



Supporto di boot

Install and maintain

NetApp
August 18, 2025

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems/c400/bootmedia-replace-overview.html> on August 18, 2025. Always check docs.netapp.com for the latest.

Sommario

Supporto di boot	1
Panoramica della sostituzione dei supporti di avvio - AFF C400	1
Verificare il supporto e lo stato della chiave di crittografia - AFF C400	1
Passaggio 1: Verificare che la versione di ONTAP in uso supporti la crittografia dei volumi NetApp	1
Fase 2: Determinare se è possibile arrestare il controller in modo sicuro	2
Spegnere il controller compromesso - AFF C400	6
Opzione 1: La maggior parte delle configurazioni	6
Opzione 2: Il controller è in una configurazione MetroCluster	7
Opzione 3: Controller in un MetroCluster a due nodi	8
Sostituire il supporto di avvio - AFF C400	10
Fase 1: Rimuovere il modulo controller	10
Fase 2: Sostituire il supporto di avvio	11
Fase 3: Trasferire l'immagine di avvio sul supporto di avvio	14
Avviare l'immagine di ripristino - AFF C400	15
Switch back aggregates in una configurazione MetroCluster a due nodi - AFF C400	18
Ripristinare la crittografia - AFF C400	19
Opzione 1: Ripristinare la configurazione di Onboard Key Manager	19
Opzione 2: Ripristinare la configurazione di External Key Manager	25
Restituire il componente guasto a NetApp - AFF C400	28

Supporto di boot

Panoramica della sostituzione dei supporti di avvio - AFF C400

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.

Verificare il supporto e lo stato della chiave di crittografia - AFF C400

Per garantire la sicurezza dei dati nel sistema di storage, è necessario verificare il supporto della chiave di crittografia e lo stato sul supporto di avvio. Verifica se la versione di ONTAP supporta la crittografia dei volumi di NetApp (NVE) e prima di arrestare il controller verifica se il gestore delle chiavi è attivo.

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.

Fasi

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

```
version -v
```

Se l'output include `10no-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.

Fasi

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

Versione di ONTAP	Eseguire questo comando
ONTAP 9.14.1 o versione successiva	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"> • Se EKM è attivato, EKM viene elencato nell'output del comando. • Se OKM è attivato, OKM viene elencato nell'output del comando. • Se nessun gestore di chiavi è attivato, No key manager keystores configured viene elencato nell'output del comando.
ONTAP 9.13.1 o versioni precedenti	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> • Se EKM è attivato, 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	<ol style="list-style-type: none">Ripristinare le chiavi di autenticazione della gestione delle chiavi esterne in tutti i nodi del cluster utilizzando il seguente comando: <pre>security key-manager external restore</pre>Se il comando non riesce, contattare "Supporto NetApp".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	<p>Eseguire manualmente il backup delle informazioni OKM.</p> <ol style="list-style-type: none"> <li data-bbox="649 270 1405 340">Accedere alla modalità avanzata immettendo <code>set -priv advanced</code> e quindi immettere <code>Y</code> quando richiesto. <li data-bbox="649 361 1318 430">Immettere il seguente comando per visualizzare le informazioni sulla gestione delle chiavi: <pre data-bbox="682 466 1359 498">security key-manager onboard show-backup</pre> <ol style="list-style-type: none"> <li data-bbox="649 530 1400 599">Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. <li data-bbox="682 629 1405 699">Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM. <li data-bbox="649 730 1442 800">È possibile arrestare il controller danneggiato in modo sicuro. Andare a "spegnere il controller danneggiato".

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

Spegnere il controller compromesso - AFF C400

Dopo aver completato le attività NVE o NSE, è necessario completare l'arresto del controller compromesso. Arrestare o sostituire il controller con problemi utilizzando la procedura appropriata per la configurazione.

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: <code>storage failover takeover -ofnode impaired_node_name</code> Quando il controller non utilizzato visualizza Waiting for giveback... (in attesa di giveback...), premere Ctrl-C e rispondere 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: Il controller è in una configurazione MetroCluster



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

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

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

Fasi

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

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

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

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

Opzione 3: Controller in un MetroCluster a due nodi

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

A proposito di questa attività

- Al termine di questa procedura, è necessario lasciare accesi gli alimentatori per alimentare il controller integro.

