



Supporto di avvio - ripristino manuale

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems/asa800/bootmedia-replace-workflow.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Supporto di avvio - ripristino manuale	1
Flusso di lavoro per il ripristino manuale del supporto di avvio - ASA A800	1
Requisiti per il ripristino manuale del supporto di avvio - ASA A800	2
Verificare il supporto e lo stato della chiave di crittografia - ASA A800	2
Passaggio 1: verificare il supporto NVE e scaricare l'immagine ONTAP corretta	3
Passaggio 2: verificare lo stato del gestore delle chiavi ed eseguire il backup della configurazione	3
Arrestare il controller per il ripristino manuale del supporto di avvio - ASA A800	7
Opzione 1: La maggior parte dei sistemi	7
Opzione 2: Il sistema è in un MetroCluster	7
Sostituisci il supporto di avvio e preparati per il ripristino manuale dell'avvio - ASA A800	8
Fase 1: Rimuovere il modulo controller	9
Fase 2: Sostituire il supporto di avvio	11
Fase 3: Trasferire l'immagine di avvio sul supporto di avvio	13
Ripristino manuale del supporto di avvio da un'unità USB - ASA A800	15
Ripristina crittografia - ASA A800	17
Restituisci il supporto di avvio non riuscito a NetApp - ASA A800	27

Supporto di avvio - ripristino manuale

Flusso di lavoro per il ripristino manuale del supporto di avvio - ASA A800

Per iniziare a sostituire il supporto di avvio nel sistema di archiviazione ASA A800, è necessario esaminare i requisiti di sostituzione, controllare lo stato della crittografia, spegnere il controller, sostituire il supporto di avvio, avviare l'immagine di ripristino, ripristinare la crittografia e verificare la funzionalità del sistema.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare ["procedura di ripristino automatico dell'avvio"](#). Se il sistema esegue una versione precedente di ONTAP, è necessario utilizzare la procedura di ripristino manuale all'avvio.

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"

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

3

"Spegnere il controller"

Spegnere il controller quando è necessario sostituire il supporto di avvio.

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 chiavi integrato o del gestore 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 per il ripristino manuale del supporto di avvio - ASA A800

Prima di sostituire il supporto di avvio nel sistema ASA A800, assicurarsi di soddisfare i requisiti necessari per una sostituzione corretta. Questo include la verifica di disporre di un'unità flash USB con la capacità di archiviazione adeguata e di disporre del dispositivo di avvio sostitutivo corretto.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare ["procedura di ripristino automatico dell'avvio"](#). Se il sistema esegue una versione precedente di ONTAP, è necessario utilizzare la procedura di ripristino manuale all'avvio.

Chiavetta USB

- Assicurati di avere una chiavetta USB formattata in FAT32.
- La chiavetta USB deve avere una capacità di archiviazione sufficiente per contenere il `image_xxx.tgz` file.

Preparazione del file

Copia il `image_xxx.tgz` file sull'unità flash USB. Questo file verrà utilizzato quando si trasferisce l'immagine ONTAP tramite l'unità flash USB.

Sostituzione dei componenti

Sostituire il componente guasto con il componente sostitutivo fornito da NetApp.

Identificazione del controllore

Quando si sostituisce il supporto di avvio danneggiato, è fondamentale applicare i comandi al controller corretto:

- Il *controller non funzionante* è il controller su cui si sta eseguendo la manutenzione.
- Il *controllore sano* è il partner HA del controllore compromesso.

Quali sono le prossime novità?

Dopo aver esaminato i requisiti per sostituire il supporto di avvio, è necessario ["controllare il supporto e lo stato della chiave di crittografia sul supporto di avvio"](#).

Verificare il supporto e lo stato della chiave di crittografia - ASA A800

Per garantire la sicurezza dei dati sul sistema di storage ASA A800, è necessario verificare il supporto e lo stato della chiave di crittografia sul supporto di avvio. Verificare se la versione ONTAP supporta NetApp Volume Encryption (NVE) e, prima di arrestare il controller, verificare che il gestore delle chiavi sia attivo.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare ["procedura di ripristino automatico dell'avvio"](#). Se il sistema esegue una versione precedente di ONTAP, è necessario utilizzare la procedura di ripristino manuale all'avvio.

Passaggio 1: verificare il supporto NVE e scaricare l'immagine ONTAP corretta

Determina se la tua versione ONTAP supporta NetApp Volume Encryption (NVE), in modo da poter scaricare l'immagine ONTAP corretta per la sostituzione del supporto di avvio.

