Supporto di boot

Install and maintain

NetApp
April 19, 2024

Sommario

Supporto di boot

Sostituire il supporto di avvio - FAS9500

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`.

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 non richiede la connessione a una rete per ripristinare `var` file system. La coppia ha in un singolo chassis ha una connessione e0S interna, che viene utilizzata per il trasferimento `var` configurare tra loro.
  - 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.

Pre-shutdown controlla le chiavi di crittografia integrate - FAS9500

Prima di spegnere il controller compromesso e controllare lo stato delle chiavi di crittografia integrate, è necessario controllare lo stato del controller compromesso, disattivare il giveback automatico e verificare quale versione di ONTAP è in esecuzione sul sistema.

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

Fasi

1. Controllare lo stato del controller compromesso:
   - Se il controller non utilizzato viene visualizzato al prompt di login, accedere come `admin`.
   - Se il controller compromesso è al prompt DEL CARICATORE e fa parte della configurazione ha, accedere come `admin` sul controller integro.
   - Se il controller compromesso si trova in una configurazione standalone e al prompt DEL CARICATORE, contattare "mysupport.netapp.com".

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

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

3. Verificare la versione di ONTAP in esecuzione sul controller compromesso se attivato o sul controller partner se il controller non funzionante è attivo, utilizzando `version -v` comando:
   - Se nell'output del comando viene visualizzato <lno-DARE> o <1Ono-DARE>, il sistema non supporta NVE, spegnere il controller.

ONTAP 9.6 e versioni successive

Prima di spegnere il controller compromesso, è necessario verificare se il sistema ha abilitato NetApp Volume Encryption (NVE) o NetApp Storage Encryption (NSE). In tal caso, è necessario verificare la configurazione.

1. Verificare se NVE è in uso per qualsiasi volume nel cluster: `volume show -is-encrypted true`

   Se nell'output sono elencati volumi, NVE viene configurato ed è necessario verificare la configurazione di NVE. Se nell'elenco non sono presenti volumi, verificare che NSE sia configurato e in uso.

2. Verificare se NSE è configurato e in uso: `storage encryption disk show`
   - Se l'output del comando elenca i dettagli del disco con le informazioni di modalità e ID chiave, NSE è configurato ed è necessario verificare la configurazione NSE e in uso.
   - Se non viene visualizzato alcun disco, NSE non è configurato.
   - Se NVE e NSE non sono configurati, nessun disco è protetto con chiavi NSE, è sicuro spegnere il controller compromesso.

Verificare la configurazione NVE

1. Visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi: `security key-manager key query`

   > Dopo la release di ONTAP 9.6, potrebbero essere disponibili altri tipi di gestore delle chiavi. I tipi sono `KMIP`, `AKV`, e. `GCP`. La procedura per la conferma di questi tipi è la stessa di quella per la conferma `external` oppure `onboard` tipi di gestore delle chiavi.

   - Se il `Key Manager` display dei tipi `external` e a. `Restored` viene visualizzata la colonna `yes`, è sicuro spegnere il controller compromesso.
   - Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, è necessario completare alcuni passaggi aggiuntivi.
   - Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.
   - Se il `Key Manager` display dei tipi `onboard` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.

2. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, Eseguire manualmente il backup delle informazioni OKM:

a. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`

b. Immettere il comando per visualizzare le informazioni di gestione delle chiavi: `security key-manager onboard show-backup`

c. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.

d. Tornare alla modalità admin: `set -priv admin`

e. Spegnere il controller compromesso.

3. Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`:

   a. Ripristinare le chiavi di autenticazione per la gestione delle chiavi esterne in tutti i nodi del cluster: `security key-manager external restore`

      Se il comando non riesce, contattare il supporto NetApp.

   "mysupport.netapp.com"

   a. Verificare che il `Restored` colonna uguale a. `yes` per tutte le chiavi di autenticazione: `security key-manager key query`

   b. Spegnere il controller compromesso.

4. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` la colonna visualizza un valore diverso da `yes`:

   a. Immettere il comando di sincronizzazione del gestore delle chiavi di sicurezza integrato: `security key-manager onboard sync`

      > Immettere la passphrase di gestione della chiave alfanumerica integrata a 32 caratteri del cliente al prompt. Se non è possibile fornire la passphrase, contattare il supporto NetApp. "mysupport.netapp.com"

   b. Verificare `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione: `security key-manager key query`

   c. Verificare che il `Key Manager` viene visualizzato il tipo `onboard`, Quindi eseguire manualmente il backup delle informazioni OKM.

   d. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`

   e. Immettere il comando per visualizzare le informazioni di backup per la gestione delle chiavi: `security key-manager onboard show-backup`

   f. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.

   g. Tornare alla modalità admin: `set -priv admin`

   h. È possibile spegnere il controller in modo sicuro.