Fasi

1. Controllare lo stato MetroCluster per determinare se il controller compromesso è passato automaticamente al controller integro: `metrocluster show`
2. A seconda che si sia verificato uno switchover automatico, procedere come indicato nella seguente tabella:

Se il controller è compromesso...	Quindi...
Si è attivata automaticamente	Passare alla fase successiva.
Non si è attivato automaticamente	Eseguire un'operazione di switchover pianificata dal controller integro: <code>metrocluster switchover</code>
Non è stato attivato automaticamente, si è tentato di eseguire lo switchover con <code>metrocluster switchover</code> e lo switchover è stato vetoed	Esaminare i messaggi di voto e, se possibile, risolvere il problema e riprovare. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

3. Risincronizzare gli aggregati di dati eseguendo `metrocluster heal -phase aggregates` dal cluster esistente.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

Se la riparazione è vetoed, si ha la possibilità di riportare il metrocluster heal con il -override-vetoed parametro. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi voto soft che impedisca l'operazione di riparazione.

4. Verificare che l'operazione sia stata completata utilizzando il comando MetroCluster Operation show.

```
controller_A_1::> metrocluster operation show
  Operation: heal-aggregates
  State: successful
  Start Time: 7/25/2016 18:45:55
  End Time: 7/25/2016 18:45:56
  Errors: -
```

5. Controllare lo stato degli aggregati utilizzando storage aggregate show comando.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State      #Vols  Nodes      RAID
Status
----- -----
...
aggr_b2      227.1GB    227.1GB    0% online      0  mcc1-a2
raid_dp, mirrored, normal...
```

6. Riparare gli aggregati root utilizzando metrocluster heal -phase root-aggregates comando.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

Se la riparazione è vetoed, si ha la possibilità di riportare il metrocluster heal comando con il parametro -override-vetoed. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi voto soft che impedisca l'operazione di riparazione.

7. Verificare che l'operazione di riparazione sia completa utilizzando metrocluster operation show sul cluster di destinazione:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
  State: successful
  Start Time: 7/29/2016 20:54:41
  End Time: 7/29/2016 20:54:42
  Errors: -
```

8. Sul modulo controller guasto, scollegare gli alimentatori.

Sostituire il supporto di avvio - AFF C400

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 modulo controller, è necessario rimuovere il modulo controller dallo chassis.

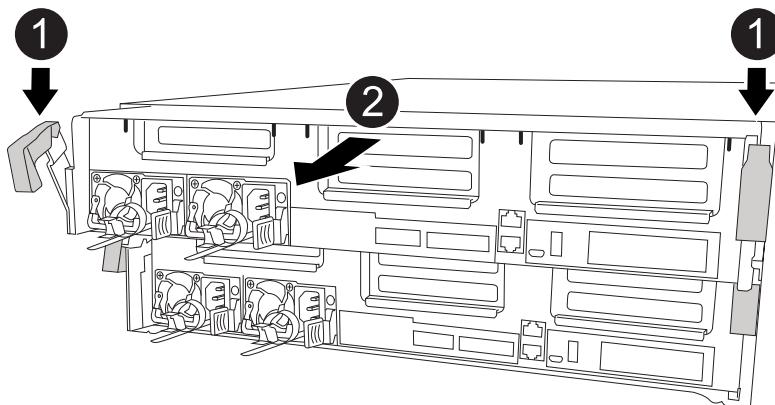
Fasi

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Rilasciare i fermi dei cavi di alimentazione, quindi scollegare i cavi dagli alimentatori.
3. 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.

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

Il modulo controller si sposta leggermente fuori dallo chassis.



1	Fermi di bloccaggio
2	Il controller si sposta leggermente fuori dallo chassis

6. Estrarre il modulo controller dal telaio.

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

7. Posizionare il modulo controller su una superficie piana e stabile.

Fase 2: Sostituire il supporto di avvio

Individuare il supporto di avvio nel modulo controller (vedere la mappa FRU sul modulo controller), quindi seguire le istruzioni per sostituirlo.

Prima di iniziare

Sebbene il contenuto del supporto di avvio sia crittografato, è consigliabile cancellare il contenuto del supporto di avvio prima di sostituirlo. Per ulteriori informazioni, consultare "["Dichiarazione di volatilità"](#) Per il tuo sistema sul sito di supporto NetApp.



