegnerne 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. Spegnerne 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 nodo - AFF A320

Dopo aver completato le attività NVE o NSE, è necessario completare la chiusura del nodo compromesso. Arrestare o sostituire il controller con problemi utilizzando la procedura appropriata per la configurazione.

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

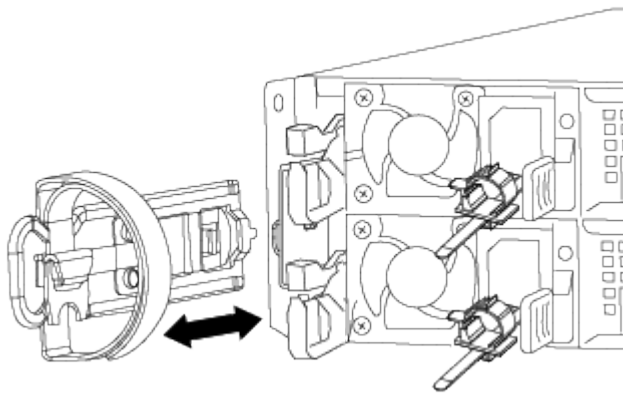
Sostituire il supporto di avvio - AFF A320

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

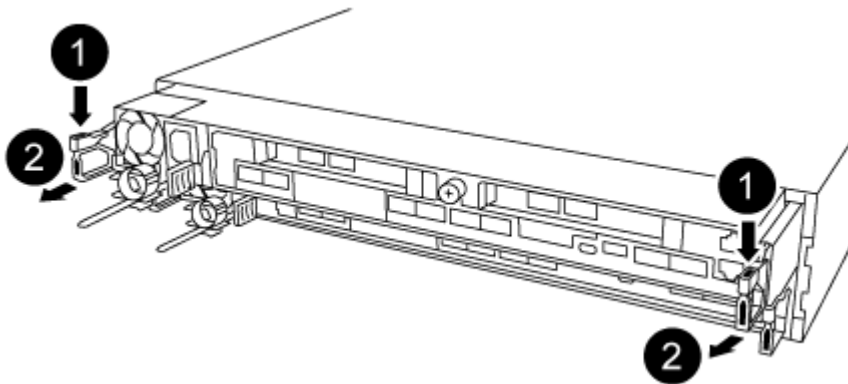
Per accedere ai componenti all'interno del modulo controller, è necessario rimuovere il modulo controller dallo chassis.

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Scollegare l'alimentazione del modulo controller dalla fonte di alimentazione.
3. 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.

4. Rimuovere e mettere da parte i dispositivi di gestione dei cavi dai lati sinistro e destro del modulo controller.
5. Rimuovere il modulo controller dal telaio:



- a. Inserire l'indice nel meccanismo di blocco su entrambi i lati del modulo controller.
- b. Premere verso il basso la linguetta arancione sulla parte superiore del meccanismo di chiusura fino a liberare il perno di chiusura sul telaio.

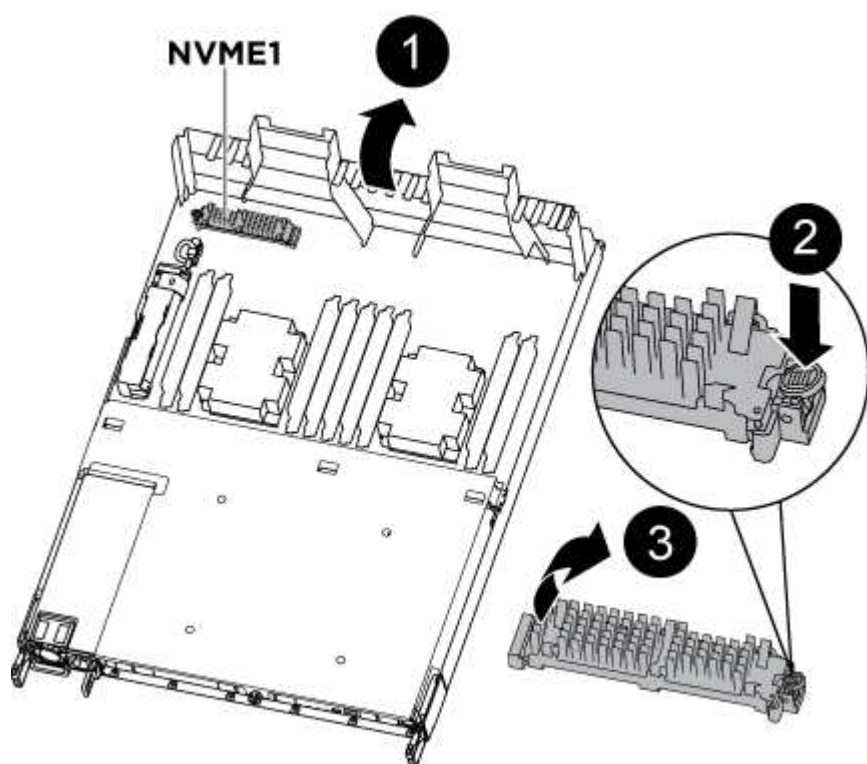
Il gancio del meccanismo di chiusura deve essere quasi verticale e non deve essere lontano dal perno del telaio.

