



Supporto di boot

Install and maintain

NetApp
December 18, 2024

Sommario

- Supporto di boot 1
 - Flusso di lavoro per la sostituzione dei supporti di avvio - AFF C80 1
 - Requisiti di sostituzione dei supporti di avvio - AFF C80 1
 - Verificare il supporto e lo stato della chiave di crittografia - AFF C80 2
 - Spegnimento del controller con problemi - AFF C80 6
 - Sostituire il supporto di avvio - AFF C80 8
 - Avviare l'immagine di ripristino - AFF C80 12
 - Ripristinare la crittografia - AFF C80 14
 - Restituire il componente guasto a NetApp - AFF C80 23

Supporto di boot

Flusso di lavoro per la sostituzione dei supporti di avvio - AFF C80

Per sostituire i supporti di avvio, attenersi alla procedura riportata di seguito.

1

"Esaminare i requisiti dei supporti di avvio"

Esaminare i requisiti per la sostituzione dei supporti di avvio.

2

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

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

3

"Spegnere il controller compromesso"

Spegnere o sostituire il controller danneggiato in modo che il controller integro continui a fornire dati dalla memoria del controller danneggiato.

4

"Sostituire il supporto di avvio"

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

5

"Avviare l'immagine di ripristino"

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

6

"Ripristino della crittografia"

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

7

"Restituire la parte guasta a NetApp"

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

Requisiti di sostituzione dei supporti di avvio - AFF C80

Prima di sostituire il supporto di avvio, verificare i seguenti requisiti.

- È necessario disporre di un'unità flash USB, formattata in FAT32, con la quantità di storage appropriata per contenere `image_XXX.tgz` file.

- È necessario copiare il `image_xxx.tgz` file nell'unità flash USB per utilizzarlo successivamente in questa procedura.
- È necessario sostituire il componente guasto con un componente FRU sostitutivo ricevuto dal provider.
- È importante applicare i comandi descritti di seguito al controller corretto:
 - Il controller *alterato* è il controller su cui si esegue la manutenzione.
 - Il controller *healthy* è il partner ha del controller compromesso.

Verificare il supporto e lo stato della chiave di crittografia - AFF C80

Prima di spegnere il controller danneggiato, verifica che la tua versione di ONTAP supporti la crittografia dei volumi NetApp (NVE) e che il tuo sistema di gestione delle chiavi sia configurato correttamente.

Passaggio 1: Verificare che la versione di ONTAP in uso supporti la crittografia dei volumi NetApp

Verifica se la versione di ONTAP in uso supporta la crittografia dei volumi di NetApp (NVE). Queste informazioni sono fondamentali per scaricare l'immagine ONTAP corretta.

1. Per determinare se la versione di ONTAP in uso supporta la crittografia, eseguire il seguente comando:

```
version -v
```

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

2. In base al supporto di NVE sul tuo sistema, esegui una delle seguenti azioni:
 - Se NVE è supportato, scarica l'immagine ONTAP con crittografia dei volumi di NetApp.
 - Se NVE non è supportato, scaricare l'immagine ONTAP **senza** crittografia del volume NetApp.

Fase 2: Determinare se è possibile arrestare il controller in modo sicuro

Per arrestare in modo sicuro un controller, identificare prima se il gestore chiavi esterno (EKM) o il gestore chiavi integrato (OKM) è attivo. Quindi, verificare il gestore delle chiavi in uso, visualizzare le informazioni sulla chiave appropriate ed eseguire le azioni necessarie in base allo stato delle chiavi di autenticazione.

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

Versione di ONTAP	Eeguire questo comando
ONTAP 9.14.1 o versione successiva	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"> • Se EKM è attivato, EKM viene elencato nell'output del comando. • Se OKM è attivato, OKM viene elencato nell'output del comando. • Se nessun gestore di chiavi è attivato, <code>No key manager keystores configured</code> viene elencato nell'output del comando.

Versione di ONTAP	Eeguire questo comando
ONTAP 9.13.1 o versioni precedenti	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> • Se EKM è attivato, <code>external</code> viene elencato nell'output del comando. • Se OKM è attivato, <code>onboard</code> viene elencato nell'output del comando. • Se nessun gestore di chiavi è attivato, <code>No key managers configured</code> viene elencato nell'output del comando.