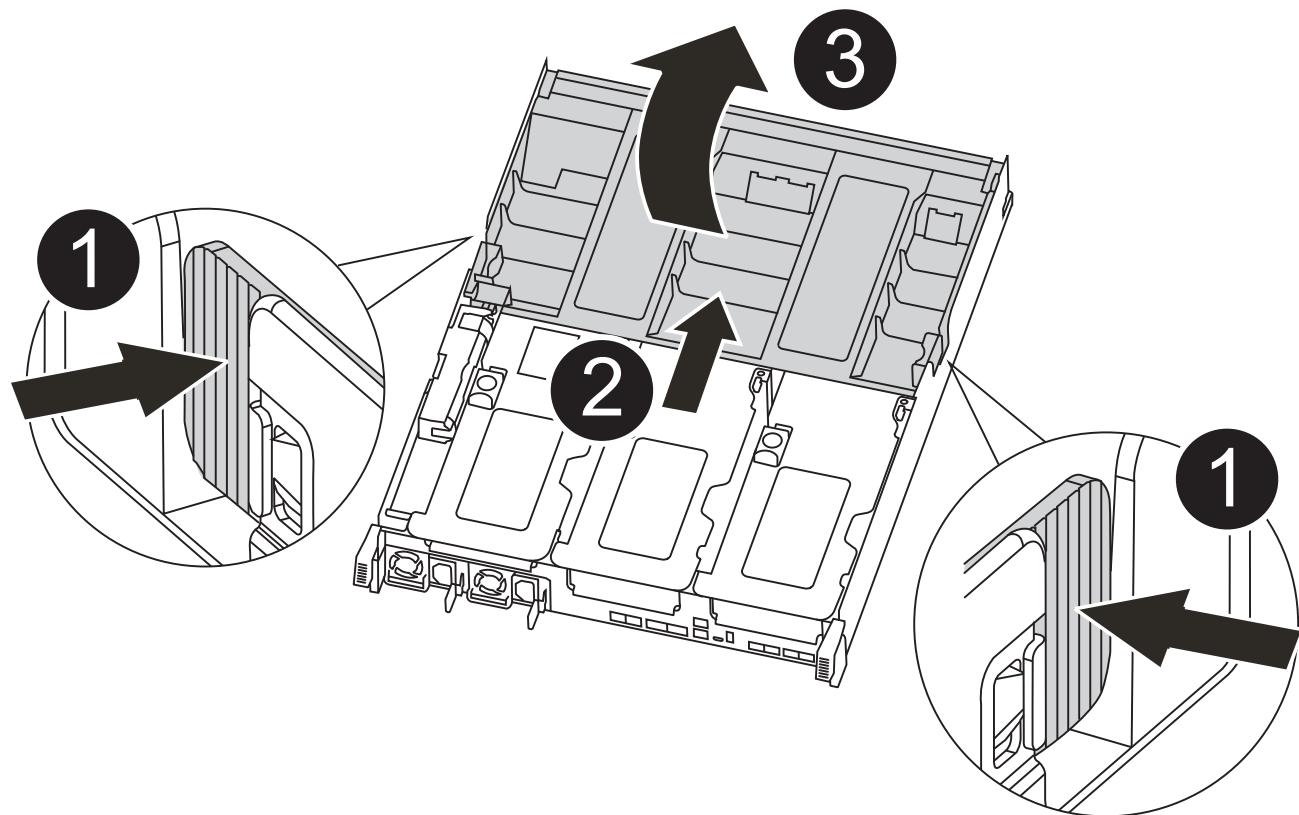
Per visualizzare la *Dichiarazione di volatilità* del sistema, è necessario accedere al sito di supporto NetApp.

Per sostituire il supporto di avvio, è possibile utilizzare la seguente animazione, illustrazione o procedura scritta.

[Animazione - sostituire il supporto di avvio](#)

