Supporto di boot

Install and maintain

NetApp
December 18, 2024

Sommario

Supporto di boot

Panoramica della sostituzione dei supporti di avvio - FAS2820

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 - FAS2820

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	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. 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

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

Gestione delle chiavi integrata

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

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

Spegnere il controller compromesso - FAS2820

Spegnere o sostituire il controller compromesso.

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

Fasi

1. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza…	Quindi…
Il prompt DEL CARICATORE	Andare a Rimozione del modulo controller.

Se il controller non utilizzato visualizza…	Quindi…
`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.

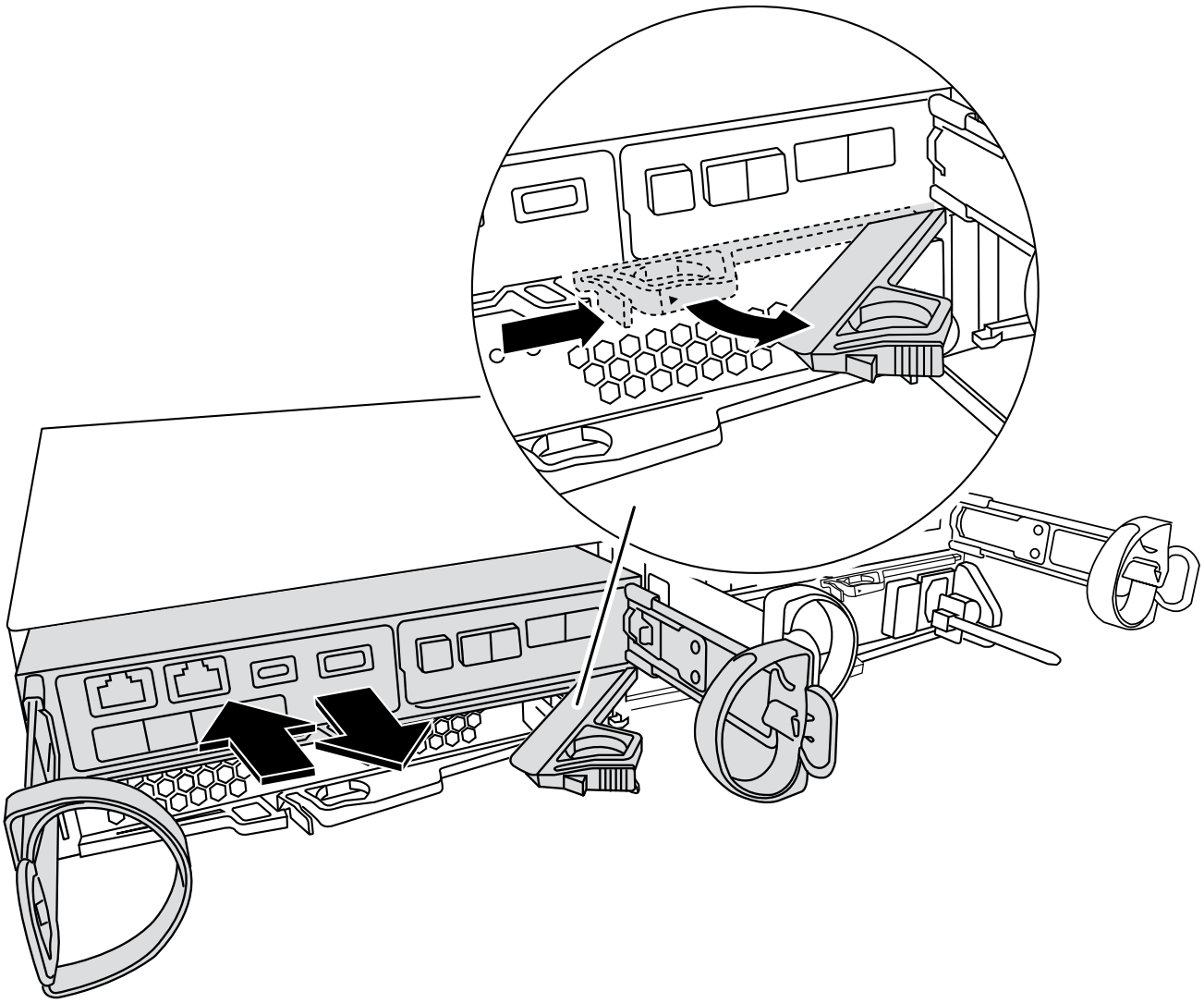
Sostituire il supporto di avvio - FAS2820

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.

