Supporto di boot

Install and maintain

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap-systems/fas2700/bootmedia-replace-overview.html on January 09, 2026. Always check docs.netapp.com for the latest.

Sommario

Supporto di boot . . . 1
Panoramica sulla sostituzione del supporto di avvio - FAS2700 . . . 1
Controllare il supporto e lo stato della chiave di crittografia - FAS2700 . . . 1
Passaggio 1: verificare il supporto NVE e scaricare l'immagine ONTAP corretta . . . 2
Passaggio 2: verificare lo stato del gestore delle chiavi ed eseguire il backup della configurazione . . . 2
Spegnere il controller compromesso - FAS2700 . . . 5
Opzione 1: La maggior parte delle configurazioni . . . 6
Opzione 2: Controller in un MetroCluster . . . 6
Sostituire il supporto di avvio - FAS2700 . . . 7
Fase 1: Rimuovere il modulo controller . . . 7
Fase 2: Sostituire il supporto di avvio . . . 9
Fase 3: Trasferire l'immagine di avvio sul supporto di avvio . . . 10
Avviare l'immagine di ripristino - FAS2700 . . . 12
Ripristina crittografia - FAS2700 . . . 14
Restituire il componente guasto a NetApp - AFF A220 e FAS2700 . . . 24

Supporto di boot

Panoramica sulla sostituzione del supporto di avvio - FAS2700

Scopri come sostituire il supporto di avvio su un sistema FAS2700 e i diversi metodi di sostituzione.

Il supporto di avvio memorizza i file immagine di avvio primari e secondari utilizzati dal sistema durante l'avvio. A seconda della configurazione della rete, è possibile eseguire una sostituzione non distruttiva (coppia HA connessa alla rete) o una sostituzione distruttiva (richiede due riavvii).

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 il supporto e lo stato della chiave di crittografia - FAS2700

Verificare il supporto e lo stato della chiave di crittografia prima di spegnere il controller danneggiato su un sistema FAS2700. Questa procedura include la verifica della compatibilità della versione ONTAP con NetApp Volume Encryption (NVE), la verifica della configurazione del gestore delle chiavi e il backup delle informazioni di crittografia per garantire la sicurezza dei dati durante il ripristino del supporto di avvio.

Il sistema FAS2700 supporta solo procedure di ripristino manuale tramite supporti di avvio. Il ripristino automatico del supporto di avvio non è supportato.

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	`security key-manager keystore show` • 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, `No key manager keystores configured` viene elencato nell'output del comando.
ONTAP 9.13.1 o versioni precedenti	`security key-manager show-key-store` • Se EKM è attivato, `external` viene elencato nell'output del comando. • Se OKM è attivato, `onboard` viene elencato nell'output del comando. • Se nessun gestore di chiavi è attivato, `No key managers configured` 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.

Spegnere il controller compromesso - FAS2700

Arrestare o riprendere il controllo del controller danneggiato utilizzando la procedura appropriata per la propria configurazione. Il sistema FAS2700 supporta solo procedure di ripristino manuale tramite supporti di avvio. Il ripristino automatico del supporto di avvio non è supportato.

Opzione 1: La maggior parte delle configurazioni

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

Fasi

1. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza…	Quindi…
Il prompt DEL CARICATORE	Andare a Rimozione del modulo controller.
`Waiting for giveback…`	Premere Ctrl-C, quindi rispondere `y` quando richiesto.
Prompt di sistema o prompt della password (inserire la password di sistema)	Assumere il controllo o arrestare il controller compromesso dal controller integro: `storage failover takeover -ofnode impaired_node_name` Quando il controller non utilizzato visualizza Waiting for giveback… (in attesa di giveback…), premere Ctrl-C e rispondere `y`.

2. Dal prompt DEL CARICATORE, immettere: `printenv` per acquisire tutte le variabili ambientali di avvio. Salvare l'output nel file di log.

Questo comando potrebbe non funzionare se il dispositivo di boot è corrotto o non funzionante.