Fasi

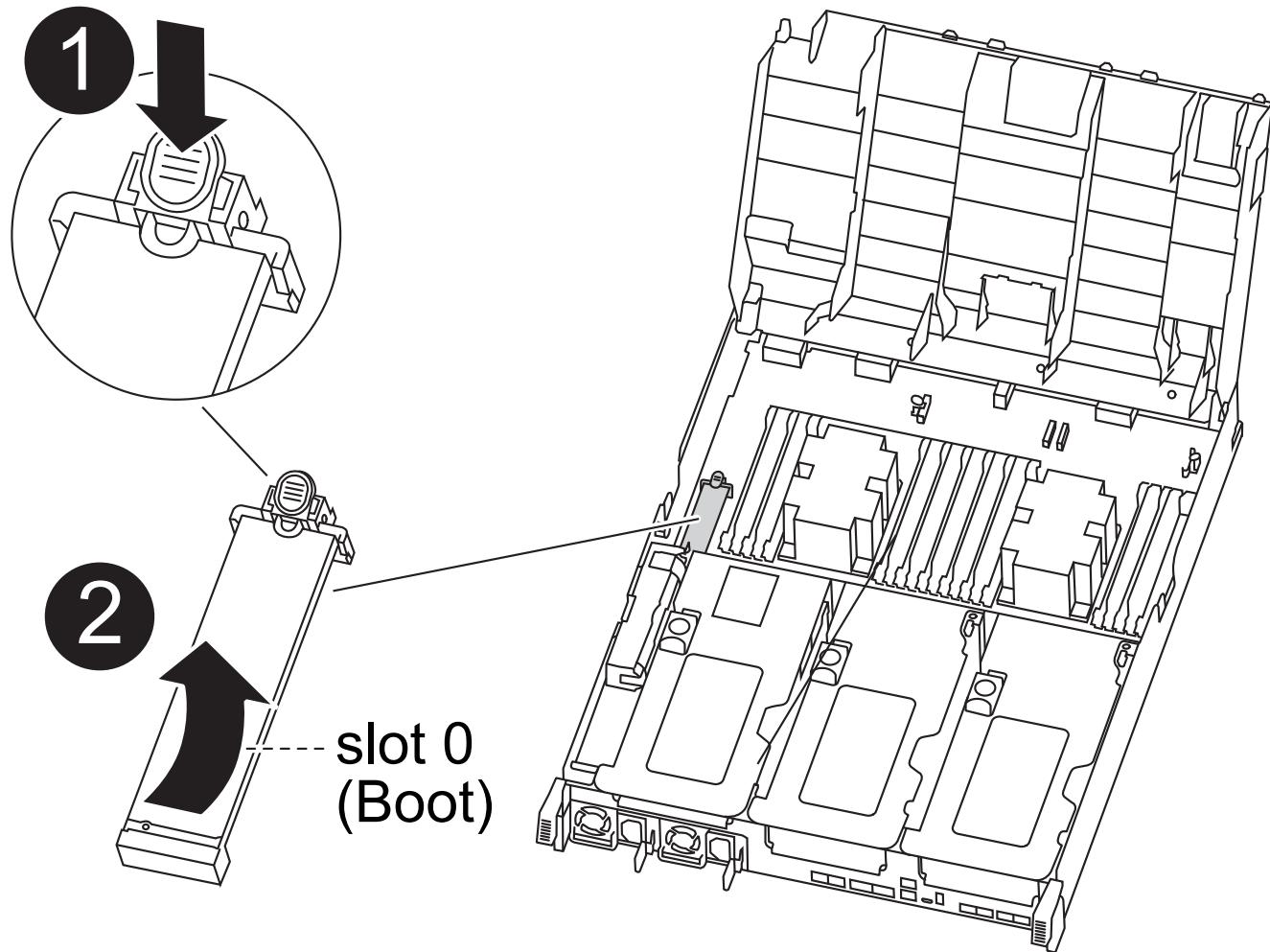
1. Aprire il condotto dell'aria:



1	Linguette di bloccaggio
2	Far scorrere il condotto dell'aria verso la parte posteriore del controller
3	Ruotare il condotto dell'aria verso l'alto

- Premere le linguette di bloccaggio sui lati del condotto dell'aria verso il centro del modulo controller.
- Far scorrere il condotto dell'aria verso la parte posteriore del modulo controller, quindi ruotarlo verso l'alto fino a portarlo in posizione completamente aperta.

2. Individuare e rimuovere il supporto di avvio dal modulo controller:



1	Premere il tasto blu
2	Ruotare il supporto di avvio verso l'alto e rimuoverlo dallo zoccolo

- Premere il tasto blu alla fine del supporto di avvio fino a quando il labbro sul supporto di avvio non scompare dal pulsante blu.
 - Ruotare il supporto di avvio verso l'alto ed estrarre delicatamente il supporto di avvio dalla presa.
- Allineare i bordi del supporto di avvio sostitutivo con lo zoccolo del supporto di avvio, quindi spingerlo delicatamente nello zoccolo.
 - Verificare che il supporto di avvio sia inserito correttamente e completamente nella presa.

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

- Bloccare il supporto di avvio in posizione:
 - Ruotare il supporto di avvio verso il basso verso la scheda madre.
 - Posizionando un dito alla fine del supporto di avvio tramite il pulsante blu, premere l'estremità del supporto di avvio per attivare il pulsante di blocco blu.
 - Tenendo premuto il supporto di avvio, sollevare il pulsante di blocco blu per bloccare il supporto di

avvio in posizione.

6. Chiudere il condotto dell'aria.

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

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

Prima di iniziare

- È necessario disporre di un'unità flash USB, formattata in MBR/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 di `var` file system.

