Metodo manuale

Install and maintain

NetApp
September 25, 2024

Sommario

Metodo manuale

Flusso di lavoro per la sostituzione dei supporti di avvio - ASA A70 e ASA A90

Per sostituire i supporti di avvio, attenersi alla procedura riportata di seguito.

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

Per sostituire i supporti di avvio, è necessario soddisfare determinati requisiti.

2. **"Controllare le chiavi di crittografia integrate"**

Verificare se il sistema dispone di un gestore delle chiavi di sicurezza abilitato o di dischi crittografati.

3. **"Spegnere il controller compromesso"**

Spegnere o sostituire il controller danneggiato in modo che il controller integro continui a erogare dati dallo storage del controller danneggiato.

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

Rimuovere il supporto di avvio guasto dal modulo di gestione del sistema e installare il supporto di avvio sostitutivo, quindi trasferire un'immagine ONTAP utilizzando un'unità flash USB sul supporto di avvio sostitutivo.

5. **"Avviare l'immagine di ripristino"**

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

6. **"Ripristino della crittografia"**

Ripristinare la configurazione del gestore delle chiavi integrato o del gestore delle chiavi esterno dal menu di avvio ONATP.

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

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

Requisiti di sostituzione dei supporti di avvio - ASA A70 e ASA A90

Prima di sostituire il supporto di avvio, verificare i seguenti requisiti.

- È necessario disporre di un'unità flash USB, formattata in FAT32, con la quantità di storage appropriata per contenere `image_xxx.tgz`.
- È necessario copiare il `image_xxx.tgz` file nell'unità flash USB per utilizzarlo successivamente in questa procedura.
- È necessario sostituire il componente guasto con un componente FRU sostitutivo ricevuto dal provider.
- È importante applicare i comandi descritti di seguito al controller corretto:
  - Il controller *alterato* è il controller su cui si esegue la manutenzione.
  - Il controller *healthy* è il partner ha del controller compromesso.

Controllare le chiavi di crittografia integrate - ASA A70 e ASA A90

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 la versione di ONTAP in esecuzione.

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".

Controllare NVE o NSE sui sistemi

Prima di arrestare il controller danneggiato, è necessario verificare se il sistema ha attivato il gestore delle chiavi di sicurezza o dischi crittografati.

Verificare la configurazione del gestore delle chiavi di protezione

Fasi

1. Determinare se Key Manager è attivo con il comando *Security key-manager keystore show*. Per ulteriori informazioni, consultare la "Security key-manager keystore mostra pagina MAN"

   È possibile che si disponga di altri tipi di gestore delle chiavi. I tipi sono `KMIP`, , `AKV`e `GCP`. Il processo di conferma di questi tipi è lo stesso dei tipi di gestore delle chiavi o di conferma `external` `onboard` .

   - Se non viene visualizzata alcuna uscita, andare a "spegnere il controller danneggiato" per arrestare il nodo danneggiato.
   - Se il comando visualizza output, il sistema è `security key-manager` attivo ed è necessario visualizzare il tipo e lo `Key Manager` stato.
2. Visualizzare le informazioni per l'attivo `Key Manager` utilizzando il comando *Security key-manager key query*.
   - Se `Key Manager` viene visualizzato il tipo `external` e la `Restored` colonna visualizza `true`, è possibile spegnere il controller danneggiato in tutta sicurezza.
   - Se viene visualizzato il `Key Manager` tipo `onboard` e la `Restored` colonna viene visualizzata `true`, è necessario completare alcuni passaggi aggiuntivi.
   - Se il `Key Manager` tipo viene visualizzato `external` e la `Restored` colonna visualizza qualcosa di

diverso da `true`, è necessario completare alcuni passaggi aggiuntivi.

- Se il `Key Manager` tipo viene visualizzato `onboard` e la `Restored` colonna visualizza qualcosa di diverso da `true`, è necessario completare alcuni passaggi aggiuntivi.