2. Selezionare una delle seguenti opzioni a seconda che sia configurato un gestore di chiavi sul sistema.

Nessun gestore delle chiavi configurato

È possibile arrestare il controller danneggiato in modo sicuro. Andare a ["spegnere il controller danneggiato"](#).

Gestore chiavi esterno o integrato configurato

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

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

- Controllare l'output per il valore nella `Restored` colonna per il gestore delle chiavi.

Questa colonna indica se le chiavi di autenticazione per il gestore delle chiavi (EKM o OKM) sono state ripristinate correttamente.

3. A seconda che il sistema utilizzi il gestore chiavi esterno o il gestore chiavi integrato, selezionare una delle seguenti opzioni.

Gestore chiavi esterno

A seconda del valore di output visualizzato nella `Restored` colonna, seguire la procedura appropriata.

Valore di output in <code>Restored</code> colonna	Attenersi alla procedura descritta di seguito...
<code>true</code>	È possibile arrestare il controller danneggiato in modo sicuro. Andare a "spegnere il controller danneggiato" .
Altro <code>true</code>	<p>a. Ripristinare le chiavi di autenticazione della gestione delle chiavi esterne in tutti i nodi del cluster utilizzando il seguente comando:</p> <pre>security key-manager external restore</pre> <p>Se il comando non riesce, contattare "Supporto NetApp".</p> <p>b. Verificare che la <code>Restored</code> colonna visualizzata <code>true</code> per tutte le chiavi di autenticazione immettendo il <code>`security key-manager key query`</code> comando.</p> <p>Se tutte le chiavi di autenticazione sono <code>true</code>, è possibile arrestare il controller danneggiato in modo sicuro. Andare a "spegnere il controller danneggiato".</p>

Gestione delle chiavi integrata

A seconda del valore di output visualizzato nella `Restored` colonna, seguire la procedura appropriata.

**Valore di output in Restored
colonna**

true

Attenersi alla procedura descritta di seguito...

Eseguire manualmente il backup delle informazioni OKM.

- a. Accedere alla modalità avanzata immettendo `set -priv advanced` e quindi immettere `Y` quando richiesto.
- b. Immettere il seguente comando per visualizzare le informazioni sulla 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. È possibile arrestare il controller danneggiato in modo sicuro. Andare a "[spegnere il controller danneggiato](#)".

Valore di output in Restored colonna	Attenersi alla procedura descritta di seguito...
Altro true	<p>a. Immettere il comando di sincronizzazione del gestore delle chiavi di sicurezza integrato:</p> <pre>security key-manager onboard sync</pre> <p>b. Immettere la passphrase di gestione della chiave integrata alfanumerica di 32 caratteri quando richiesto.</p> <p>Se non è possibile fornire la passphrase, contattare "Supporto NetApp".</p> <p>c. Verificare che venga visualizzata la Restored colonna true per tutte le chiavi di autenticazione:</p> <pre>security key-manager key query</pre> <p>d. Verificare che il Key Manager tipo sia visualizzato onboard, quindi eseguire manualmente il backup delle informazioni OKM.</p> <p>e. Immettere il comando per visualizzare le informazioni di backup per la gestione delle chiavi:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log.</p> <p>Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.</p> <p>g. È possibile arrestare il controller danneggiato in modo sicuro. Andare a "spegnere il controller danneggiato".</p>

Spegnimento del controller con problemi - AFF C80

Arrestare il controller danneggiato utilizzando la procedura appropriata per la configurazione.

Opzione 1: La maggior parte dei sistemi

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

A proposito di questa attività

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

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

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

Fasi

1. Se AutoSupport è attivato, sospendere la creazione automatica dei casi richiamando un messaggio AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=<# of hours>h`

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

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

2. Disattivare il giveback automatico dalla console del controller integro: `storage failover modify -node local -auto-giveback false`



Quando viene visualizzato *Vuoi disattivare il giveback automatico?*, inserisci *y*.

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 <i>y</i> quando richiesto.
Prompt di sistema o prompt della password	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 <i>Waiting for giveback...</i> (in attesa di giveback...), premere Ctrl-C e rispondere <i>y</i> .

