Supporto di avvio - ripristino automatico

Install and maintain

NetApp
February 13, 2026

Sommario

Supporto di avvio - ripristino automatico

Flusso di lavoro di ripristino automatico dei boot media - ASA C250

Il ripristino automatico dell'immagine di boot prevede che il sistema identifichi e selezioni automaticamente l'opzione appropriata del menu di boot. Utilizza l'immagine di boot sul nodo partner per reinstallare ONTAP sul supporto di boot sostitutivo nel sistema storage ASA C250.

Il processo di ripristino automatico del supporto di avvio è supportato solo in ONTAP 9.18.1 e versioni successive. Se il sistema storage esegue una versione precedente di ONTAP, utilizzare il "procedura di ripristino manuale dell'avvio".

Per iniziare, rivedere i requisiti di sostituzione, arrestare il controller, sostituire il supporto di avvio, consentire al sistema di ripristinare l'immagine e verificare la funzionalità del sistema.

1. **"Esaminare i requisiti dei supporti di avvio"**

Esaminare i requisiti per la sostituzione dei supporti di avvio.

2. **"Spegnere il controller"**

Arrestare il controller nel sistema di storage quando è necessario sostituire i supporti di avvio.

3. **"Sostituire il supporto di avvio"**

Rimuovere il supporto di avvio non riuscito dal modulo controller e installare il supporto di avvio sostitutivo.

4. **"Ripristinare l'immagine sul supporto di avvio"**

Ripristinare l'immagine ONTAP dal controller partner.

5. **"Restituire la parte guasta a NetApp"**

Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Requisiti per il ripristino automatico dei supporti di boot - ASA C250

Prima di sostituire il boot media nel tuo ASA C250, assicurati di soddisfare i requisiti necessari per una sostituzione corretta. Ciò include la verifica di avere il boot media sostitutivo corretto, la conferma che la porta e0S (e0M wrench) sul controller guasto non sia difettosa e la determinazione se Onboard Key Manager (OKM) o External Key Manager (EKM) siano abilitati.

Il processo di ripristino automatico del supporto di avvio è supportato solo in ONTAP 9.18.1 e versioni successive. Se il sistema storage esegue una versione precedente di ONTAP, utilizzare il "procedura di ripristino manuale dell'avvio".

- È necessario sostituire il componente guasto con un componente FRU sostitutivo della stessa capacità ricevuta da NetApp.
- Verificare che la porta e0M (chiave inglese) sul controller danneggiato sia collegata e non sia difettosa.

  La porta e0M viene utilizzata per comunicare tra i due controller durante il processo di ripristino automatico dell'avvio.

- Per OKM, è necessaria la passphrase dell'intero cluster e anche i dati di backup.
- Per EKM, è necessario copiare i seguenti file dal nodo partner:
  - file /cfcard/kmip/servers.cfg.
  - file /cfcard/kmip/certs/client.crt.
  - file /cfcard/kmip/certs/client.key.
  - File /cfcard/kmip/certs/CA.pem.
- Quando si sostituisce il supporto di avvio danneggiato, è fondamentale applicare i comandi al controller corretto:
  - Il *controller non funzionante* è il controller su cui si sta eseguendo la manutenzione.
  - Il *controllore sano* è il partner HA del controllore compromesso.

Cosa succederà

Dopo aver esaminato i requisiti dei supporti di avvio, si "spegnere il controller".

Arrestare il controller per il ripristino automatico del boot media - ASA C250

Arresta il controller danneggiato nel tuo sistema storage ASA C250 per evitare la perdita di dati e mantenere la stabilità del sistema durante il processo automatico di ripristino del supporto di boot.

Il processo di ripristino automatico del supporto di avvio è supportato solo in ONTAP 9.18.1 e versioni successive. Se il sistema storage esegue una versione precedente di ONTAP, utilizzare il "procedura di ripristino manuale dell'avvio".