Opzione 2: Controller in un MetroCluster

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

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

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

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

Fasi

1. Se AutoSupport è attivato, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

Il seguente messaggio AutoSupport elimina la creazione automatica del caso per due ore: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disattivare il giveback automatico dalla console del controller integro: `storage failover modify –node local -auto-giveback false`
3. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza…	Quindi…
Il prompt DEL CARICATORE	Passare alla fase successiva.
In attesa di un giveback…	Premere Ctrl-C, quindi rispondere `y` quando richiesto.
Prompt di sistema o prompt della password (inserire la password di sistema)	Assumere il controllo o arrestare il controller compromesso dal controller integro: `storage failover takeover -ofnode` *`impaired_node_name`* Quando il controller non utilizzato visualizza Waiting for giveback… (in attesa di giveback…), premere Ctrl-C e rispondere `y`.

Sostituire il supporto di avvio - FAS2700

Sostituire il supporto di avvio non riuscito su un modulo controller FAS2700. Questa procedura include la rimozione del modulo controller dallo chassis, la sostituzione fisica del componente del supporto di avvio, il trasferimento dell'immagine di avvio sul supporto sostitutivo tramite un'unità flash USB e il ripristino del normale funzionamento del sistema.

Il sistema FAS2700 supporta solo procedure di ripristino manuale tramite supporti di avvio. Il ripristino automatico del supporto di avvio non è supportato.

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

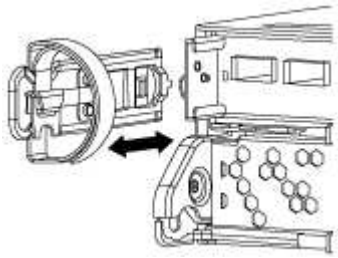
Per accedere ai componenti all'interno del controller, rimuovere prima il modulo controller dal sistema, quindi rimuovere il coperchio sul modulo controller.

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

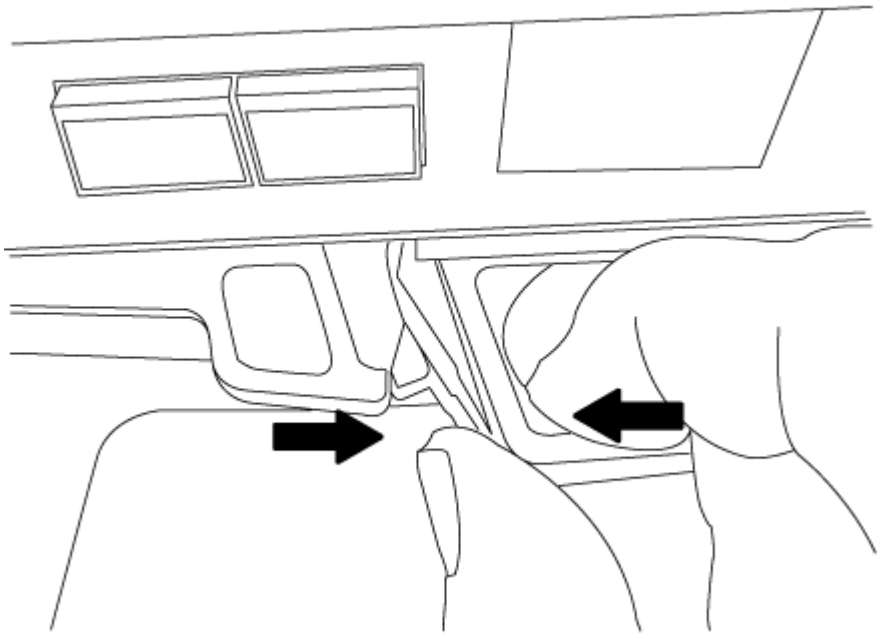
   Lasciare i cavi nel dispositivo di gestione dei cavi in modo che quando si reinstalla il dispositivo di gestione dei cavi, i cavi siano organizzati.