3. Se viene visualizzato il `Key Manager` tipo `onboard` e viene visualizzata la `Restored` colonna `true`, eseguire manualmente il backup delle informazioni OKM:
   a. Immettere `y` quando viene richiesto di continuare: `set -priv advanced`
   b. Immettere il comando per visualizzare le informazioni sulla gestione delle chiavi: *Security key-manager onboard show-backup*
   c. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
   d. È possibile arrestare il controller danneggiato in modo sicuro.
4. Se il `Key Manager` tipo viene visualizzato `onboard` e la `Restored` colonna visualizza qualcosa di diverso da `true`:
   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 integrata alfanumerica di 32 caratteri al prompt. Se non è possibile fornire la passphrase, contattare l'assistenza NetApp. "mysupport.netapp.com"

   b. Verificare che venga visualizzata la `Restored` colonna `true` per tutte le chiavi di autenticazione: `security key-manager key query`
   c. Verificare che il `Key Manager` tipo sia visualizzato `onboard`, quindi eseguire manualmente il backup delle informazioni OKM.
   d. Immettere il comando per visualizzare le informazioni di backup della 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. È possibile spegnere il controller in modo sicuro.
5. Se il `Key Manager` tipo viene visualizzato `external` e la `Restored` colonna visualizza qualcosa di diverso da `true`:
   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 l'assistenza NetApp all'indirizzo "mysupport.netapp.com".

   b. Verificare che venga visualizzata la `Restored` colonna `true` per tutte le chiavi di autenticazione: *Security key-manager key query*
   c. È possibile arrestare il controller danneggiato in modo sicuro.

Spegnere il controller - ASA A70 e ASA A90

Dopo aver completato le attività NVE o NSE, è necessario completare l'arresto del controller compromesso. Spegnere o sostituire il controller 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 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, 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, sospendere la creazione automatica dei casi 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. 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`.

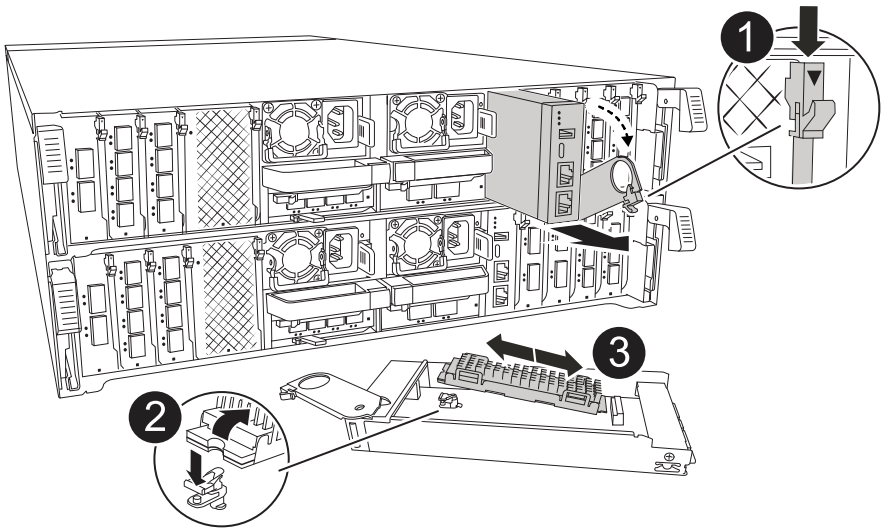
Sostituire i supporti di avvio - ASA A70 e ASA A90

Per sostituire il supporto di avvio, è necessario rimuovere il modulo di gestione del sistema dal retro del sistema, rimuovere il supporto di avvio danneggiato e installare il

supporto di avvio sostitutivo nel modulo di gestione del sistema.