Opzione 2: Controller in un MetroCluster

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

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

Fasi

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

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

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

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

2. 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:

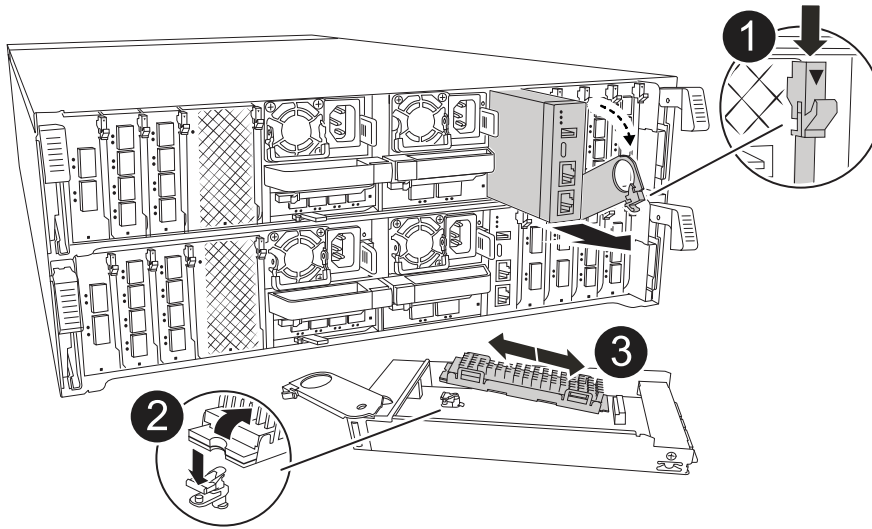
Se il controller non utilizzato visualizza...	Quindi...
Il prompt DEL CARICATORE	Passare alla sezione successiva.
In attesa di un giveback...	Premere Ctrl-C, quindi rispondere <i>y</i> quando richiesto.
Prompt di sistema o prompt della password (inserire la password di sistema)	Assumere il controllo 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 <code>Waiting for giveback...</code> (in attesa di <code>giveback...</code>), premere Ctrl-C e rispondere <i>y</i> .

Sostituire il supporto di avvio - AFF C80

È necessario scollegare il modulo controller, rimuovere il modulo di gestione del sistema dal retro del sistema, rimuovere il supporto di avvio danneggiato e installare il supporto di avvio sostitutivo nel modulo di gestione del sistema.

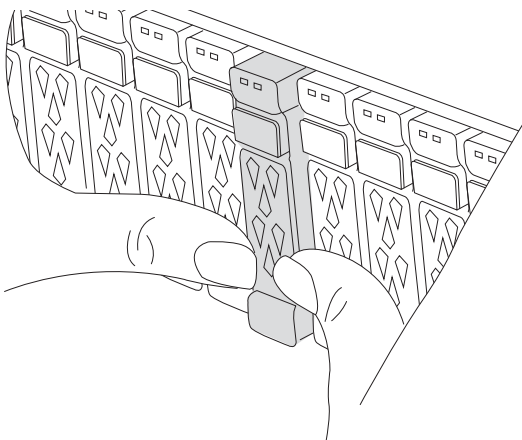
Fase 1: Sostituire il supporto di avvio

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



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

1. Nella parte anteriore dello chassis, premere con decisione ciascun disco fino a quando non si avverte un arresto positivo. In questo modo, i dischi sono posizionati saldamente sulla scheda intermedia dello chassis.



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

3. Scollegare l'alimentazione al modulo controller estraendo il modulo controller di circa tre pollici:

- a. Premere verso il basso entrambi i fermi di bloccaggio del modulo controller, quindi ruotare entrambi i fermi contemporaneamente verso il basso.