Verificare la configurazione NSE

1. Visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi: `security key-manager key query -key-type NSE-AK`

   > Dopo la release di ONTAP 9.6, potrebbero essere disponibili altri tipi di gestore delle chiavi. I tipi sono `KMIP`, `AKV`, e. `GCP`. La procedura per la conferma di questi tipi è la stessa di quella per la conferma `external` oppure `onboard` tipi di gestore delle chiavi.

   - Se il `Key Manager` display dei tipi `external` e a. `Restored` viene visualizzata la colonna `yes`, è sicuro spegnere il controller compromesso.
   - Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, è necessario completare alcuni passaggi aggiuntivi.
   - Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.
   - Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.

2. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` viene visualizzata la colonna `yes`, Eseguire manualmente il backup delle informazioni OKM:

   a. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`

   b. Immettere il comando per visualizzare le informazioni di gestione delle chiavi: `security key-manager onboard show-backup`

   c. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.

   d. Tornare alla modalità admin: `set -priv admin`

   e. È possibile spegnere il controller in modo sicuro.

3. Se il `Key Manager` display dei tipi `external` e a. `Restored` la colonna visualizza un valore diverso da `yes`:

   a. Ripristinare le chiavi di autenticazione per la gestione delle chiavi esterne in tutti i nodi del cluster: `security key-manager external restore`

      Se il comando non riesce, contattare il supporto NetApp.

   "mysupport.netapp.com"

   a. Verificare che il `Restored` colonna uguale a. `yes` per tutte le chiavi di autenticazione: `security key-manager key query`

   b. È possibile spegnere il controller in modo sicuro.

4. Se il `Key Manager` display dei tipi `onboard` e a. `Restored` la colonna visualizza un valore diverso da `yes`:

   a. Immettere il comando di sincronizzazione del gestore delle chiavi di sicurezza integrato: `security key-manager onboard sync`

Immettere la passphrase di gestione della chiave alfanumerica integrata a 32 caratteri del cliente al prompt. Se non è possibile fornire la passphrase, contattare il supporto NetApp.

"mysupport.netapp.com"

a. Verificare `Restored` viene visualizzata la colonna `yes` per tutte le chiavi di autenticazione: `security key-manager key query`
b. Verificare che il `Key Manager` viene visualizzato il tipo `onboard`, Quindi eseguire manualmente il backup delle informazioni OKM.
c. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
d. Immettere il comando per visualizzare le informazioni di backup per la gestione delle chiavi: `security key-manager onboard show-backup`
e. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
f. Tornare alla modalità admin: `set -priv admin`
g. È possibile spegnere il controller in modo sicuro.

Spegnere il controller compromesso - FAS9500

Arrestare o sostituire il controller compromesso utilizzando una delle seguenti opzioni.

Dopo aver completato le attività NVE o NSE, è necessario completare la chiusura del nodo compromesso.

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

A proposito di questa attività

- Se si dispone di un sistema SAN, è necessario controllare i messaggi di evento `cluster kernel-service show`) Per blade SCSI del controller deteriorati. Il `cluster kernel-service show` command visualizza il nome del nodo, lo stato del quorum di quel nodo, lo stato di disponibilità di quel nodo e lo stato operativo di quel nodo.

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

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

Fasi

1. Se AutoSupport è attivato, 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`

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

3. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza…	**Quindi…**
Il prompt DEL CARICATORE	Passare alla fase successiva.
In attesa di un giveback…	Premere Ctrl-C, quindi rispondere `y` quando richiesto.
Prompt di sistema o prompt della password	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`.

Rimuovere il controller, sostituire il supporto di avvio e trasferire l'immagine di avvio - FAS9500

È necessario rimuovere e aprire il modulo controller, individuare e sostituire il supporto di avvio nel controller, quindi trasferire l'immagine sul supporto di avvio sostitutivo.