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 aver controllato i messaggi di evento `cluster kernel-service show`) per il blade SCSI del controller danneggiato. Il `cluster kernel-service show` comando (dalla modalità avanzata precedente) visualizza il nome del nodo, "stato 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=<# of hours>h
   ```

   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. Disattiva la restituzione automatica:
   a. Immettere il seguente comando dalla console del controller funzionante:

      ```
      storage failover modify -node impaired_node_name -auto-giveback false
      ```

   b. Entra `y` quando vedi il messaggio *Vuoi disattivare la restituzione automatica?*
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 -halt true` Il parametro *-halt true* consente di visualizzare il prompt di Loader.

Cosa succederà

Dopo aver spento il controller danneggiato, si "sostituire il supporto di avvio".

Sostituire il boot media per il ripristino automatico dell'avvio - ASA C250

Il boot media nel sistema ASA C250 memorizza i dati essenziali del firmware e della configurazione. Il processo di sostituzione prevede la rimozione e l'apertura del modulo controller, la rimozione del boot media danneggiato, l'installazione del boot media sostitutivo nel modulo controller e quindi la reinstallazione del modulo controller.

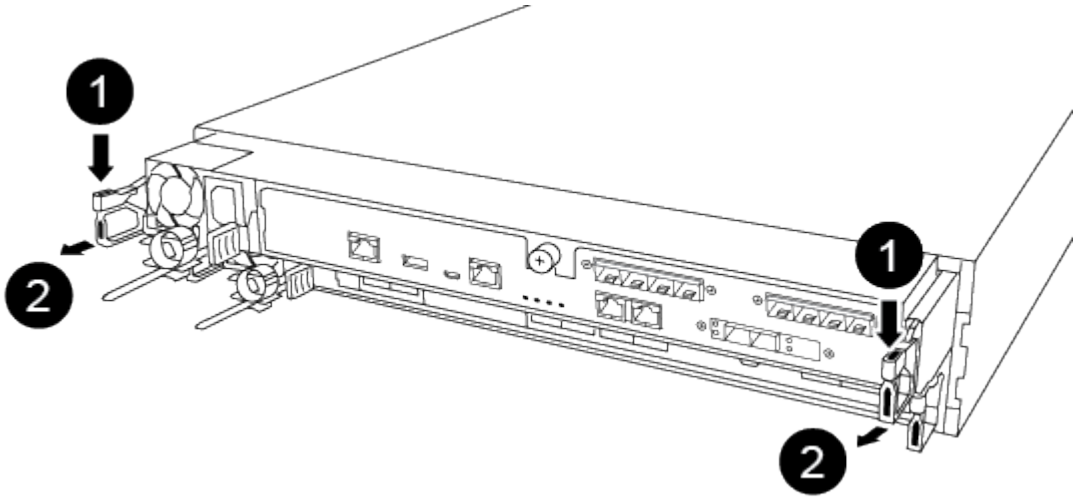
Il processo di ripristino automatico del supporto di avvio è supportato solo in ONTAP 9.18.1 e versioni successive. Se il sistema storage esegue una versione precedente di ONTAP, utilizzare il "procedura di ripristino manuale dell'avvio".