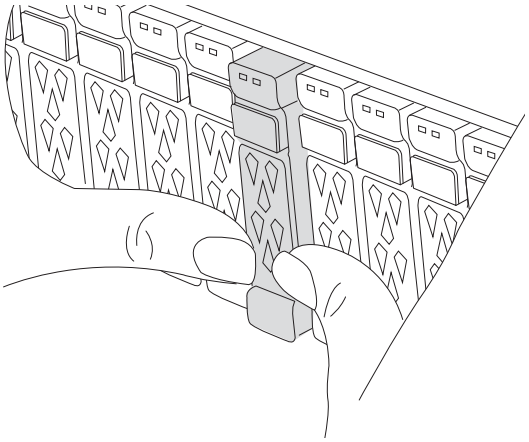
Fase 1: Sostituire il supporto di avvio

Il supporto di avvio si trova all'interno del modulo di gestione del sistema ed è accessibile rimuovendo il modulo dal sistema.



1	Dispositivo di chiusura della camma del modulo di gestione del sistema
2	Pulsante di blocco dei supporti di avvio
3	Supporto di boot

1. Nella parte anteriore dello chassis, premere con decisione ciascun disco fino a quando non si avverte un arresto positivo. In questo modo, i dischi sono posizionati saldamente sulla scheda intermedia dello chassis.



2. Andare sul retro del telaio. Se non si è già collegati a terra, mettere a terra l'utente.
3. Scollegare l'alimentazione al modulo controller estraendo il modulo controller di circa tre pollici:
    a. Premere verso il basso entrambi i fermi di bloccaggio del modulo controller, quindi ruotare entrambi i fermi contemporaneamente verso il basso.
    b. Estrarre il modulo controller di circa 3 pollici dal telaio per disinserire l'alimentazione.
    c. Rimuovere tutti i cavi collegati al modulo di gestione del sistema. Assicurarsi di etichettare il punto in cui sono stati collegati i cavi, in modo da poterli collegare alle porte corrette quando si reinstalla il modulo.
    d. Ruotare il vassoio di gestione dei cavi verso il basso tirando i pulsanti su entrambi i lati all'interno del vassoio di gestione dei cavi, quindi ruotare il vassoio verso il basso.
    e. Premere il pulsante della camma di gestione del sistema. La leva della camma si allontana dal telaio.
    f. Ruotare la leva della camma completamente verso il basso e rimuovere il modulo di gestione del sistema dal modulo controller.
    g. Posizionare il modulo di gestione del sistema su un tappetino antistatico, in modo che il supporto di avvio sia accessibile.
4. Rimuovere il supporto di avvio dal modulo di gestione:
    a. Premere il pulsante di bloccaggio blu.
    b. Ruotare il supporto di avvio verso l'alto, farlo scorrere fuori dallo zoccolo e metterlo da parte.
5. Installare il supporto di avvio sostitutivo nel modulo di gestione del sistema:
    a. Allineare i bordi del supporto di avvio con l'alloggiamento dello zoccolo, quindi spingerlo delicatamente a squadra nello zoccolo.
    b. Ruotare il supporto di avvio verso il basso verso il pulsante di bloccaggio.
    c. Premere il pulsante di bloccaggio, ruotare completamente il supporto di avvio e rilasciare il pulsante di bloccaggio.
6. Reinstallare il modulo di gestione del sistema:
    a. Ruotare il vassoio di gestione dei cavi verso l'alto fino alla posizione di chiusura.
    b. Eseguire il richiamo del modulo Gestione del sistema.

Fase 2: Trasferire l'immagine di avvio sul supporto di avvio

Il supporto di avvio sostitutivo installato non dispone di un'immagine ONTAP, pertanto è necessario trasferire

un'immagine ONTAP utilizzando un'unità flash USB.

Prima di iniziare

- È necessario disporre di un'unità flash USB, formattata con FAT32, con almeno 4 GB di capacità.
- È necessario disporre di una copia della stessa versione dell'immagine di ONTAP del controller danneggiato in esecuzione. È possibile scaricare l'immagine appropriata dalla "Download" sezione sul sito di assistenza NetApp
  - Se NVE è supportato, scaricare l'immagine con crittografia dei volumi di NetApp, come indicato nel pulsante di download.
  - Se NVE non è supportato, scaricare l'immagine senza crittografia dei volumi di NetApp, come indicato nel pulsante di download.
- Se il sistema è una coppia ha, è necessario disporre di una connessione di rete tra le porte di gestione dei nodi dei controller (in genere le interfacce e0M).