- c. Tirare delicatamente il modulo controller di alcuni pollici verso di sé in modo da poter afferrare i lati del modulo controller.
- d. Con entrambe le mani, estrarre delicatamente il modulo controller dal telaio e posizionare il modulo su una superficie piana e stabile.

Fase 2: Sostituire il supporto di avvio

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

1. Aprire il condotto dell'aria e individuare il supporto di avvio utilizzando la seguente illustrazione o la mappa FRU sul modulo del controller:
2. Individuare e rimuovere il supporto di avvio dal modulo controller:



- a. Premere il tasto blu alla fine del supporto di avvio fino a quando il labbro sul supporto di avvio non scompare dal pulsante blu.
- b. Ruotare il supporto di avvio verso l'alto ed estrarre delicatamente il supporto di avvio dalla presa.
 - i. Verificare che il supporto di avvio sia inserito correttamente e completamente nella presa.

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

3. Bloccare il supporto di avvio in posizione:
 - a. Ruotare il supporto di avvio verso il basso verso la scheda madre.
 - b. Posizionando un dito alla fine del supporto di avvio tramite il pulsante blu, premere l'estremità del supporto di avvio per attivare il pulsante di blocco blu.
 - c. Tenendo premuto il supporto di avvio, sollevare il pulsante di blocco blu per bloccare il supporto di avvio in posizione.

4. Chiudere il condotto dell'aria.

Fase 3: Trasferire l'immagine di avvio sul supporto di avvio utilizzando un'unità flash USB

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.
 - i. Scarica l'immagine del servizio nel tuo spazio di lavoro sul laptop.
 - ii. 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

- iii. 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.

- iv. Rimuovere l'unità flash USB dal computer portatile.

- b. In caso contrario, chiudere il condotto dell'aria.
- c. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
- d. Reinstallare il dispositivo di gestione dei cavi e rieseguire il sistema secondo necessità.

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

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

g. Completare la reinstallazione del modulo controller:

- i. Assicurarsi che i bracci del dispositivo di chiusura siano bloccati in posizione estesa.
- ii. Utilizzando i bracci del dispositivo di chiusura, spingere il modulo controller nell'alloggiamento dello chassis fino a quando non si arresta.



Non spingere verso il basso il meccanismo di chiusura sulla parte superiore dei bracci del dispositivo di chiusura. Per farlo, sollevare il meccanismo di blocco e impedire lo scorrimento del modulo controller nel telaio.

- iii. Tenere premuti le linguette arancioni sulla parte superiore del meccanismo di chiusura.
- iv. Spingere delicatamente il modulo controller nell'alloggiamento dello chassis fino a quando non è a filo con i bordi dello chassis.



I bracci del meccanismo di chiusura scorrono nel telaio.

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

- i. Rilasciare i fermi per bloccare il modulo controller in posizione.
- ii. Se non è già stato fatto, reinstallare il dispositivo di gestione dei cavi.
 - a. Interrompere il processo di avvio premendo Ctrl-C per interrompere il PROCESSO al prompt DEL CARICATORE.

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


- b. Dal prompt DEL CARICATORE, avviare l'immagine di ripristino dall'unità flash USB:

```
boot_recovery
```

L'immagine viene scaricata dall'unità flash USB.

- c. Quando richiesto, inserire il nome dell'immagine o accettare l'immagine predefinita visualizzata tra parentesi sullo schermo.
 - d. Una volta installata l'immagine, avviare il processo di ripristino:
 - iii. Registrare l'indirizzo IP del nodo con problemi visualizzato sullo schermo.
 - iv. Premere `y` quando viene richiesto di ripristinare la configurazione di backup.
 - v. Premere `y` quando viene richiesto di sovrascrivere `/etc/ssh/ssh_host_dsa_key`.
 - a. Dal nodo partner nel livello di privilegio avanzato, avviare la sincronizzazione della configurazione utilizzando l'indirizzo IP registrato nel passaggio precedente: `system node restore-backup -node local -target-address impaired_node_IP_address`
 - b. Se il ripristino ha esito positivo, premere `y` sul nodo non utilizzato quando viene richiesto di utilizzare la copia ripristinata?.
 - c. Premere `y` quando viene visualizzato il messaggio `confirm backup procedure was successful` (conferma procedura di backup riuscita), quindi premere `y` quando viene richiesto di riavviare il nodo.