Fasi

1. Controlla se la tua versione ONTAP supporta la crittografia:

```
version -v
```

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

2. Scarica l'immagine ONTAP appropriata in base al supporto NVE:
 - Se NVE è supportato: scaricare l'immagine ONTAP con NetApp Volume Encryption
 - Se NVE non è supportato: scaricare l'immagine ONTAP senza NetApp Volume Encryption



Scarica l'immagine ONTAP dal sito di supporto NetApp sul tuo server HTTP o FTP o in una cartella locale. Questo file immagine sarà necessario durante la procedura di sostituzione del supporto di avvio.

Passaggio 2: verificare lo stato del gestore delle chiavi ed eseguire il backup della configurazione

Prima di spegnere il controller danneggiato, verificare la configurazione del gestore delle chiavi ed eseguire il backup delle informazioni necessarie.

Fasi

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

Versione di ONTAP	Eseguire questo comando
ONTAP 9.14.1 o versione successiva	<pre>security key-manager keystore show</pre> • Se EKM è attivato, <code>EKM</code> viene elencato nell'output del comando. • Se OKM è attivato, <code>OKM</code> 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.
ONTAP 9.13.1 o versioni precedenti	<pre>security key-manager show-key-store</pre> • 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. A seconda che sul sistema sia configurato un gestore delle chiavi, procedere in uno dei seguenti modi:

Se non è configurato alcun gestore chiavi:

È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Se è configurato un gestore delle chiavi (EKM o OKM):

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

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

- b. Rivedere l'output e controllare il valore nel `Restored` colonna. Questa colonna indica se le chiavi di autenticazione per il gestore delle chiavi (EKM o OKM) sono state ripristinate correttamente.

3. Completare la procedura appropriata in base al tipo di responsabile delle chiavi:

Gestore chiavi esterno (EKM)

Completare questi passaggi in base al valore nel `Restored` colonna.

Se vengono visualizzate tutte le chiavi `true` nella colonna **Ripristinato**:

È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Se una qualsiasi delle chiavi mostra un valore diverso da `true` nella colonna **Ripristinato**:

- a. Ripristinare le chiavi di autenticazione della gestione delle chiavi esterne su tutti i nodi del cluster:

```
security key-manager external restore
```

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

- b. Verificare che tutte le chiavi di autenticazione siano state ripristinate:

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

Confermare che il `Restored` display a colonna `true` per tutte le chiavi di autenticazione.

- c. Se tutte le chiavi vengono ripristinate, è possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Onboard Key Manager (OKM)

Completare questi passaggi in base al valore nel `Restored` colonna.

Se vengono visualizzate tutte le chiavi `true` nella colonna **Ripristinato**:

- a. Eseguire il backup delle informazioni OKM:

- i. Passa alla modalità privilegio avanzata:

```
set -priv advanced
```

Entra `y` quando ti viene chiesto di continuare.

- i. Visualizza le informazioni di backup della gestione delle chiavi:

```
security key-manager onboard show-backup
```

- ii. Copiare le informazioni di backup in un file separato o nel file di registro.

Queste informazioni di backup saranno necessarie se sarà necessario ripristinare manualmente OKM durante la procedura di sostituzione.

- iii. Torna alla modalità amministratore:

```
set -priv admin
```

- b. È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Se una qualsiasi delle chiavi mostra un valore diverso da `true` nella colonna Ripristinato:

- a. Sincronizzare il gestore delle chiavi integrato:

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

Quando richiesto, immettere la passphrase alfanumerica di 32 caratteri per la gestione delle chiavi integrate.



Questa è la passphrase per l'intero cluster creata durante la configurazione iniziale di Onboard Key Manager. Se non si dispone di questa passphrase, contattare l'assistenza NetApp .

- b. Verificare che tutte le chiavi di autenticazione siano state ripristinate:

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

Confermare che il `Restored display` a colonna `true` per tutte le chiavi di autenticazione e `Key Manager tipo spettacoli onboard` .

- c. Eseguire il backup delle informazioni OKM:

- i. Passa alla modalità privilegio avanzata:

```
set -priv advanced
```

Entra `y` quando ti viene chiesto di continuare.

- i. Visualizza le informazioni di backup della gestione delle chiavi:

```
security key-manager onboard show-backup
```

- ii. Copiare le informazioni di backup in un file separato o nel file di registro.

Queste informazioni di backup saranno necessarie se sarà necessario ripristinare manualmente OKM durante la procedura di sostituzione.