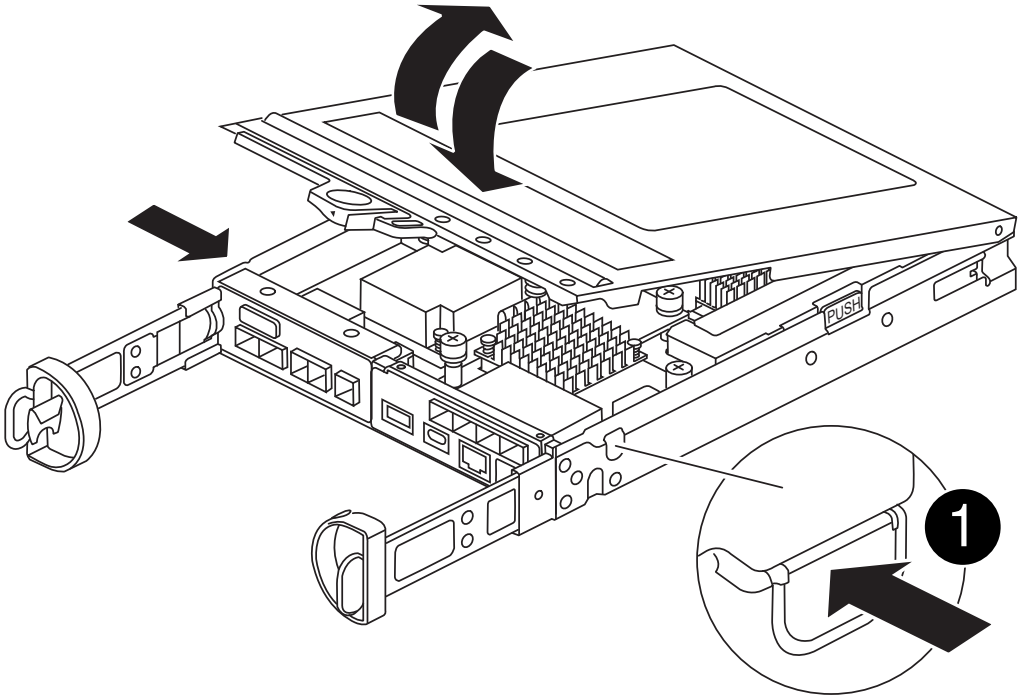
Fase 1: Rimuovere il modulo controller

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.
3. 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.



4. Capovolgere il modulo controller e posizionarlo su una superficie piana e stabile.
5. Aprire il coperchio premendo i pulsanti blu sui lati del modulo controller per rilasciare il coperchio, quindi ruotare il coperchio verso l'alto e verso l'esterno del modulo controller.