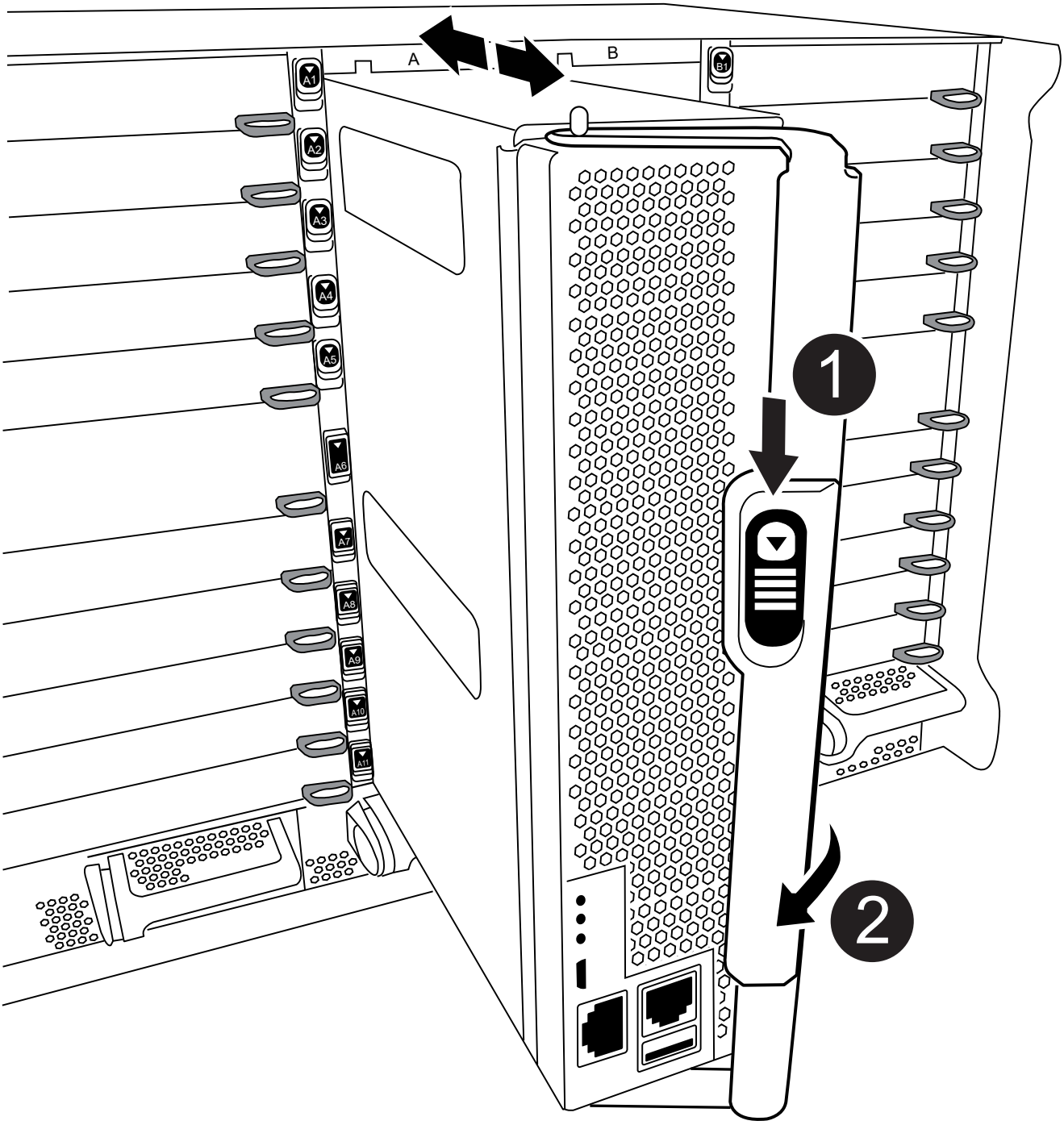
Fase 1: Rimuovere il modulo controller

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

Fasi

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Scollegare i cavi dal modulo controller guasto e tenere traccia del punto in cui sono stati collegati i cavi.
3. Far scorrere verso il basso il pulsante terra cotta sulla maniglia della camma fino a sbloccarla.