- iii. Torna alla modalità amministratore:

```
set -priv admin
```

- d. È possibile spegnere in sicurezza il controller danneggiato e procedere con la procedura di spegnimento.

Quali sono le prossime novità?

Dopo aver verificato il supporto e lo stato della chiave di crittografia sul supporto di avvio, è necessario ["spegnere il controller"](#).

Arrestare il controller per il ripristino manuale del supporto di avvio - ASA A800

Arrestare il controller danneggiato nel sistema di archiviazione ASA A800 per evitare la perdita di dati e mantenere la stabilità del sistema durante il processo di ripristino automatico del supporto di avvio.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare ["procedura di ripristino automatico dell'avvio"](#). Se il sistema esegue una versione precedente di ONTAP, è necessario utilizzare la procedura di ripristino manuale all'avvio.

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)	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 giveback...), premere Ctrl-C e rispondere <code>y</code>.

Quali sono le prossime novità?

Dopo aver spento il controller, è necessario ["sostituire il supporto di avvio"](#).

Sostituisci il supporto di avvio e preparati per il ripristino manuale dell'avvio - ASA A800

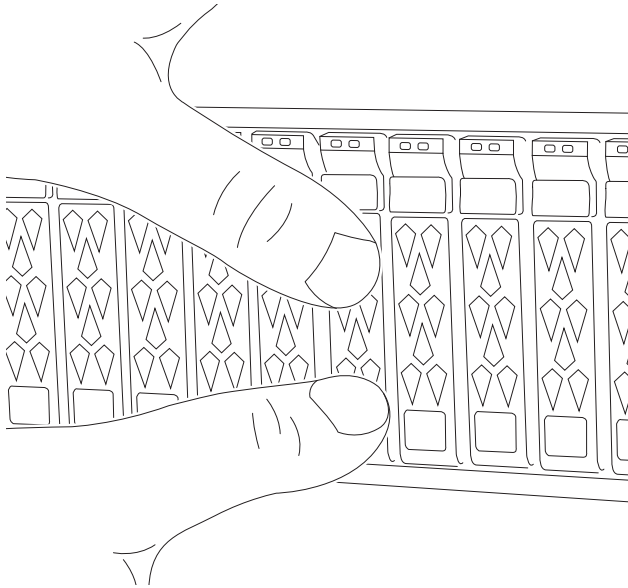
Il supporto di avvio del sistema ASA A800 memorizza i dati essenziali del firmware e della configurazione. La procedura di sostituzione prevede la rimozione del modulo di gestione del sistema, la rimozione del supporto di avvio danneggiato, l'installazione del supporto di avvio sostitutivo e il trasferimento manuale dell'immagine ONTAP sul supporto di avvio sostitutivo tramite un'unità flash USB.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare ["procedura di ripristino automatico dell'avvio"](#). Se il sistema esegue una versione precedente di ONTAP, è necessario utilizzare la procedura di ripristino manuale all'avvio.

Fase 1: Rimuovere il modulo controller

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

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane, utilizzando i pollici per spingere ciascuna unità fino a quando non si avverte un arresto positivo.