Il supporto di avvio si trova all'interno del modulo controller sotto il condotto dell'aria ed è accessibile rimuovendo il modulo controller dal sistema.

Fase 1: Rimuovere il modulo controller

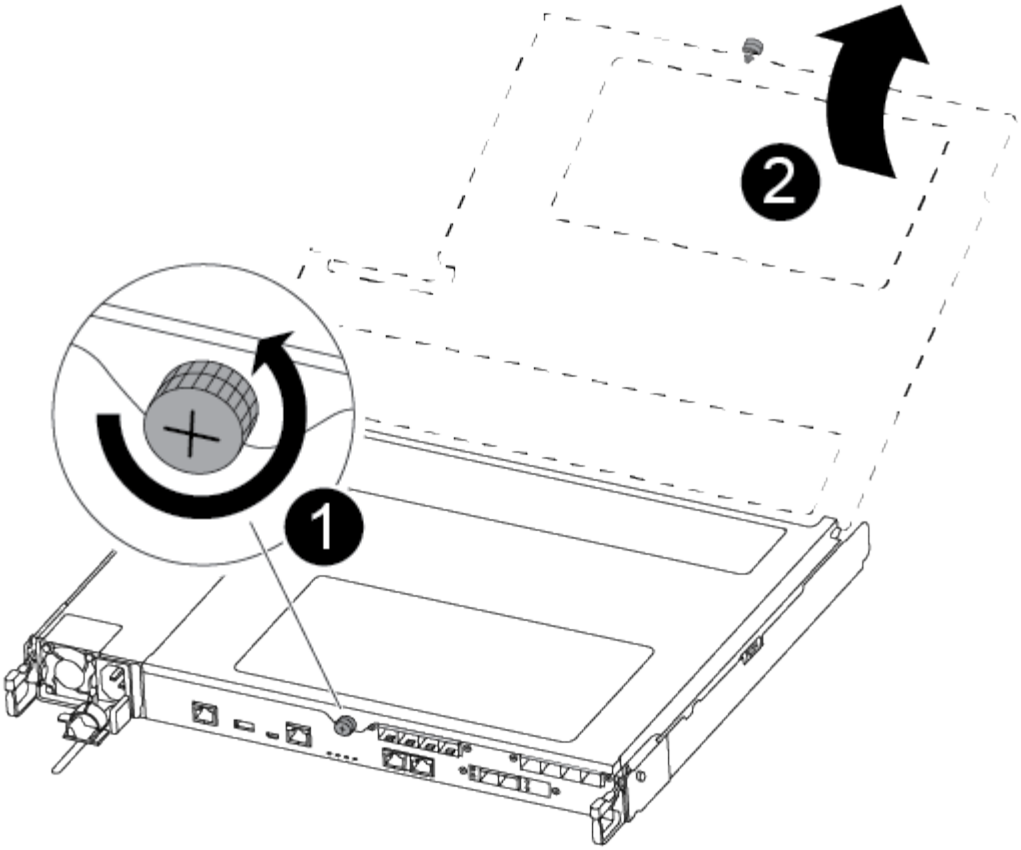
1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Scollegare gli alimentatori del modulo controller dalla fonte di alimentazione.
3. Rilasciare i fermi dei cavi di alimentazione, quindi scollegare i cavi dagli alimentatori.
4. Scollegare i cavi i/o dal modulo controller.
5. Inserire l'indice nel meccanismo di blocco su entrambi i lati del modulo controller, premere la leva con il pollice ed estrarre delicatamente il controller dal telaio.

> In caso di difficoltà nella rimozione del modulo controller, posizionare le dita di riferimento attraverso i fori all'interno (incrociando le braccia).



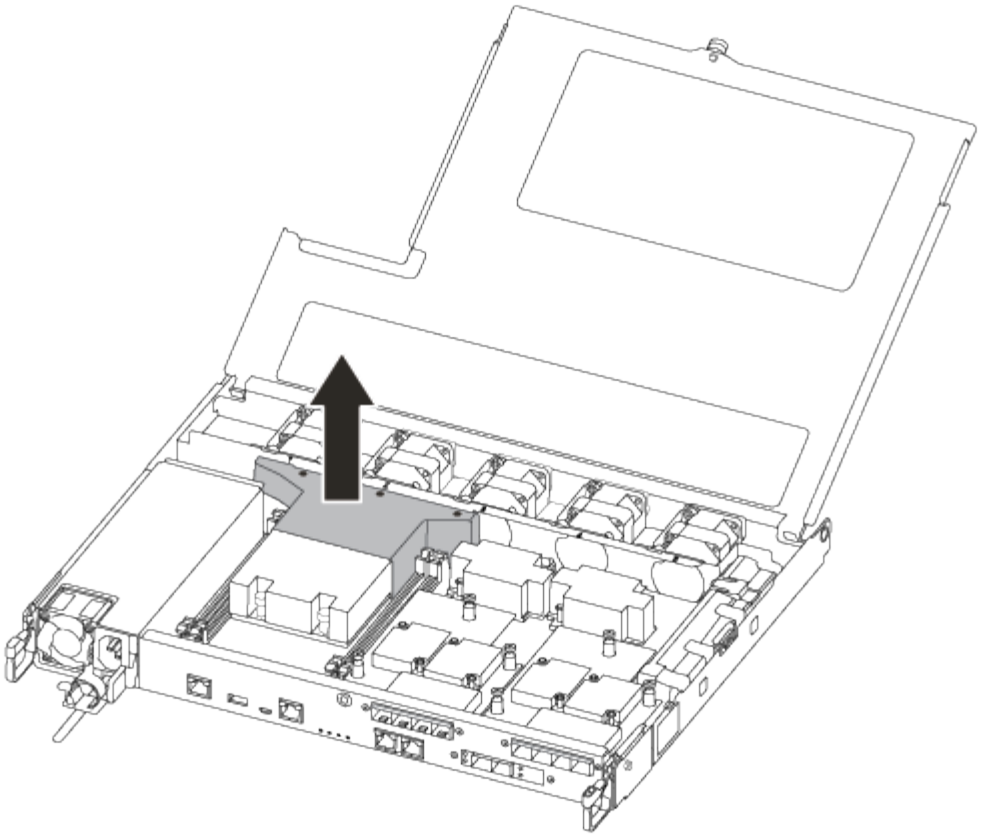
1	Leva
2	Meccanismo di blocco

6. Con entrambe le mani, afferrare i lati del modulo controller ed estrarlo delicatamente dallo chassis e posizionare il modulo su una superficie piana e stabile.
7. Ruotare la vite a testa zigrinata sulla parte anteriore del modulo controller in senso antiorario e aprire il coperchio del modulo controller.



1	Vite a testa zigrinata
2	Coperchio del modulo controller.

8. Estrarre il coperchio del condotto dell’aria.



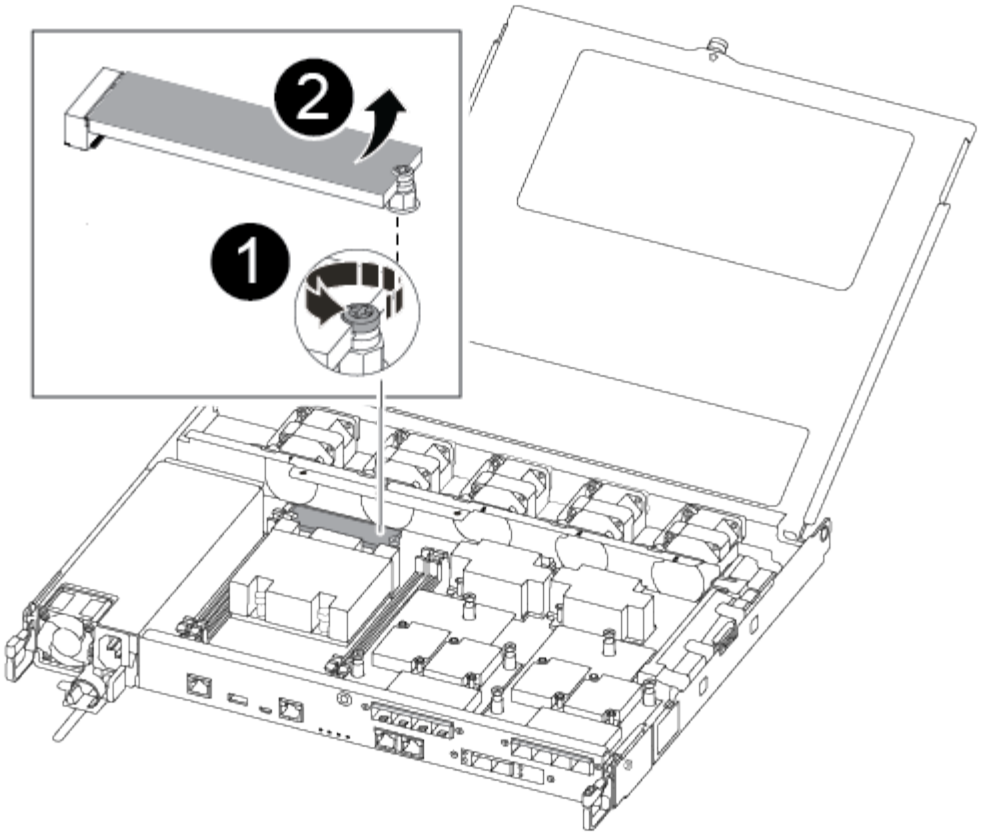
Fase 2: Sostituire il supporto di avvio

Per sostituire il supporto di avvio, è possibile utilizzare il seguente video o la procedura tabulare:

Animazione - sostituire il supporto di avvio

1. Individua e sostituisci il supporto di avvio danneggiato dal modulo controller:

> Per rimuovere la vite che tiene in posizione il supporto di avvio, è necessario un cacciavite a croce magnetico n. 1. A causa dei limiti di spazio all'interno del modulo controller, è necessario disporre anche di un magnete per trasferire la vite in modo da non perderla.

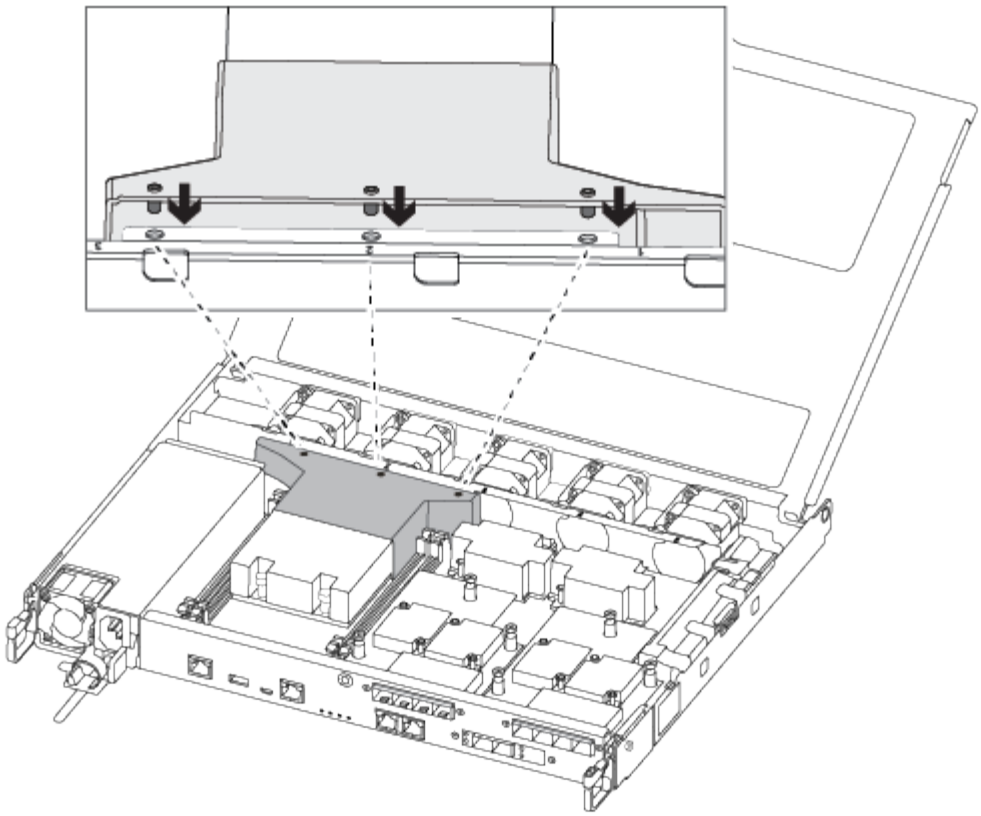


1	Rimuovere la vite che fissa il supporto di avvio alla scheda madre nel modulo controller.
2	Estrarre il supporto di avvio dal modulo controller.

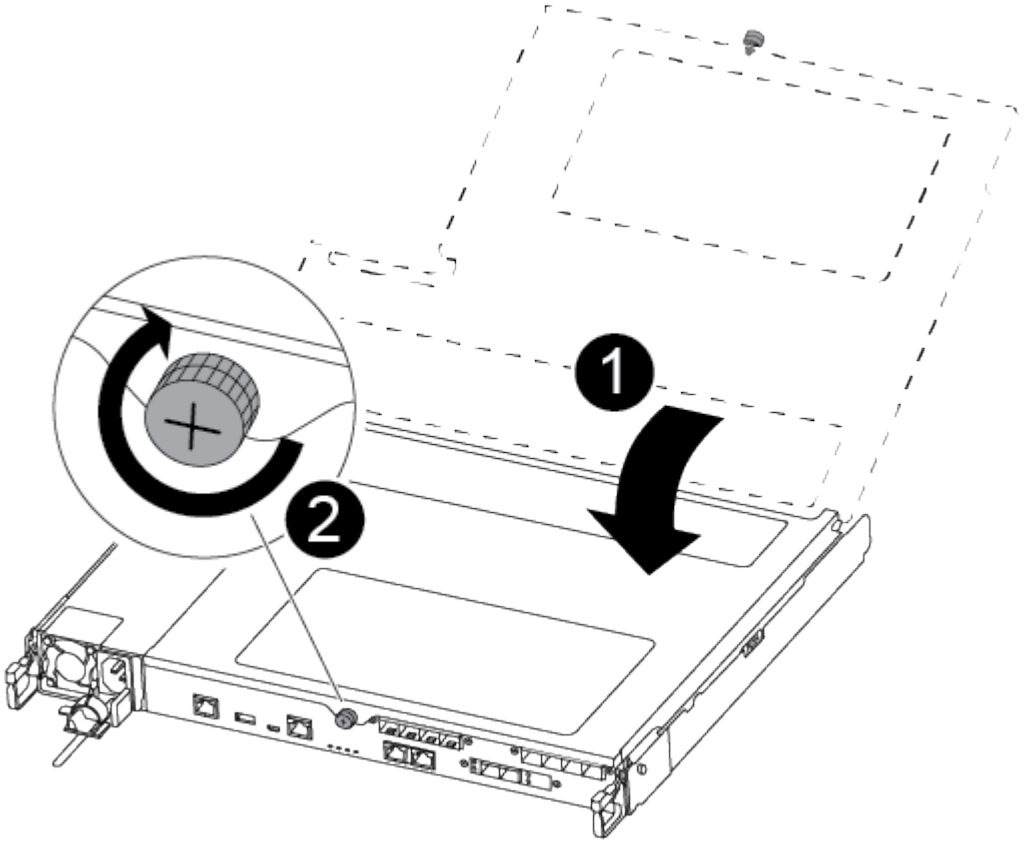
a. Utilizzando il cacciavite magnetico n. 1, rimuovere la vite dal supporto di avvio compromesso e metterla da parte in modo sicuro sul magnete.
b. Sollevare delicatamente il supporto di avvio compromesso direttamente dalla presa e metterlo da parte.
c. Rimuovere il supporto di avvio sostitutivo dalla confezione antistatica e allinearlo in posizione sul modulo controller.
d. Utilizzando il cacciavite magnetico n. 1, inserire e serrare la vite sul supporto di avvio.

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

e. Installare il condotto dell'aria.



f. Chiudere il coperchio del modulo controller e serrare la vite a testa zigrinata.



1	Coperchio del modulo controller
2	Vite a testa zigrinata

2. 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. Inserire completamente il modulo controller nello chassis:
   c. Posizionare le dita di riferimento attraverso i fori per le dita dall'interno del meccanismo di blocco.
   d. Premere i pollici verso il basso sulle linguette arancioni sulla parte superiore del meccanismo di blocco e spingere delicatamente il modulo controller oltre il fermo.