   Animazione - rimuovere il modulo controller



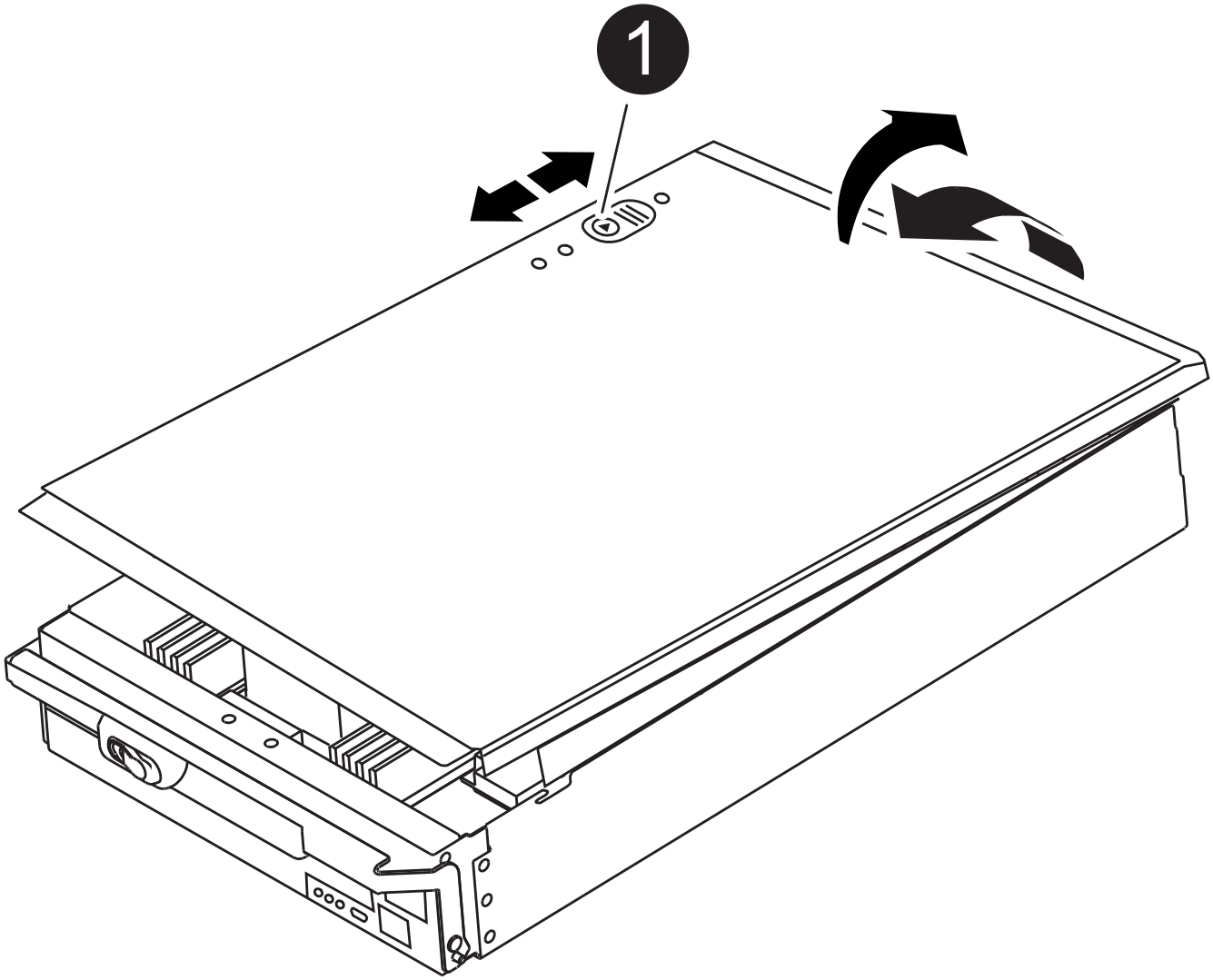
1	Pulsante di rilascio della maniglia della camma

2	Maniglia CAM

4. Ruotare la maniglia della camma in modo da disimpegnare completamente il modulo controller dal telaio, quindi estrarre il modulo controller dal telaio.

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

5. Posizionare il coperchio del modulo controller con il lato rivolto verso l'alto su una superficie stabile e piana, premere il pulsante blu sul coperchio, far scorrere il coperchio sul retro del modulo controller, quindi sollevare il coperchio ed estrarlo dal modulo controller.