- d. Verificare che le variabili ambientali siano impostate come previsto.
 - vi. Portare il nodo al prompt DEL CARICATORE.
- Dal prompt di ONTAP, è possibile eseguire il comando `system node halt -skip-lif-migration-before-shutdown true -ignore-quorum-warnings true -inhibit-takeover true`.
- vii. Controllare le impostazioni delle variabili di ambiente con `printenv` comando.
 - viii. Se una variabile di ambiente non è impostata come previsto, modificarla con `setenv environment-variable-name changed-value` comando.
 - ix. Salvare le modifiche utilizzando `savenv` comando.
 - x. Riavviare il nodo.
 - a. Con il nodo con problemi riavviati che visualizza `Waiting for giveback...` eseguire un giveback dal nodo integro:

Se il sistema è in...	Quindi...
Una coppia ha	<p>Dopo che il nodo non ha superato la visualizzazione di <code>Waiting for giveback...</code> eseguire un giveback dal nodo integro:</p> <ul style="list-style-type: none"> i. Dal nodo integro: <code>storage failover giveback -ofnode partner_node_name</code> <p>Il nodo compromesso recupera lo storage, termina l'avvio, quindi si riavvia e viene nuovamente sostituito dal nodo integro.</p> <div style="display: flex; align-items: center;">  <div> <p>Se il giveback viene vetoed, puoi prendere in considerazione la possibilità di ignorare i veti.</p> </div> </div> <p>"Gestione delle coppie HA"</p> <ul style="list-style-type: none"> ii. Monitorare l'avanzamento dell'operazione di giveback utilizzando <code>storage failover show-giveback</code> comando. iii. Una volta completata l'operazione di giveback, verificare che la coppia ha sia in buone condizioni e che sia possibile effettuare il takeover utilizzando <code>storage failover show</code> comando. iv. Ripristinare il giveback automatico se è stato disattivato utilizzando il comando di modifica del failover dello storage.

- b. Uscire dal livello di privilegio avanzato sul nodo integro.

Avviare l'immagine di ripristino - AFF A320

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

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

L'immagine viene scaricata dall'unità flash USB.

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

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

Se il sistema dispone di...	Quindi...
Nessuna connessione di rete e si trova in una configurazione MetroCluster IP	<p>a. Premere n quando viene richiesto di ripristinare la configurazione di backup.</p> <p>b. Riavviare il sistema quando richiesto dal sistema.</p> <p>c. Attendere che le connessioni dello storage iSCSI si connettano.</p> <p>È possibile procedere dopo aver visualizzato i seguenti messaggi:</p> <pre> 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). 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). 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). 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).</pre> <p>d. Selezionare l'opzione Update flash from backup config (Sync flash) dal menu visualizzato.</p> <p>Se viene richiesto di continuare con l'aggiornamento, premere y.</p>

4. Assicurarsi che le variabili ambientali siano impostate come previsto:

- Portare il nodo al prompt DEL CARICATORE.
- Controllare le impostazioni delle variabili di ambiente con `printenv` comando.
- Se una variabile di ambiente non è impostata come previsto, modificarla con `setenv environment_variable_name changed_value` comando.
- 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 [Fasi di sostituzione dei supporti post-boot per OKM, NSE e NVE](#)

- 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 nodo partner. b. Verificare che il nodo di destinazione sia pronto per il giveback con <code>storage failover show</code> comando.

7. Collegare il cavo della console al nodo partner.

8. Restituire il nodo 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 nodo 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 A320

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: <code>boot_ontap menu</code>
In attesa di un giveback	<ul style="list-style-type: none">a. Invio <code>Ctrl-C</code> quando richiestob. Quando viene visualizzato il messaggio: Interrompere questo nodo invece di attendere <code>[y/n]?</code> , inserire: <code>y</code>c. Al prompt DEL CARICATORE, immettere <code>boot_ontap menu</code> 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-----
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----- FINE BACKUP-----
```

7. Nel menu di avvio, selezionare l'opzione Normal Boot (Avvio normale).
Il sistema si avvia in attesa di 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. 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.

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.

- 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.

13. Spostare il cavo della console sul controller partner.

14. Restituire il controller di destinazione utilizzando `storage failover giveback -fromnode local` comando.

15. 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.

16. 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.

17. Spostare il cavo della console sul controller di destinazione ed eseguire `version -v` Per controllare le versioni di ONTAP.

18. 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...	<ol style="list-style-type: none"> a. Accedere al controller partner. b. Verificare che il controller di destinazione sia pronto per il giveback con <code>storage failover show</code> 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 A320

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.