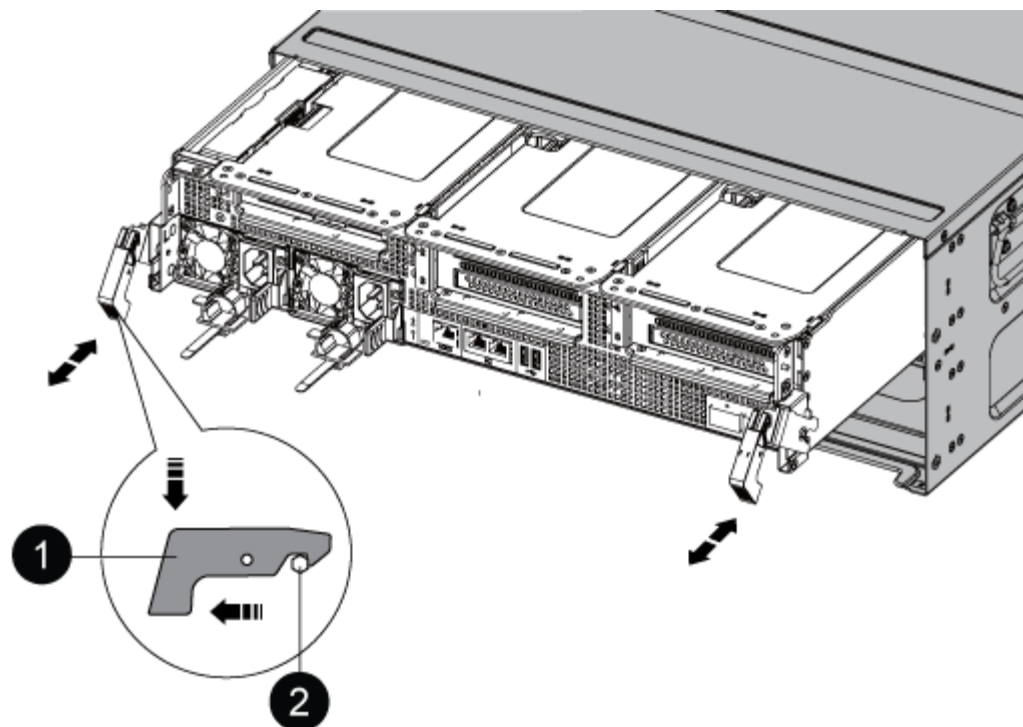


3. Scollegare gli alimentatori del modulo controller dalla fonte di alimentazione.
4. Rilasciare i fermi dei cavi di alimentazione, quindi scollegare i cavi dagli alimentatori.
5. Allentare il gancio e la fascetta che fissano i cavi al dispositivo di gestione dei cavi, quindi scollegare i cavi di sistema e i moduli SFP e QSFP (se necessario) dal modulo controller, tenendo traccia della posizione 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.

6. Rimuovere il dispositivo di gestione dei cavi dal modulo controller e metterlo da parte.
7. Premere verso il basso entrambi i fermi di bloccaggio, quindi ruotare entrambi i fermi verso il basso contemporaneamente.

Il modulo controller si sposta leggermente fuori dallo chassis.



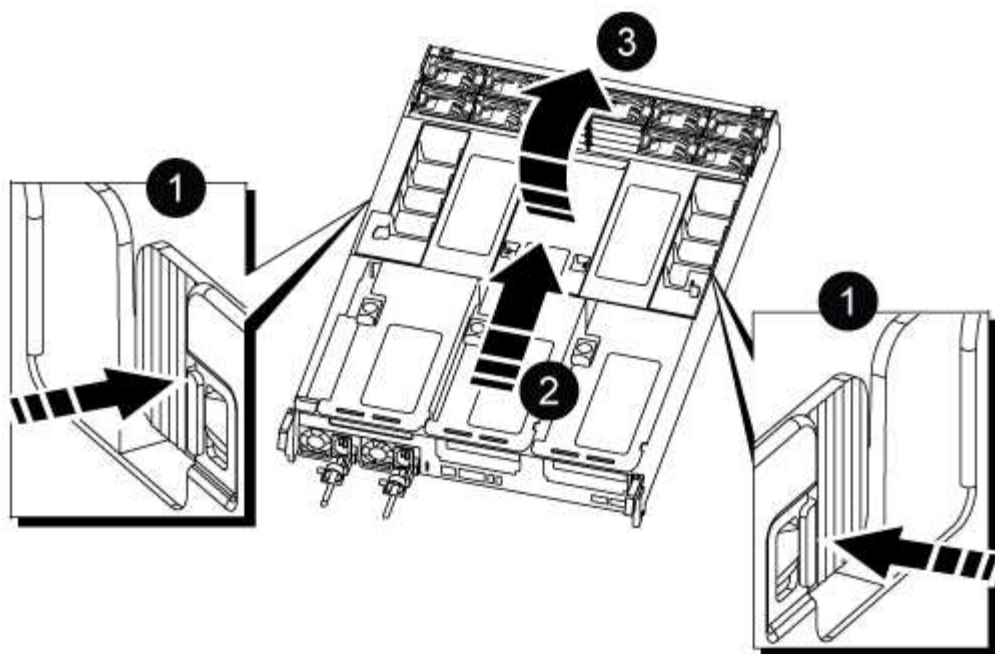
1	Fermo di bloccaggio
2	Perno di bloccaggio

8. Estrarre il modulo controller dal telaio.

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

9. Posizionare il modulo controller su una superficie piana e stabile, quindi aprire il condotto dell'aria:

- a. Premere verso l'interno le linguette di bloccaggio sui lati del condotto dell'aria verso il centro del modulo controller.
- b. Far scorrere il condotto dell'aria verso i moduli delle ventole, quindi ruotarlo verso l'alto fino a portarlo in posizione completamente aperta.