Fasi

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



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

Il file di immagine del servizio decompresso contiene due cartelle:

- boot
- efi

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



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

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

2. In caso contrario, chiudere il condotto dell'aria.
3. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

4. Reinstallare il dispositivo di gestione dei cavi e rieseguire il sistema secondo necessità.

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

5. Collegare il cavo di alimentazione all'alimentatore e reinstallare il fermo del cavo di alimentazione.

6. 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.

7. Completare l'installazione del modulo controller:

- a. Collegare il cavo di alimentazione all'alimentatore, reinstallare il collare di bloccaggio del cavo di alimentazione, quindi collegare l'alimentatore alla fonte di alimentazione.
- b. Spingere con decisione il modulo controller nello chassis fino a quando non raggiunge la scheda intermedia e non è completamente inserito.

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



Non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio per evitare di danneggiare i connettori.

Il modulo controller inizia ad avviarsi non appena viene inserito completamente nello chassis. Prepararsi ad interrompere il processo di avvio.

- a. Ruotare i fermi di bloccaggio verso l'alto, inclinandoli in modo da liberare i perni di bloccaggio, quindi abbassarli in posizione di blocco.
- b. Se non è già stato fatto, reinstallare il dispositivo di gestione dei cavi.

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

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

9. 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 initiator adapter_name`
- c. Halt per tornare alla modalità di manutenzione: `halt`

Le modifiche verranno implementate all'avvio del sistema.

Avviare l'immagine di ripristino - AFF C400

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

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. Se richiesto sul controller danneggiato, premere Y per 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](#)".

Switch back aggregates in una configurazione MetroCluster a due nodi - AFF C400

Una volta completata la sostituzione dell'unità FRU in una configurazione MetroCluster a due nodi, è possibile eseguire l'operazione di switchback dell'unità MetroCluster. In questo modo, la configurazione torna al suo normale stato operativo, con le macchine virtuali dello storage di origine sincronizzata (SVM) sul sito precedentemente compromesso ora attive e che forniscono i dati dai pool di dischi locali.

Questa attività si applica solo alle configurazioni MetroCluster a due nodi.

Fasi

1. Verificare che tutti i nodi si trovino in `enabled` stato: `metrocluster node show`

```
cluster_B::> metrocluster node show

DR          Configuration  DR
Group Cluster Node  State      Mirroring Mode
-----  -----
-----  -----
1      cluster_A
      controller_A_1 configured  enabled    heal roots
completed
      cluster_B
      controller_B_1 configured  enabled    waiting for
switchback recovery
2 entries were displayed.
```

2. Verificare che la risincronizzazione sia completa su tutte le SVM: `metrocluster vserver show`
3. Verificare che tutte le migrazioni LIF automatiche eseguite dalle operazioni di riparazione siano state completate correttamente: `metrocluster check lif show`
4. Eseguire lo switchback utilizzando `metrocluster switchback` comando da qualsiasi nodo del cluster esistente.
5. Verificare che l'operazione di switchback sia stata completata: `metrocluster show`

L'operazione di switchback è ancora in esecuzione quando un cluster si trova in `waiting-for-switchback` stato:

```
cluster_B::> metrocluster show
Cluster          Configuration State    Mode
-----
Local: cluster_B configured          switchover
Remote: cluster_A configured        waiting-for-switchback
```

L'operazione di switchback è completa quando i cluster si trovano in `normal` stato:

```
cluster_B::> metrocluster show
Cluster          Configuration State    Mode
-----
Local: cluster_B configured          normal
Remote: cluster_A configured        normal
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando `metrocluster config-replication resync-status show` comando.

6. Ripristinare le configurazioni SnapMirror o SnapVault.

Ripristinare la crittografia - AFF C400

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 <div data-bbox="638 354 1470 1170" style="border: 1px solid #ccc; padding: 10px; border-radius: 10px;"><p>Please choose one of the following:</p><ul style="list-style-type: none">(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.<p>Selection (1-11)? 10</p></div>

Versione di ONTAP	Selezionare questa opzione
ONTAP 9.7 e versioni precedenti	<p>Selezionare l'opzione nascosta <code>recover_onboard_keymanager</code></p> <p>Mostra un esempio di menu di avvio</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager</pre> </div>

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

Mostra prompt di esempio

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

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

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

Mostra prompt di esempio

Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:

5. Immettere le informazioni di backup.

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

Mostra prompt di esempio

Enter the backup data:

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-----  
<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
```

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....  
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 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 immettendo il seguente comando.

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

Restituire il componente guasto a NetApp - AFF C400

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

Informazioni sul copyright

Copyright © 2025 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 COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.