1	Pulsante di bloccaggio del coperchio del modulo controller

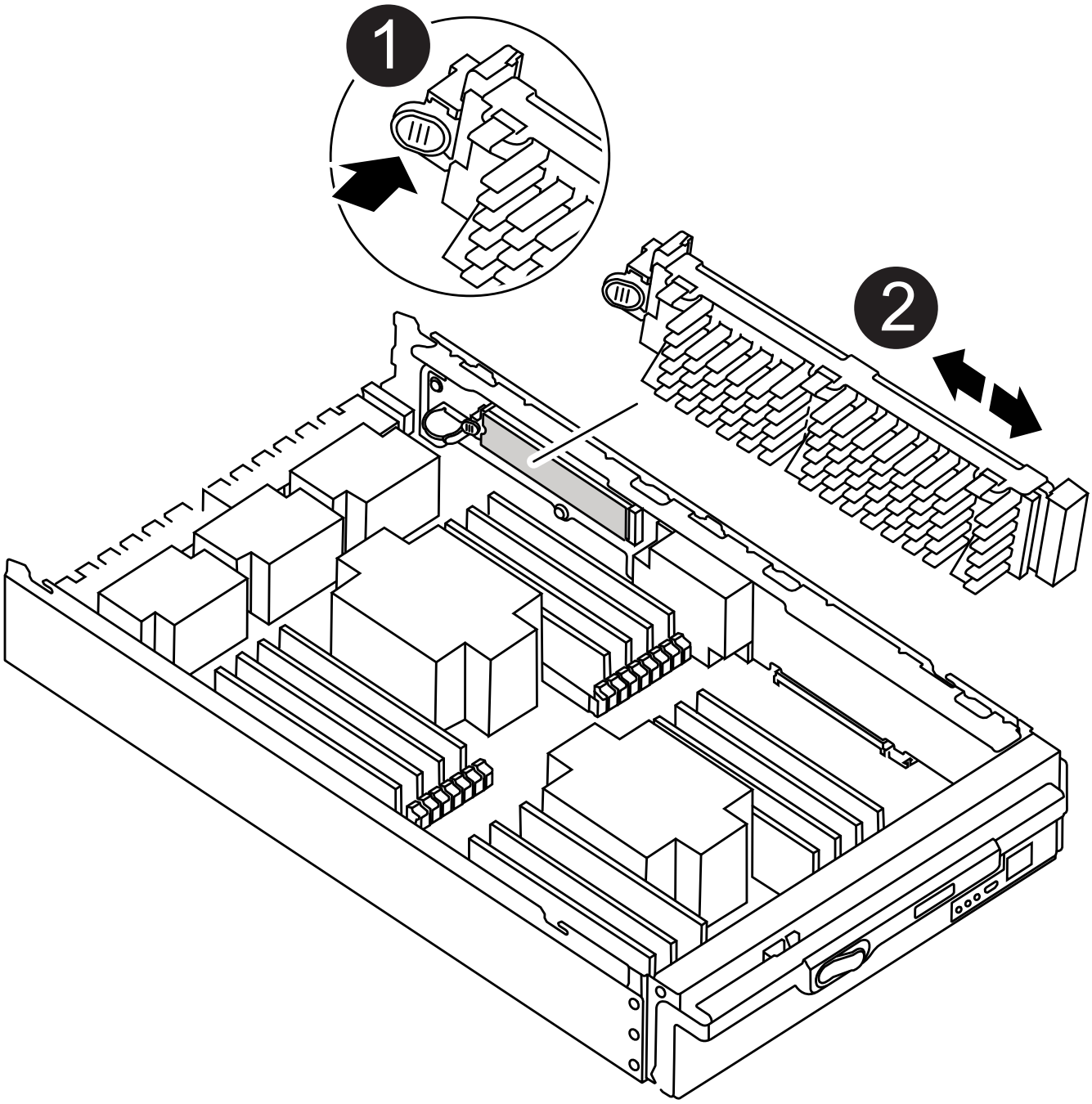
Fase 2: Sostituire il supporto di avvio

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

Fasi

1. Sollevare il condotto d'aria nero sul retro del modulo controller, quindi individuare il supporto di avvio utilizzando la seguente illustrazione o la mappa FRU sul modulo controller:

   Animazione - sostituire il supporto di avvio



1	Premere il tasto di rilascio Tab
2	Supporto di boot

2. 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.