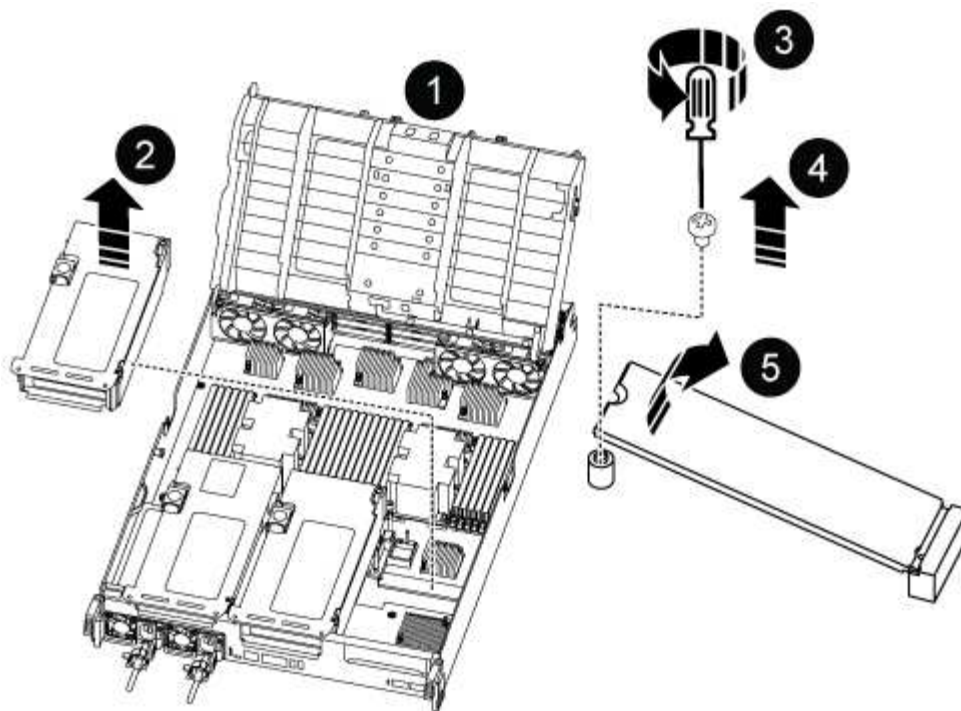
1	Linguette di bloccaggio del condotto dell'aria
2	Far scorrere il condotto dell'aria verso i moduli delle ventole
3	Ruotare il condotto dell'aria verso i moduli delle ventole

Fase 2: Sostituire il supporto di avvio

Individuare il supporto di avvio guasto nel modulo controller rimuovendo il riser 3 sul modulo controller prima di sostituire il supporto di avvio.

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

1. Individuare il supporto di avvio:



1	Condotto dell'aria
2	Riser 3
3	Cacciavite Phillips n. 1
4	Vite del supporto di avvio
5	Supporto di boot

2. Rimuovere il supporto di avvio dal modulo controller:

- Utilizzando un cacciavite Phillips n. 1, rimuovere la vite che fissa il supporto di avvio e mettere da parte la vite in un luogo sicuro.
- Afferrare i lati del supporto di avvio, ruotare delicatamente il supporto di avvio verso l'alto, quindi estrarre il supporto di avvio dalla presa e metterlo da parte.

3. Installare il supporto di avvio sostitutivo nel modulo controller:

- Allineare i bordi del supporto di avvio con l'alloggiamento dello zoccolo, quindi spingerlo delicatamente a squadra nello zoccolo.
- Ruotare il supporto di avvio verso il basso verso la scheda madre.
- Fissare il supporto di avvio alla scheda madre utilizzando la vite del supporto di avvio.

Non serrare eccessivamente la vite per evitare di danneggiare il supporto di avvio.

4. Reinstallare il riser nel modulo controller.

5. Chiudere il condotto dell'aria:

- a. Ruotare il condotto dell'aria verso il basso.
- b. Far scorrere il condotto dell'aria verso i montanti fino a farlo scattare in posizione.

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

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

Prima di iniziare

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

Fasi

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

Il file di immagine del servizio decompresso contiene due cartelle:

- avviare
 - efi
- c. Copiare la cartella efi nella directory principale dell'unità flash USB.