- b. Estrarre il modulo controller di circa 3 pollici dal telaio per disinserire l'alimentazione.
 - c. Rimuovere tutti i cavi collegati al modulo di gestione del sistema. Assicurarsi di etichettare il punto in cui sono stati collegati i cavi, in modo da poterli collegare alle porte corrette quando si reinstalla il modulo.
 - d. Ruotare il vassoio di gestione dei cavi verso il basso tirando i pulsanti su entrambi i lati all'interno del vassoio di gestione dei cavi, quindi ruotare il vassoio verso il basso.
 - e. Premere il pulsante della camma di gestione del sistema. La leva della camma si allontana dal telaio.
 - f. Ruotare la leva della camma completamente verso il basso e rimuovere il modulo di gestione del sistema dal modulo controller.
 - g. Posizionare il modulo di gestione del sistema su un tappetino antistatico, in modo che il supporto di avvio sia accessibile.
4. Rimuovere il supporto di avvio dal modulo di gestione:
 - a. Premere il pulsante di bloccaggio blu.
 - b. Ruotare il supporto di avvio verso l'alto, farlo scorrere fuori dallo zoccolo e metterlo da parte.
 5. Installare il supporto di avvio sostitutivo nel modulo di gestione del sistema:
 - a. Allineare i bordi del supporto di avvio con l'alloggiamento dello zoccolo, quindi spingerlo delicatamente a squadra nello zoccolo.
 - b. Ruotare il supporto di avvio verso il basso verso il pulsante di bloccaggio.
 - c. Premere il pulsante di bloccaggio, ruotare completamente il supporto di avvio e rilasciare il pulsante di bloccaggio.
 6. Reinstallare il modulo di gestione del sistema:
 - a. Ruotare il vassoio di gestione dei cavi verso l'alto fino alla posizione di chiusura.
 - b. Eseguire il richiamo del modulo Gestione del sistema.

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

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

Prima di iniziare

- È necessario disporre di un'unità flash USB, formattata con FAT32, con almeno 4 GB di capacità.
- Scaricare una copia della stessa versione dell'immagine di ONTAP del controller danneggiato in esecuzione. Puoi scaricare l'immagine appropriata dalla sezione Downloads del sito di supporto NetApp. USA il `version -v` comando per visualizzare se la tua versione di ONTAP supporta NVE. Se viene visualizzato il comando output `<10no- DARE>`, la versione di ONTAP non supporta NVE.
 - Se NVE è supportato dalla tua versione di ONTAP, scarica l'immagine con crittografia dei volumi di NetApp, come indicato nel pulsante di download.
 - Se NVE non è supportato, scaricare l'immagine senza crittografia dei volumi di NetApp, come indicato nel pulsante di download.
- Se il sistema è una coppia ha, è necessario disporre di una connessione di rete tra le porte di gestione dei nodi dei controller (in genere le interfacce e0M).

Fasi

1. Scaricare e copiare l'immagine di servizio appropriata da "[Sito di supporto NetApp](#)" nell'unità flash USB.
 - a. Scaricare l'immagine del servizio dal collegamento Download nella pagina, nello spazio di lavoro del computer portatile.
 - b. Decomprimere l'immagine del servizio.



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

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

- a. Rimuovere l'unità flash USB dal computer portatile.
2. Inserire l'unità flash USB nella porta USB-A del modulo di gestione del sistema.

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

3. Ricollegare l'alimentazione al modulo controller:
 - a. Spingere con decisione il modulo controller nello chassis fino a quando non raggiunge la scheda intermedia e non è completamente inserito.

I fermi di bloccaggio si sollevano quando il modulo controller è completamente inserito.

- b. Ruotare i fermi di bloccaggio verso l'alto in posizione bloccata.

Il controller inizia ad avviarsi non appena l'alimentazione viene ricollegata al sistema.

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

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

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

- Se si sta configurando DHCP: `ifconfig e0M -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 e0M -addr=filer_addr -mask=netmask -gw=gateway`
 - 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.



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

Avviare l'immagine di ripristino - AFF C80

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

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:

Opzione 1: ONTAP 9.16,0 o versione precedente

- a. Sul controller con problemi, premere `Y` quando viene visualizzato `Do you want to restore the backup configuration now?`
- b. Sul controller danneggiato, premere `Y` quando viene richiesto di sovrascrivere `/etc/ssh/ssh_host_ecdsa_key`.
- c. Sul controller partner sano, impostare il controller con problemi sul livello di privilegi avanzato: `set -privilege advanced`.
- d. Sul controller partner integro, eseguire il comando di ripristino del backup: `system node restore-backup -node local -target-address impaired_node_IP_address`.

NOTA: se viene visualizzato un messaggio diverso da un ripristino riuscito, contattare ["Supporto NetApp"](#).

- e. Sul controller partner sano, riportare il controller danneggiato al livello di amministratore: `set -privilege admin`.
- f. Sul controller con problemi, premere `Y` quando viene visualizzato `Was the restore backup procedure successful?`.
- g. Sul controller con problemi, premere `Y` quando viene visualizzato `...would you like to use this restored copy now?`.
- h. Sul controller danneggiato, premere `Y` quando richiesto per riavviare il controller danneggiato e premere `ctrl-c` per il menu di avvio.
- i. Se il sistema non utilizza la crittografia, selezionare *opzione 1 Avvio normale.*, altrimenti andare a ["Ripristino della crittografia"](#).