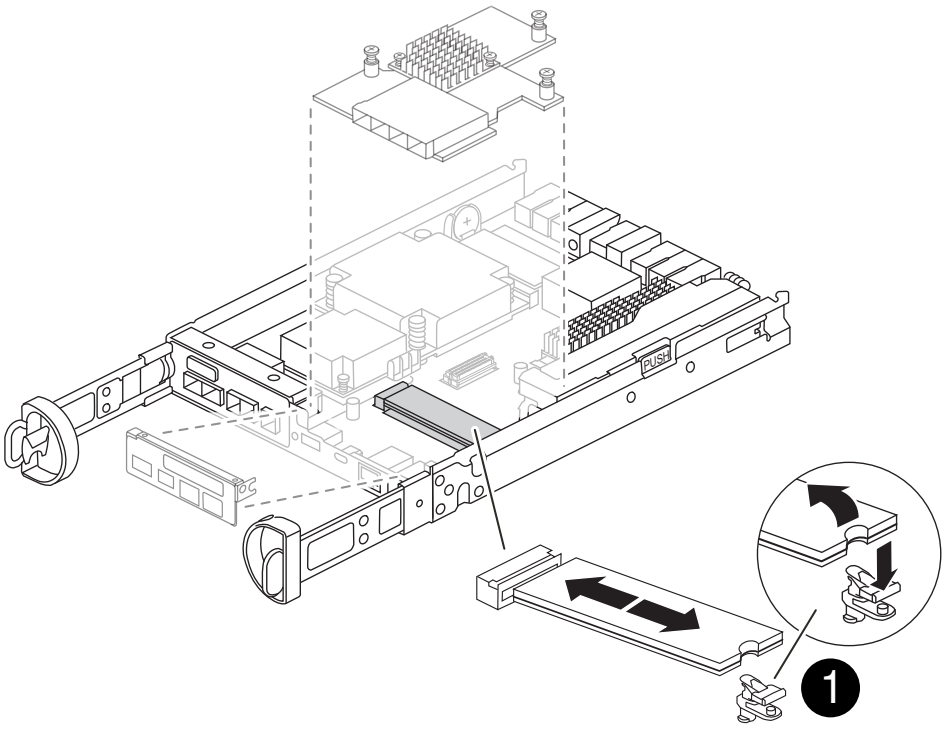


1	Pulsante di rilascio del coperchio del modulo controller

Fase 2: Sostituire il supporto di avvio

Individuare il supporto di avvio nel modulo controller, situato sotto la scheda mezzanine e seguire le istruzioni per sostituirlo.

Animazione - sostituire il supporto di avvio



1	Linguetta di blocco dei supporti di avvio

Fasi

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Rimuovere la scheda mezzanine utilizzando la seguente illustrazione o la mappa FRU sul modulo controller:
   a. Rimuovere la piastra io facendola scorrere verso l'esterno dal modulo controller.
   b. Allentare le viti a testa zigrinata sulla scheda mezzanino.

      È possibile allentare le viti a testa zigrinata con le dita o con un cacciavite. Se si utilizzano le dita, potrebbe essere necessario ruotare la batteria NV verso l'alto per un migliore acquisto con le dita sulla vite a testa zigrinata accanto ad essa.

   c. Sollevare la scheda mezzanine.
3. Sostituire il supporto di avvio:
   a. Premere il pulsante blu sull'alloggiamento del supporto di avvio per rilasciare il supporto di avvio dall'alloggiamento, ruotare il supporto di avvio verso l'alto, 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.

   b. Allineare i bordi del supporto di avvio sostitutivo con lo zoccolo del supporto di avvio, quindi spingerlo delicatamente nello zoccolo. Controllare il supporto di avvio per assicurarsi che sia inserito correttamente e completamente nella presa e, se necessario, rimuovere il supporto di avvio e reinserirlo nella presa.
   c. Premere il pulsante di blocco blu, ruotare il supporto di avvio completamente verso il basso, quindi rilasciare il pulsante di blocco per bloccare il supporto di avvio in posizione.
4. Reinstallare la scheda mezzanine:
   a. Allineare lo zoccolo della scheda madre allo zoccolo della scheda mezzanine, quindi inserire delicatamente la scheda nello zoccolo.
   b. Serrare le tre viti a testa zigrinata sulla scheda mezzanino.
   c. Rimontare la piastra io.
5. Reinstallare il coperchio del modulo controller e bloccarlo in posizione.

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

Installare l'immagine di sistema sul supporto di avvio sostitutivo utilizzando un'unità flash USB con l'immagine installata. Durante questa procedura, è necessario ripristinare il file system var.

Prima di iniziare

- È necessario disporre di un'unità flash USB, formattata in MBR/FAT32, con almeno 4 GB di capacità.
- È necessario disporre di una connessione di rete.

Fasi

1. Scaricare la versione dell'immagine appropriata di ONTAP sull'unità flash USB formattata:
   a. Utilizzare "Come determinare se la versione di ONTAP in esecuzione supporta la crittografia dei volumi NetApp (NVE)" per determinare se la crittografia del volume è attualmente supportata.
      - Se NVE è supportato sul cluster, scaricare l'immagine con crittografia volume NetApp.
      - Se NVE non è supportato sul cluster, scaricare l'immagine senza crittografia volume NetApp. Vedere "Quale immagine ONTAP è necessario scaricare? Con o senza crittografia del volume?" per ulteriori dettagli.
2. Decomprimere l'immagine scaricata.

   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:

   - `boot`
   - `efi`

     i. Copiare il `efi` Nella directory principale dell'unità flash USB.

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

     ii. Rimuovere l'unità flash USB dal computer portatile.
3. Installare il modulo controller:
   a. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
   b. Ricable del modulo controller.

      Quando si esegue la modifica, ricordarsi di reinstallare i convertitori di supporti (SFP) se sono stati rimossi.
4. 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.
5. 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.
6. 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.
7. 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.

8. 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 - FAS2820

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".

Ripristina crittografia - FAS2820

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	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. 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--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---------------------------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-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/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 - FAS2820

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

Informazioni sul marchio commerciale