   e. Rilasciare i pollici dalla parte superiore dei meccanismi di blocco e continuare a spingere fino a quando i meccanismi di blocco non scattano in posizione.

      Il modulo controller deve essere inserito completamente e a filo con i bordi dello chassis.
3. Ricollegare i cavi i/o del modulo controller.
4. Inserire i cavi di alimentazione negli alimentatori, reinstallare il collare di bloccaggio del cavo di alimentazione, quindi collegare gli alimentatori alla fonte di alimentazione.

   Il modulo controller inizia l'avvio e si arresta al prompt LOADER.

Cosa succederà

Dopo aver sostituito fisicamente i supporti di avvio danneggiati, "Ripristinare l'immagine ONTAP dal nodo partner".

Ripristino automatico del supporto di boot dal nodo partner - ASA C250

Dopo aver installato il nuovo boot media device nel sistema ASA C250, puoi avviare il processo automatico di ripristino del boot media per ripristinare la configurazione dal nodo partner. Durante il processo di ripristino, il sistema verifica se la crittografia è abilitata e determina il tipo di key encryption in uso. Se la key encryption è abilitata, il sistema ti guida attraverso i passaggi appropriati per ripristinarla.

Il processo di ripristino automatico del supporto di avvio è supportato solo in ONTAP 9.18.1 e versioni successive. Se il sistema storage esegue una versione precedente di ONTAP, utilizzare il "procedura di ripristino manuale dell'avvio".

Prima di iniziare

- Determina il tipo di gestore delle chiavi:
  - Onboard Key Manager (OKM): richiede passphrase e dati di backup per l'intero cluster