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

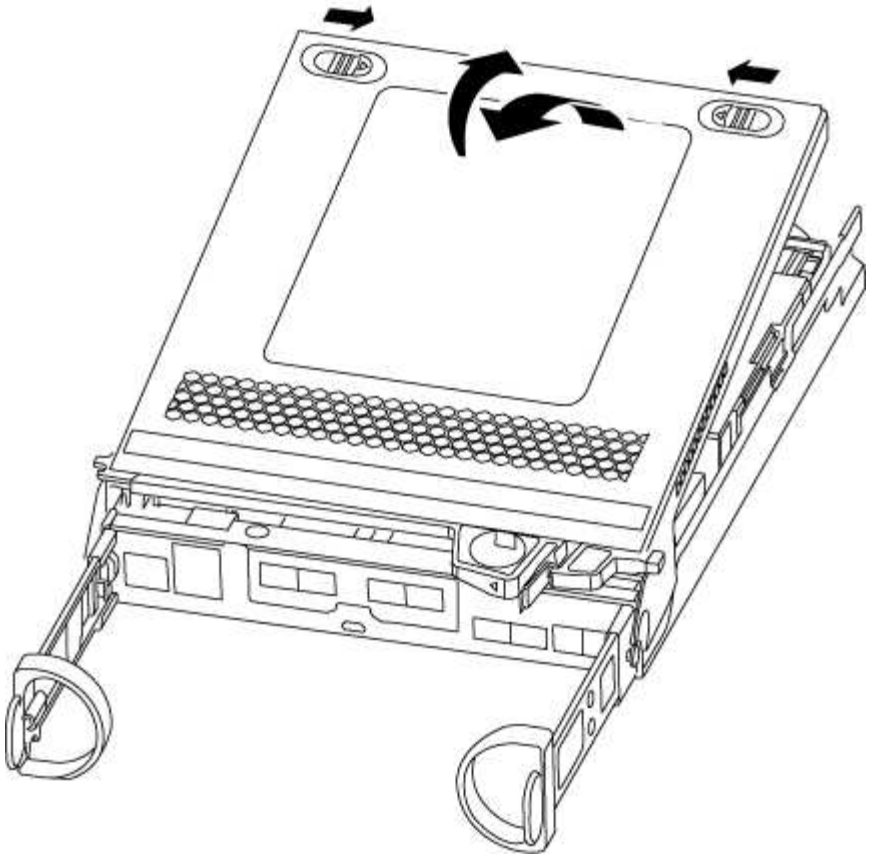
controller.



4. Premere il dispositivo di chiusura sulla maniglia della camma fino al rilascio, aprire completamente la maniglia della camma per rilasciare il modulo controller dalla scheda intermedia, quindi estrarre il modulo controller dallo chassis con due mani.



5. Capovolgere il modulo controller e posizionarlo su una superficie piana e stabile.
6. Aprire il coperchio facendo scorrere le linguette blu per sganciarlo, quindi ruotare il coperchio verso l'alto e aprirlo.

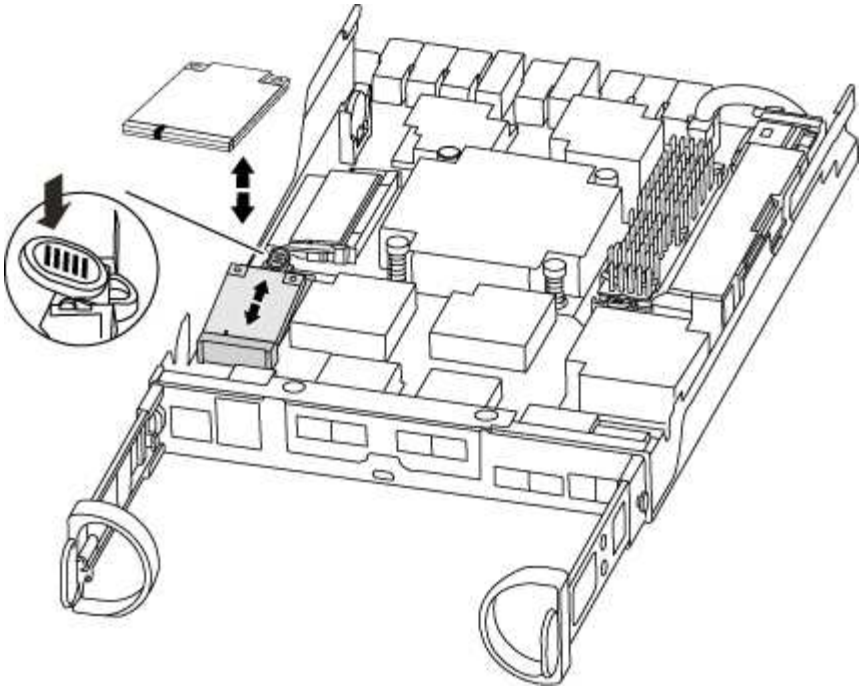


Fase 2: Sostituire il supporto di avvio

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

Fasi

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



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

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

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

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

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

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

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

- È necessario disporre di un'unità flash USB, formattata con FAT32, con almeno 4 GB di capacità.
- 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. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
2. Reinstallare il dispositivo di gestione dei cavi e rieseguire il sistema secondo necessità.