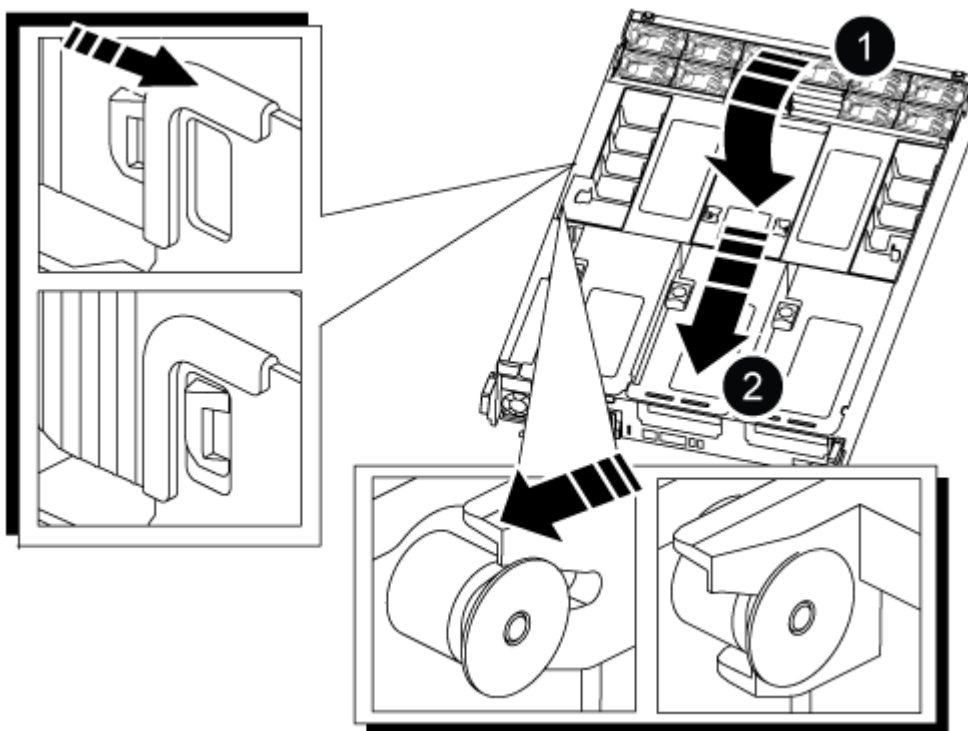


Se l'immagine di servizio non dispone di una cartella efi, vedere "[Cartella EFI mancante dal file di download dell'immagine di servizio utilizzato per il ripristino del dispositivo di avvio per i modelli FAS e AFF^](#)".

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

- d. Rimuovere l'unità flash USB dal computer portatile.
2. In caso contrario, chiudere il condotto dell'aria:
 - a. Ruotare completamente il condotto dell'aria verso il basso fino al modulo controller.

- b. Far scorrere il condotto dell'aria verso i montanti fino a quando le linguette di bloccaggio non scattano in posizione.
- c. Ispezionare il condotto dell'aria per assicurarsi che sia posizionato correttamente e bloccato in posizione.



1	Condotto dell'aria
2	Riser

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

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

5. 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.

6. Spingere delicatamente il modulo controller completamente nel sistema fino a quando i ganci di bloccaggio del modulo controller non iniziano a sollevarsi, spingere con decisione i ganci di bloccaggio per terminare l'alloggiamento del modulo controller, quindi ruotare i ganci di bloccaggio in posizione di blocco sui piedini del modulo controller.
7. Inserire i cavi di alimentazione negli alimentatori, reinstallare il collare di bloccaggio del cavo di alimentazione, quindi collegare gli alimentatori alla fonte di alimentazione.

Il modulo controller inizia ad avviarsi non appena viene ripristinata l'alimentazione. Prepararsi ad interrompere il processo di avvio.

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

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

Quali sono le prossime novità?

Dopo aver sostituito il supporto di avvio, è necessario ["avviare l'immagine di ripristino"](#).

Ripristino manuale del supporto di avvio da un'unità USB - ASA A800

Dopo aver installato il nuovo dispositivo di avvio nel sistema ASA A800 , è possibile avviare l'immagine di ripristino da un'unità USB e ripristinare la configurazione dal nodo partner.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare ["procedura di ripristino automatico dell'avvio"](#) . Se il sistema esegue una versione precedente di ONTAP, è necessario utilizzare la procedura di ripristino manuale all'avvio.

Prima di iniziare

- Assicurati che la tua console sia collegata al controller non compatibile.
- Verifica di avere un'unità flash USB con l'immagine di ripristino.
- Determina se il tuo sistema utilizza la crittografia. Sarà necessario selezionare l'opzione appropriata nel passaggio 3 a seconda che la crittografia sia abilitata o meno.

Fasi

1. Dal prompt LOADER sul controller danneggiato, avviare l'immagine di ripristino dall'unità flash USB:

```
boot_recovery
```

L'immagine di ripristino viene scaricata dall'unità flash USB.