  - External Key Manager (EKM): richiede i seguenti file dal nodo partner:
    - `/cfcard/kmip/servers.cfg`

- `/cfcard/kmip/certs/client.crt`
- `/cfcard/kmip/certs/client.key`
- `/cfcard/kmip/certs/CA.pem`

Fasi

1. Dal prompt LOADER, avviare il processo di ripristino del supporto di avvio:

   `boot_recovery -partner`

   Sullo schermo viene visualizzato il seguente messaggio:

   `Starting boot media recovery (BMR) process. Press Ctrl-C to abort…`

2. Monitorare il processo di ripristino dell'installazione dei supporti di avvio.

   Il processo viene completato e viene visualizzato il `Installation complete` messaggio.

3. Il sistema verifica la crittografia e visualizza uno dei seguenti messaggi:

Se viene visualizzato questo messaggio…	Eseguire questa operazione…
`key manager is not configured. Exiting.`	La crittografia non è installata sul sistema. a. Attendi che venga visualizzato il prompt di accesso. b. Accedi al nodo e restituisci lo storage: `storage failover giveback -ofnode` *`impaired_node_name`* c. Vai a riattivazione della restituzione automatica se fosse disabilitato.
`key manager is configured.`	La crittografia è installata. Vai aripristino del gestore delle chiavi .

> Se il sistema non riesce a identificare la configurazione del gestore delle chiavi, visualizza un messaggio di errore e chiede di confermare se il gestore delle chiavi è configurato e di che tipo (integrato o esterno). Rispondi alle richieste per procedere.

4. Ripristina il key manager utilizzando la procedura appropriata per la tua configurazione:

Onboard Key Manager (OKM)

Il sistema visualizza il seguente messaggio e inizia a eseguire l'opzione BootMenu 10:

```
key manager is configured.
Entering Bootmenu Option 10...

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

a. Entra `y` alla richiesta di conferma di voler avviare il processo di ripristino OKM.
b. Quando richiesto, immettere la passphrase per la gestione delle chiavi integrate.
c. Quando richiesto, immettere nuovamente la passphrase per confermare.
d. Quando richiesto, immettere i dati di backup per il gestore delle chiavi integrato.

Mostra un esempio di richiesta di passphrase e dati di backup

```
Enter the passphrase for onboard key management:
-----BEGIN PASSPHRASE-----
<passphrase_value>
-----END PASSPHRASE-----
Enter the passphrase again to confirm:
-----BEGIN PASSPHRASE-----
<passphrase_value>
-----END PASSPHRASE-----
Enter the backup data:
-----BEGIN BACKUP-----
<passphrase_value>
-----END BACKUP-----
```

e. Monitorare il processo di ripristino mentre ripristina i file appropriati dal nodo partner.

Una volta completato il processo di ripristino, il nodo si riavvia. I seguenti messaggi indicano un ripristino riuscito:

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.keydb file.

Successfully recovered keymanager secrets.
```

f. Dopo il riavvio del nodo, verificare che il sistema sia di nuovo online e operativo.

g. Riportare la centralina guasta al normale funzionamento restituendo la memoria:

   `storage failover giveback -ofnode impaired_node_name`

h. Dopo che il nodo partner è completamente attivo e fornisce dati, sincronizzare le chiavi OKM nel cluster:

   `security key-manager onboard sync`

   Vai a riattivazione della restituzione automatica se fosse disabilitato.

Gestore chiavi esterno (EKM)

Il sistema visualizza il seguente messaggio e inizia a eseguire l'opzione BootMenu 11:

```
key manager is configured.
Entering Bootmenu Option 11...
```

a. Quando richiesto, immettere le impostazioni di configurazione EKM:

   i. Immettere il contenuto del certificato client da `/cfcard/kmip/certs/client.crt` file:

      Mostra un esempio di contenuto del certificato client

      ```
      -----BEGIN CERTIFICATE-----
      <certificate_value>
      -----END CERTIFICATE-----
      ```

   ii. Immettere il contenuto del file chiave client da `/cfcard/kmip/certs/client.key` file:

      Mostra un esempio di contenuto del file della chiave client

      ```
      -----BEGIN RSA PRIVATE KEY-----
      <key_value>
      -----END RSA PRIVATE KEY-----
      ```

   iii. Immettere il contenuto del file CA del server KMIP da `/cfcard/kmip/certs/CA.pem` file:

      Mostra un esempio del contenuto del file del server KMIP

      ```
      -----BEGIN CERTIFICATE-----
      <KMIP_certificate_CA_value>
      -----END CERTIFICATE-----
      ```

iv. Immettere il contenuto del file di configurazione del server da `/cfcard/kmip/servers.cfg` file:

Mostra un esempio del contenuto del file di configurazione del server

```
xxx.xxx.xxx.xxx:5696.host=xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx:5696.port=5696
xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4
1xxx.xxx.xxx.xxx:5696.timeout=25
xxx.xxx.xxx.xxx:5696.nbio=1
xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.cr
t
xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key
xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:
!RC2:!RC4:!SEED:!eNULL:!aNULL"
xxx.xxx.xxx.xxx:5696.verify=true
xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value>
```

v. Se richiesto, immettere l'UUID del cluster ONTAP dal nodo partner. È possibile controllare l'UUID del cluster dal nodo partner utilizzando `cluster identify show` comando.

Mostra un esempio di prompt UUID del cluster ONTAP

```
Notice: bootarg.mgwd.cluster_uuid is not set or is empty.
Do you know the ONTAP Cluster UUID? {y/n} y
Enter the ONTAP Cluster UUID: <cluster_uuid_value>


System is ready to utilize external key manager(s).
```

vi. Se richiesto, immettere l'interfaccia di rete temporanea e le impostazioni per il nodo:

- L'indirizzo IP per la porta
- La netmask per la porta
- L'indirizzo IP del gateway predefinito

Mostra un esempio di richieste di impostazione di rete temporanee

```
In order to recover key information, a temporary network
interface needs to be
configured.

Select the network port you want to use (for example,
'e0a')
e0M

Enter the IP address for port : xxx.xxx.xxx.xxx
Enter the netmask for port : xxx.xxx.xxx.xxx
Enter IP address of default gateway: xxx.xxx.xxx.xxx
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
```

b. Verificare lo stato di ripristino della chiave:

- Se vedi `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` nell'output, la configurazione EKM è stata ripristinata correttamente. Il processo ripristina i file appropriati dal nodo partner e riavvia il nodo. Procedere al passaggio successivo.
- Se il ripristino della chiave non riesce, il sistema si blocca e visualizza messaggi di errore e di avviso. Eseguire nuovamente il processo di ripristino dal prompt LOADER: `boot_recovery -partner`

Mostrare un esempio di messaggi di errore e di avvertenza relativi al ripristino della chiave

```
ERROR: kmip_init: halting this system with encrypted
mroot...
WARNING: kmip_init: authentication keys might not be
available.
*****************************************************
*                 A T T E N T I O N                 *
*                                                   *
*       System cannot connect to key managers.      *
*                                                   *
*****************************************************
ERROR: kmip_init: halting this system with encrypted
mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

c. Dopo il riavvio del nodo, verificare che il sistema sia di nuovo online e operativo.

d. Riportare il controller al funzionamento normale restituendo lo storage:

```
storage failover giveback -ofnode impaired_node_name
```

Vai a riattivazione della restituzione automatica se fosse disabilitato.

5. Se il giveback automatico è stato disabilitato, riabilitalo:

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

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

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

Cosa succederà

Dopo aver ripristinato l'immagine ONTAP e dopo aver attivato e distribuito i dati, si "Restituire la parte guasta a NetApp".

Restituire il supporto di avvio non riuscito a NetApp - ASA C250

Se un componente nel tuo sistema ASA C250 si guasta, restituisci la parte guasta a NetApp. Vedi la "Restituzione e sostituzione delle parti" pagina per ulteriori informazioni.

Informazioni sul copyright

Informazioni sul marchio commerciale