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

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

5. Premere il supporto di avvio verso il basso per inserire il pulsante di blocco sull'alloggiamento del supporto di avvio.
6. Reinstallare il coperchio del modulo controller allineando i perni sul coperchio con gli slot sul supporto della scheda madre, quindi far scorrere il coperchio in posizione.

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 `var` file system durante questa procedura.

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 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. Se necessario, è possibile ricable il modulo controller.
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, quindi spingere la maniglia della camma in posizione chiusa.

   Il nodo inizia ad avviarsi non appena viene completamente installato 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 di avvio in modalità manutenzione, quindi arrestare il nodo per avviare IL CARICATORE.

6. Sebbene le variabili d'ambiente e i bootargs siano conservati, è necessario verificare che tutte le variabili d'ambiente di boot e i bootargs necessari siano impostati correttamente per il tipo di sistema e per la configurazione utilizzando il `printenv bootarg name` e correggere eventuali errori utilizzando `setenv variable-name <value>` comando.
   a. Controllare le variabili di ambiente di boot:
      - bootarg.init.boot_clustered
      - partner-sysid
      - bootarg.init.flash_optimized per AFF
      - bootarg.init.san_optimized per AFF
      - bootarg.init.switchless_cluster.enable
   b. Se External Key Manager (Gestore chiavi esterne) è attivato, controllare i valori di boot, elencati in `kenv` Output ASUP:
      - bootarg.storageencryption.support <value>
      - bootarg.keymanager.support <value>
      - kmip.init.interface <value>
      - kmip.init.ipaddr <value>
      - kmip.init.netmask <value>
      - kmip.init.gateway <value>
   c. Se Onboard Key Manager è attivato, controllare i valori di boot, elencati nella `kenv` Output ASUP:
      - bootarg.storageencryption.support <value>
      - bootarg.keymanager.support <value>
      - bootarg.onboard_keymanager <value>
   d. Salvare le variabili di ambiente modificate con `savenv` comando
   e. Confermare le modifiche utilizzando `printenv variable-name` comando.
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 nodo compromesso dal nodo 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. Per ulteriori informazioni, immettere help ifconfig al prompt del firmware.

8. Se il controller si trova in un MetroCluster esteso o collegato al fabric, è necessario ripristinare la configurazione dell'adattatore FC:

   a. Avvio in modalità di manutenzione: `boot_ontap maint`

   b. Impostare le porte MetroCluster come iniziatori: `ucadmin modify -m fc -t iniitator adapter_name`

   c. Halt per tornare alla modalità di manutenzione: `halt`

   Le modifiche verranno implementate all'avvio del sistema.

Avviare l'immagine di ripristino - FAS9500

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

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

   L'immagine viene scaricata dall'unità flash USB.

2. Quando richiesto, inserire il nome dell'immagine o accettare l'immagine predefinita visualizzata tra parentesi sullo schermo.

3. Ripristinare il file system var:

Se il sistema dispone di…	Quindi…
Una connessione di rete	a. Premere `y` quando viene richiesto di ripristinare la configurazione di backup. b. Premere `y` quando viene richiesto di sovrascrivere `/etc/ssh/ssh_host_ecdsa_key`. c. Premere `y` quando viene richiesto di confermare se il backup di ripristino è stato eseguito correttamente. d. Premere `Y` quando viene richiesto di ripristinare la copia della configurazione. e. Impostare il nodo integro sul livello di privilegio avanzato: `set -privilege advanced` f. Eseguire il comando di ripristino del backup: `system node restore-backup -node local -target-address impaired_node_IP_address` g. Riportare il nodo al livello admin: `set -privilege admin` h. Premere `y` quando viene richiesto di utilizzare la configurazione ripristinata. i. Premere `y` quando viene richiesto di riavviare il nodo.
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`.

Se il sistema dispone di…	Quindi…

Nessuna connessione di rete e si trova in una configurazione MetroCluster IP	a. Premere `n` quando viene richiesto di ripristinare la configurazione di backup.
	b. Riavviare il sistema quando richiesto dal sistema.
	c. Attendere che le connessioni dello storage iSCSI si connettano.
	
	È possibile procedere dopo aver visualizzato i seguenti messaggi:
	
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	
	d. 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 nodo 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 `setenvenvironment_variable_name changed_value` comando.
   d. Salvare le modifiche utilizzando `saveenv` comando.
5. Il successivo dipende dalla configurazione del sistema:
   - Se il sistema dispone di onboard keymanager, NSE o NVE configurati, visitare il sito Fasi di sostituzione dei supporti post-boot per OKM, NSE e NVE

- Se il sistema non dispone di onboard keymanager, NSE o NVE configurati, completare la procedura descritta in questa sezione.