2. Quando richiesto, immettere il nome dell'immagine o premere **Invio** per accettare l'immagine predefinita visualizzata tra parentesi.
3. Ripristinare il file system var utilizzando la procedura per la versione ONTAP in uso:

ONTAP 9.16.0 o versioni precedenti

Completare i seguenti passaggi sul controller non funzionante e sul controller partner:

a. **Sul controller non compatibile:** Premere Y quando vedi `Do you want to restore the backup configuration now?`

b. **Sul controller non compatibile:** Se richiesto, premere Y per sovrascrivere `/etc/ssh/ssh_host_ecdsa_key`.

c. **Sul controller partner:** Imposta il controller non autorizzato al livello di privilegio avanzato:

```
set -privilege advanced
```

d. **Sul controller partner:** eseguire il comando di ripristino del backup:

```
system node restore-backup -node local -target-address  
impaired_node_IP_address
```



Se viene visualizzato un messaggio diverso da quello di ripristino riuscito, contattare l'assistenza NetApp .

e. **Sul controller partner:** Torna al livello amministratore:

```
set -privilege admin
```

f. **Sul controller non compatibile:** Premere Y quando vedi `Was the restore backup procedure successful?`

g. **Sul controller non compatibile:** Premere Y quando vedi `...would you like to use this restored copy now?`

h. **Sul controller non compatibile:** Premere Y quando viene richiesto di riavviare, quindi premere `Ctrl-C` quando vedi il menu di avvio.

i. **Sul controller con disabilità:** Eseguire una delle seguenti operazioni:

- Se il sistema non utilizza la crittografia, selezionare *Opzione 1 Avvio normale* dal menu di avvio.
- Se il sistema utilizza la crittografia, vai a ["Ripristino della crittografia"](#) .

ONTAP 9.16.1 o successivo

Completare i seguenti passaggi sul controller non funzionante:

a. Premere Y quando viene richiesto di ripristinare la configurazione di backup.

Una volta completata correttamente la procedura di ripristino, viene visualizzato il seguente messaggio: `syncflash_partner: Restore from partner complete`

b. Premere Y quando viene richiesto di confermare che il backup di ripristino è stato eseguito correttamente.

c. Premere Y quando viene richiesto di utilizzare la configurazione ripristinata.

d. Premere Y quando viene richiesto di riavviare il nodo.

- e. Premere **Y** quando viene richiesto di riavviare nuovamente, quindi premere **Ctrl-C** quando vedi il menu di avvio.
- f. Effettuare una delle seguenti operazioni:
 - Se il sistema non utilizza la crittografia, selezionare *Opzione 1 Avvio normale* dal menu di avvio.
 - Se il sistema utilizza la crittografia, vai a ["Ripristino della crittografia"](#) .

4. Collegare il cavo della console al controller partner.
5. Riportare il controller al funzionamento normale restituendo lo storage:

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

6. Se hai disattivato la restituzione automatica, riattivala:

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

7. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi:

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

Quali sono le prossime novità?

Dopo aver avviato l'immagine di ripristino, è necessario ["ripristinare la crittografia sul supporto di avvio"](#).

Ripristina crittografia - ASA A800

Ripristinare la crittografia sul supporto di avvio sostitutivo nel sistema ASA A800 per garantire una protezione continua dei dati. Il processo di sostituzione prevede la verifica della disponibilità della chiave, la riapplicazione delle impostazioni di crittografia e la conferma dell'accesso sicuro ai dati.

Se il sistema di archiviazione esegue ONTAP 9.17.1 o versione successiva, utilizzare ["procedura di ripristino automatico dell'avvio"](#) . Se il sistema esegue una versione precedente di ONTAP, è necessario utilizzare la procedura di ripristino manuale all'avvio.

Completare i passaggi appropriati per ripristinare la crittografia sul sistema in base al tipo di gestore delle chiavi. Se non sei sicuro del gestore chiavi utilizzato dal tuo sistema, controlla le impostazioni acquisite all'inizio della procedura di sostituzione del supporto di avvio.