Opzione 2: ONTAP 9.16,1 o versione successiva

- a. Sul controller danneggiato, premere `Y` quando viene richiesto di ripristinare la configurazione di backup.

Una volta completata la procedura di ripristino, questo messaggio viene visualizzato sulla console `-syncflash_partner: Restore from partner complete`.

- b. Sul controller danneggiato, premere `Y` quando richiesto per confermare se il backup di ripristino è stato eseguito correttamente.
- c. Sul controller danneggiato, premere `Y` quando viene richiesto di utilizzare la configurazione ripristinata.
- d. Sul controller danneggiato, premere `Y` quando viene richiesto di riavviare il nodo.
- e. Sul controller danneggiato, premere `Y` quando richiesto per riavviare il controller danneggiato e premere `ctrl-c` per il menu di avvio.
- f. Se il sistema non utilizza la crittografia, selezionare *opzione 1 Avvio normale.*, altrimenti andare a ["Ripristino della crittografia"](#).

4. Collegare il cavo della console al controller partner.
5. Restituire il controller utilizzando `storage failover giveback -fromnode local` comando.
6. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node`

`local -auto-giveback true` comando.

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

NOTA: se il processo non riesce, contattare ["Supporto NetApp"](#).

Ripristinare la crittografia - AFF C80

Ripristinare la crittografia sul supporto di avvio sostitutivo.

È necessario completare i passaggi specifici per i sistemi che hanno attivato Gestione chiavi integrato (OKM), crittografia storage NetApp (NSE) o crittografia del volume NetApp (NVE) utilizzando le impostazioni acquisite all'inizio della procedura di sostituzione dei supporti di avvio.

A seconda di quale gestore di chiavi è configurato sul sistema, selezionare una delle seguenti opzioni per ripristinarlo dal menu di avvio.

- ["Opzione 1: Ripristinare la configurazione di Onboard Key Manager"](#)
- ["Opzione 2: Ripristinare la configurazione di External Key Manager"](#)

Opzione 1: Ripristinare la configurazione di Onboard Key Manager

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

Prima di iniziare

- Durante il ripristino della configurazione OKM, assicurarsi di disporre delle seguenti informazioni:
 - Passphrase a livello di cluster immessa ["consentendo la gestione delle chiavi integrata"](#).
 - ["Informazioni di backup per il Key Manager integrato"](#).
- Eseguire la ["Come verificare il backup della gestione delle chiavi integrata e la passphrase a livello del cluster"](#) procedura prima di procedere.

Fasi

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

Versione di ONTAP	Selezionare questa opzione
ONTAP 9.8 o versione successiva	<p data-bbox="621 153 938 191">Selezionare l'opzione 10.</p> <p data-bbox="621 222 1081 260">Mostra un esempio di menu di avvio</p> <div data-bbox="654 296 1456 1079" style="border: 1px solid #ccc; padding: 10px;"><p data-bbox="683 331 1295 369">Please choose one of the following:</p><ul data-bbox="683 411 1370 1010" style="list-style-type: none"><li data-bbox="683 411 971 449">(1) Normal Boot.<li data-bbox="683 453 1133 491">(2) Boot without /etc/rc.<li data-bbox="683 495 1045 533">(3) Change password.<li data-bbox="683 537 1370 606">(4) Clean configuration and initialize all disks.<li data-bbox="683 611 1154 648">(5) Maintenance mode boot.<li data-bbox="683 653 1328 690">(6) Update flash from backup config.<li data-bbox="683 695 1240 732">(7) Install new software first.<li data-bbox="683 737 971 774">(8) Reboot node.<li data-bbox="683 779 1192 848">(9) Configure Advanced Drive Partitioning.<li data-bbox="683 852 1333 921">(10) Set Onboard Key Manager recovery secrets.<li data-bbox="683 926 1317 995">(11) Configure node for external key management.<p data-bbox="683 1010 1036 1047">Selection (1-11)? 10</p></div>

Versione di ONTAP	Selezionare questa opzione
ONTAP 9.7 e versioni precedenti	<p data-bbox="621 163 1450 195">Selezionare l'opzione nascosta <code>recover_onboard_keymanager</code></p> <p data-bbox="621 233 1078 264">Mostra un esempio di menu di avvio</p> <div data-bbox="654 306 1455 968" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre data-bbox="683 342 1369 930"> Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager </pre> </div>

3. Confermare che si desidera continuare il processo di ripristino.

Mostra prompt di esempio

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

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

Quando si inserisce la passphrase, la console non visualizza alcun input.