6. Dal prompt DEL CARICATORE, immettere `boot_ontap` comando.

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

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

   Se le interfacce sono elencate come "false", ripristinarle alla porta home utilizzando `net int revert` comando.

10. Spostare il cavo della console sul nodo riparato ed eseguire `version -v` Per controllare le versioni di ONTAP.
11. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

Procedura di sostituzione dei supporti post-boot per OKM, NSE e NVE - FAS9500

Una volta controllate le variabili di ambiente, è necessario completare i passaggi specifici per ripristinare Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) e NetApp Volume Encryption (NVE).

1. Determinare la sezione da utilizzare per ripristinare le configurazioni OKM, NSE o NVE: Se NSE o NVE sono attivati insieme a Onboard Key Manager, è necessario ripristinare le impostazioni acquisite all'inizio di questa procedura.
   - Se NSE o NVE sono attivati e Onboard Key Manager è attivato, passare a. Restore NVE or NSE (Ripristina NVE o NSE) quando Onboard Key Manager è attivato.
   - Se NSE o NVE sono abilitati per ONTAP 9.6, passare a. Ripristinare NSE/NVE nei sistemi che eseguono ONTAP 9.6 e versioni successive.

Restore NVE or NSE (Ripristina NVE o NSE) quando Onboard Key Manager è attivato

1. Collegare il cavo della console al nodo di destinazione.
2. Utilizzare `boot_ontap` Al prompt DEL CARICATORE per avviare il nodo.
3. Controllare l'output della console:

Se la console visualizza…	Quindi…
Il prompt DEL CARICATORE	Avviare il nodo dal menu di boot: `boot_ontap menu`
In attesa di un giveback	a. Invio `Ctrl-C` quando richiesto b. Quando viene visualizzato il messaggio: Interrompere questo nodo invece di attendere [y/n]? , inserire: `y` c. Al prompt DEL CARICATORE, immettere `boot_ontap menu` comando.

4. Nel menu di avvio, immettere il comando nascosto, `recover_onboard_keymanager`e rispondere `y` quando richiesto.
5. Inserire la passphrase per il gestore delle chiavi integrato ottenuto dal cliente all'inizio di questa procedura.
6. Quando viene richiesto di inserire i dati di backup, incollare i dati di backup acquisiti all'inizio di questa sezione, quando richiesto. Incollare l'output di `security key-manager backup show` OPPURE `security key-manager onboard show-backup` comando.

   > I dati vengono generati da entrambi `security key-manager backup show` o il comando show-backup` integrato del security key-manager.

   Esempio di dati di backup:

   Inserire i dati di backup:

   ```
   ---------- INIZIA IL BACKUP----------
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . .
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

   ---------- FINE BACKUP----------
   ```

7. Nel menu di avvio, selezionare l'opzione Normal Boot (Avvio normale).

   Il sistema si avvia in attesa di giveback… prompt.

8. Spostare il cavo della console nel nodo partner e accedere come admin.
9. Verificare che il nodo di destinazione sia pronto per il giveback con `storage failover show` comando.
10. Restituire solo gli aggregati CFO con `storage failover giveback -fromnode local -only-cfo-aggregates true` comando.
    - Se il comando non riesce a causa di un disco guasto, disinnestare fisicamente il disco guasto, ma lasciare il disco nello slot fino a quando non viene ricevuto un disco sostitutivo.
    - Se il comando non riesce a causa di una sessione CIFS aperta, verificare con il cliente come chiudere le sessioni CIFS.

> La chiusura di CIFS può causare la perdita di dati.

- Se il comando non riesce perché il partner non è pronto, attendere 5 minuti per la sincronizzazione delle NVRAM.
- Se il comando non riesce a causa di un processo NDMP, SnapMirror o SnapVault, disattivare il processo. Per ulteriori informazioni, consultare il contenuto appropriato.

11. Una volta completato il giveback, controllare lo stato di failover e giveback con `storage failover show` e i comandi di show-giveback per il failover dello storage.

    Verranno mostrati solo gli aggregati CFO (aggregato root e aggregati di dati di stile CFO).