Onboard Key Manager (OKM)

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

Prima di iniziare

Assicurati di avere a disposizione le seguenti informazioni:

- Passphrase a livello di cluster inserita durante ["abilitazione della gestione delle chiavi di bordo"](#)
- ["Informazioni di backup per il Key Manager integrato"](#)
- Verifica di avere la passphrase corretta e i dati di backup utilizzando ["Come verificare il backup della gestione delle chiavi integrata e la passphrase a livello del cluster"](#) procedura

Fasi

Sul controller non autorizzato:

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

Versione di ONTAP	Selezionare questa opzione
ONTAP 9.8 o versione successiva	Selezionare l'opzione 10. Mostra un esempio di menu di avvio 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. (10) Set Onboard Key Manager recovery secrets. (11) Configure node for external key management. Selection (1-11)? 10

Versione di ONTAP	Selezionare questa opzione
ONTAP 9.7 e versioni precedenti	Selezionare l'opzione nascosta recover_onboard_keymanager Mostra un esempio di menu di avvio <pre> 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>

3. Quando richiesto, conferma di voler 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.

Durante l'inserimento della passphrase, la console non mostra alcun input.

Mostra prompt di esempio

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. Inserisci le informazioni di backup:

a. Incollare l'intero contenuto dalla riga BEGIN BACKUP alla riga END BACKUP, inclusi i trattini.

Mostra prompt di esempio

Enter the backup data:

-----BEGIN

BACKUP-----

01234567890123456789012345678901234567890123456789012345678901
23

12345678901234567890123456789012345678901234567890123456789012
34

23456789012345678901234567890123456789012345678901234567890123
45

34567890123456789012345678901234567890123456789012345678901234
56

45678901234567890123456789012345678901234567890123456789012345
67

[illegible][illegible][illegible][illegible][illegible][illegible][illegible]

A
A

[illegible][illegible][illegible][illegible][illegible][illegible][illegible]

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA

-----END
BACKUP-----
```

b. Premere Invio due volte alla fine dell'input.

Il processo di ripristino viene completato e viene visualizzato il seguente messaggio:

Successfully recovered keymanager secrets.

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. Seleziona 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)
```

Sul controller del partner:

8. Restituire il controller non funzionante:

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

Sul controller non autorizzato:

9. Dopo aver avviato solo con l'aggregato CFO, sincronizzare il gestore delle chiavi:

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

10. Quando richiesto, immettere la passphrase dell'intero 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, viene restituito il prompt del cluster senza messaggi aggiuntivi. Se la sincronizzazione fallisce, viene visualizzato un messaggio di errore prima di tornare al prompt del cluster. Non continuare finché l'errore non sarà stato corretto e la sincronizzazione non sarà stata eseguita correttamente.

11. Verificare che tutte le chiavi siano sincronizzate:

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

Il comando non dovrebbe restituire alcun risultato. Se vengono visualizzati dei risultati, ripetere il comando sync finché non vengono restituiti più risultati.

Sul controller del partner:

12. Restituire il controller non funzionante:

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

13. Ripristinare lo sconto automatico se è stato disattivato:

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

14. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi:

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

Gestore chiavi esterno (EKM)

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

Prima di iniziare

Raccogli i seguenti file da un altro nodo del cluster o dal tuo backup:

- ``/cfcard/kmip/servers.cfg`` file o l'indirizzo e la porta del server KMIP
- ``/cfcard/kmip/certs/client.crt`` file (certificato client)
- ``/cfcard/kmip/certs/client.key`` file (chiave client)
- ``/cfcard/kmip/certs/CA.pem`` file (certificati CA del server KMIP)

Fasi

Sul controller non autorizzato:

1. Collegare il cavo della console al controller non funzionante.
2. Seleziona 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, conferma 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 sul client e sul server:

- a. Immettere il contenuto del file del certificato client (client.crt), comprese le righe BEGIN e END.
- b. Immettere il contenuto del file della chiave client (client.key), comprese le righe BEGIN e END.
- c. Immettere il contenuto del file CA(s) del server KMIP (CA.pem), comprese le righe BEGIN e END.
- d. Immettere l'indirizzo IP del server KMIP.
- e. Immettere la porta del server KMIP (premere Invio per utilizzare la porta predefinita 5696).

Mostra esempio

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----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-----
<certificate_value>
-----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
```

Il processo di ripristino viene completato e viene visualizzato il seguente messaggio:

```
Successfully recovered keymanager secrets.
```

Mostra esempio

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Seleziona 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 lo sconto automatico se è stato disattivato:

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

7. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi:

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

Quali sono le prossime novità?

Dopo aver ripristinato la crittografia sul supporto di avvio, è necessario ["Restituire la parte guasta a NetApp"](#).

Restituisci il supporto di avvio non riuscito a NetApp - ASA A800

Se un componente del sistema di storage ASA A800 si guasta, restituire la parte guasta a NetApp. Vedi il ["Restituzione e sostituzione delle parti"](#) pagina per ulteriori informazioni.

Informazioni sul copyright

Copyright © 2026 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.