Mostra prompt di esempio

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. Immettere le informazioni di backup.

a. Incollare l'intero contenuto dalla riga `DI BACKUP BEGIN` attraverso la riga di `BACKUP FINALE`.

Mostra prompt di esempio

Enter the backup data:

```
-----BEGIN BACKUP-----  
012345678901234567890123456789012345678901234567890123456789012345678901234567890123  
123456789012345678901234567890123456789012345678901234567890123456789012345678901234  
234567890123456789012345678901234567890123456789012345678901234567890123456789012345  
345678901234567890123456789012345678901234567890123456789012345678901234567890123456  
456789012345678901234567890123456789012345678901234567890123456789012345678901234567  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
012345678901234567890123456789012345678901234567890123456789012345678901234567890123  
123456789012345678901234567890123456789012345678901234567890123456789012345678901234  
234567890123456789012345678901234567890123456789012345678901234567890123456789012345  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
-----END BACKUP-----
```

b. Premere due volte il tasto invio alla fine dell'immissione.

Il processo di ripristino è stato completato.

Mostra prompt di esempio

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

Successfully recovered keymanager secrets.

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



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

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

Mostra prompt di esempio

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

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

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

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

8. Dal nodo partner, eseguire un giveback per il controller partner immettendo il seguente comando.

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

9. Dopo l'avvio con solo l'aggregato CFO, eseguire il comando seguente.

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

10. Immettere la passphrase a livello di cluster per Onboard Key Manager.

Mostra prompt di esempio

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

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



Se la sincronizzazione ha esito positivo, il prompt del cluster viene restituito senza messaggi aggiuntivi. Se la sincronizzazione non riesce, viene visualizzato un messaggio di errore prima di tornare al prompt del cluster. Non continuare fino a quando l'errore non viene corretto e la sincronizzazione non viene eseguita correttamente.

11. Assicurarsi che tutte le chiavi siano sincronizzate immettendo il seguente comando.

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

```
There are no entries matching your query.
```



Nessun risultato dovrebbe comparire quando si filtra per false nel parametro ripristinato.

12. Eseguire il giveback del nodo dal partner immettendo il seguente comando.

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

13. Ripristinare il giveback automatico, se è stato disattivato, immettendo il seguente comando.

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

14. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi immettendo il seguente comando.

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

Opzione 2: Ripristinare la configurazione di External Key Manager

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

Prima di iniziare

Per ripristinare la configurazione di EKM (External Key Manager) sono necessarie le seguenti informazioni.

- Una copia del file `/cfcard/kmip/servers.cfg` da un altro nodo del cluster o le seguenti informazioni:
 - L'indirizzo del server KMIP.
 - Porta KMIP.

- Una copia del `/cfcard/kmip/certs/client.crt` file da un altro nodo cluster o dal certificato client.
- Una copia del `/cfcard/kmip/certs/client.key` file da un altro nodo cluster o dalla chiave client.
- Una copia del `/cfcard/kmip/certs/CA.pem` file da un altro nodo cluster o dalle CA del server KMIP.

Fasi

1. Collegare il cavo della console al controller di destinazione.
2. Selezionare l'opzione 11 dal menu di avvio di ONTAP.

Mostra un esempio di menu di avvio

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

3. Quando richiesto, confermare di aver raccolto le informazioni richieste.

Mostra prompt di esempio

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

4. Quando richiesto, immettere le informazioni relative al client e al server.

Mostra prompt

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Mostra esempio

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk51
MSUwQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpzbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

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

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----END CERTIFICATE-----

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

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

Dopo aver immesso le informazioni sul client e sul server, il processo di ripristino viene completato.

Mostra esempio

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```


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

Mostra prompt di esempio

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

6. Ripristinare il giveback automatico, se è stato disattivato, immettendo il seguente comando.

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

7. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi immettendo il seguente comando.

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

Restituire il componente guasto a NetApp - AFF C80

Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit. Vedere la ["Restituzione e sostituzione delle parti"](#) pagina 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.