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

3. 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.

4. Inserire completamente il modulo controller nel sistema, assicurandosi che la maniglia della camma si allontani dall'unità flash USB, spingere con decisione la maniglia della camma per terminare l'inserimento del modulo controller, spingere la maniglia della camma in posizione chiusa, quindi serrare la vite a testa zigrinata.

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

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

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

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

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

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

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

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

   - Se si configurano connessioni manuali: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - Filer_addr è l'indirizzo IP del sistema di storage.
     - Netmask è la maschera di rete della rete di gestione connessa al partner ha.
     - gateway è il gateway per la rete.
     - dns_addr è l'indirizzo IP di un name server sulla rete.
     - dns_domain è il nome di dominio DNS (Domain Name System).

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

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

Avviare l'immagine di ripristino - FAS2700

Avviare l'immagine di ripristino ONTAP dall'unità USB su un sistema FAS2700 per ripristinare il supporto di avvio. Questa procedura include l'avvio dall'unità flash USB, il ripristino del file system, la verifica delle variabili ambientali e il ripristino del normale funzionamento del controller dopo la sostituzione del supporto di avvio.

Il sistema FAS2700 supporta solo procedure di ripristino manuale tramite supporti di avvio. Il ripristino automatico del supporto di avvio non è supportato.

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:

Se il sistema dispone di…	Quindi…
Una connessione di rete	a. Premere `y` quando viene richiesto di ripristinare la configurazione di backup. b. Impostare il controller integro su un livello di privilegio avanzato: `set -privilege advanced` c. Eseguire il comando di ripristino del backup: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Riportare il controller al livello di amministrazione: `set -privilege admin` e. Premere `y` quando viene richiesto di utilizzare la configurazione ripristinata. f. Premere `y` quando viene richiesto di riavviare il controller.

Se il sistema dispone di…	Quindi…
Nessuna connessione di rete	a. Premere `n` 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. Se viene richiesto di continuare con l'aggiornamento, premere `y`.

4. Assicurarsi che le variabili ambientali siano impostate come previsto:
   a. Portare il controller al prompt DEL CARICATORE.
   b. Controllare le impostazioni delle variabili di ambiente con `printenv` comando.
   c. Se una variabile di ambiente non è impostata come previsto, modificarla con `setenv` *`environment-variable-name changed-value`* comando.
   d. Salvare le modifiche utilizzando `savenv` comando.
5. Il successivo dipende dalla configurazione del sistema:
   - Se il sistema dispone di onboard keymanager, NSE o NVE configurati, visitare il sito Ripristinare OKM, NSE e NVE secondo necessità
   - Se il sistema non dispone di onboard keymanager, NSE o NVE configurati, completare la procedura descritta in questa sezione.
6. Dal prompt DEL CARICATORE, immettere `boot_ontap` comando.

Se viene visualizzato…	Quindi…
Prompt di login	Passare alla fase successiva.
In attesa di un giveback…	a. Accedere al controller partner. b. Verificare che il controller di destinazione sia pronto per il giveback con `storage failover show` comando.

7. Collegare il cavo della console al controller partner.
8. Restituire il controller utilizzando `storage failover giveback -fromnode local` comando.
9. Al prompt del cluster, controllare le interfacce logiche con `net int -is-home false` comando.

   Se le interfacce sono elencate come "false", ripristinarle alla porta home utilizzando `net int revert` comando.
10. Spostare il cavo della console sul controller riparato ed eseguire `version -v` Per controllare le versioni di ONTAP.
11. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

Ripristina crittografia - FAS2700

Ripristinare la crittografia sul supporto di avvio sostitutivo. Il sistema FAS2700 supporta solo procedure di ripristino manuale tramite supporti di avvio. Il ripristino automatico del supporto di avvio non è supportato.

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
	
	`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`

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
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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
   ```

Restituire il componente guasto a NetApp - AFF A220 e FAS2700

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.

Il sistema FAS2700 supporta solo procedure di ripristino manuale tramite supporti di avvio. Il ripristino automatico del supporto di avvio non è supportato.

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.