12. Se si utilizza ONTAP 9.6 o versione successiva, eseguire la sincronizzazione integrata del Security Key-Manager:
    a. Eseguire `security key-manager onboard sync` e inserire la passphrase quando richiesto.
    b. Inserire il `security key-manager key-query` per visualizzare una vista dettagliata di tutte le chiavi memorizzate nel gestore delle chiavi integrato e verificare che `Restored` colonna = `yes/true` per tutte le chiavi di autenticazione.

    > Se il `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes/true`, Contattare il supporto clienti.

    c. Attendere 10 minuti per la sincronizzazione della chiave nel cluster.
13. Spostare il cavo della console nel nodo partner.
14. Restituire il nodo di destinazione utilizzando `storage failover giveback -fromnode local` comando.
15. Controllare lo stato del giveback, tre minuti dopo il completamento del report, utilizzando `storage failover show` comando.

    Se il giveback non viene completato dopo 20 minuti, contattare l'assistenza clienti.

16. Al prompt di clustershell, immettere `net int show -is-home false` comando per elencare le interfacce logiche che non si trovano sul nodo principale e sulla porta.

    Se le interfacce sono elencate come `false`, ripristinare tali interfacce alla porta home utilizzando `net int revert` comando.

17. Spostare il cavo della console sul nodo di destinazione ed eseguire `version -v` Per controllare le versioni di ONTAP.
18. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

Ripristinare NSE/NVE nei sistemi che eseguono ONTAP 9.6 e versioni successive

1. Collegare il cavo della console al nodo di destinazione.
2. Utilizzare `boot_ontap` Al prompt DEL CARICATORE per avviare il nodo.
3. Controllare l'output della console:

Se la console visualizza…	Quindi…
Prompt di login	Passare alla fase 7.
In attesa di un giveback…	a. Accedere al nodo partner. b. Verificare che il nodo di destinazione sia pronto per il giveback con `storage failover show` comando.

4. Spostare il cavo della console sul nodo partner e restituire lo storage del nodo di destinazione utilizzando `storage failover giveback -fromnode local -only-cfo-aggregates true local` comando.
   - Se il comando non riesce a causa di un disco guasto, disinnestare fisicamente il disco guasto, ma lasciare il disco nello slot fino a quando non viene ricevuto un disco sostitutivo.
   - Se il comando non riesce a causa di sessioni CIFS aperte, verificare con il cliente come chiudere le sessioni CIFS.

     La chiusura di CIFS può causare la perdita di dati.

   - Se il comando non riesce perché il partner è "non pronto", attendere 5 minuti per la sincronizzazione di NVMEM.
   - Se il comando non riesce a causa di un processo NDMP, SnapMirror o SnapVault, disattivare il processo. Per ulteriori informazioni, consultare il contenuto appropriato.
5. Attendere 3 minuti e controllare lo stato di failover con `storage failover show` comando.
6. Al prompt di clustershell, immettere `net int show -is-home false` comando per elencare le interfacce logiche che non si trovano sul nodo principale e sulla porta.

   Se le interfacce sono elencate come `false`, ripristinare tali interfacce alla porta home utilizzando `net int revert` comando.

7. Spostare il cavo della console sul nodo di destinazione ed eseguire `version -v` Per controllare le versioni di ONTAP.
8. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.
9. Utilizzare `storage encryption disk show` al prompt di clustershell, per rivedere l'output.
10. Utilizzare `security key-manager key-query` per visualizzare le chiavi di crittografia e autenticazione memorizzate nei server di gestione delle chiavi.
    - Se il `Restored` colonna = `yes/true`, è possibile completare il processo di sostituzione.
    - Se il `Key Manager type` = `external` e a. `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes/true`, utilizzare `security key-manager external restore` Comando per ripristinare gli ID delle chiavi di autenticazione.

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

    - Se il `Key Manager type` = `onboard` e a. `Restored` column (colonna) = qualsiasi altro elemento diverso da `yes/true`, utilizzare `security key-manager onboard sync` Comando per risync il tipo di Key Manager.

Utilizzare `security key-manager key-query` per verificare che il `Restored` colonna = `yes/true` per tutte le chiavi di autenticazione.

11. Collegare il cavo della console al nodo partner.
12. Restituire il nodo utilizzando `storage failover giveback -fromnode local` comando.
13. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

Restituire il componente guasto a NetApp - FAS9500

Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit. Vedere "Parti restituita sostituzioni" per ulteriori informazioni.