Fasi

1. Scaricare e copiare l'immagine di servizio appropriata da "Sito di supporto NetApp" nell'unità flash USB.
   a. Scaricare l'immagine del servizio dal collegamento Download nella pagina, nello spazio di lavoro del computer portatile.
   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.

      L'unità flash USB dovrebbe avere l'immagine ONTAP appropriata di ciò che il controller danneggiato è in esecuzione.

   c. Rimuovere l'unità flash USB dal computer portatile.
2. Inserire l'unità flash USB nella porta USB-A del modulo di gestione del sistema.

   Assicurarsi di installare l'unità flash USB nello slot contrassegnato per i dispositivi USB e non nella porta della console USB.
3. Ricollegare l'alimentazione al modulo controller:
   a. 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.

   b. Ruotare i fermi di bloccaggio verso l'alto in posizione bloccata.

      Il controller inizia ad avviarsi non appena l'alimentazione viene ricollegata al sistema.
4. 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 arrestare il controller per avviare IL CARICATORE.
5. Impostare il tipo di connessione di rete al prompt DEL CARICATORE:

- Se si sta configurando DHCP: `ifconfig e0M -auto`

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

- Se si configurano connessioni manuali: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway`
  - 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.

> Potrebbero essere necessari altri parametri per l'interfaccia. Per ulteriori informazioni, immettere help ifconfig al prompt del firmware.

Avviare l'immagine di ripristino - ASA A70 e ASA A90

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

Fasi

1. Dal prompt del CARICATORE, avviare l'immagine di ripristino dall'unità flash USB: *Boot_recovery*

   L'immagine viene scaricata dall'unità flash USB.

2. Quando richiesto, inserire il nome dell'immagine o accettare l'immagine predefinita visualizzata tra parentesi sullo schermo.
3. Ripristinare il file system var:

Se il sistema è in esecuzione…	Quindi…
ONTAP 9.16.0 o versioni precedenti	a. Sul controller danneggiato, premere *Y* quando viene visualizzato `Do you want to restore the backup configuration now?` b. Sul controller danneggiato, premere *Y* quando viene richiesto di sovrascrivere `/etc/ssh/ssh_host_ecdsa_key`. c. Sul controller partner integro, impostare il controller con problemi al 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 impainted_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 danneggiato, premere *y* quando viene visualizzato `Was the restore backup procedure successful?`. g. Sul controller danneggiato, premere *y* quando viene visualizzato … `would you like to use this restored copy now?`. h. Sul controller danneggiato, premere *y* quando viene richiesto di 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 "Ripristinare i gestori delle chiavi". j. Collegare il cavo della console al controller partner. k. Restituire il controller utilizzando il comando *storage failover giveback -fromnode local*. l. Ripristinare il giveback automatico se è stato disattivato utilizzando il comando *storage failover modify -node local -auto -giveback true*. m. Se AutoSupport è abilitato, ripristinare/riattivare la creazione automatica dei casi utilizzando il comando *system node AutoSupport Invoke -node * -type all -message MAINT=END*. **NOTA:** se il processo non riesce, contattare "Supporto NetApp".

Se il sistema è in esecuzione…	Quindi…
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 viene richiesto di 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 "Ripristinare i gestori delle chiavi". g. Collegare il cavo della console al controller partner. h. Restituire il controller utilizzando il comando *storage failover giveback -fromnode local*. i. Ripristinare il giveback automatico se è stato disattivato utilizzando il comando *storage failover modify -node local -auto -giveback true*. j. Se AutoSupport è abilitato, ripristinare/riattivare la creazione automatica dei casi utilizzando il comando *system node AutoSupport Invoke -node * -type all -message MAINT=END*. **NOTA:** se il processo non riesce, contattare "Supporto NetApp".

Ripristinare la crittografia - ASA A70 e ASA A90

Ripristinare la crittografia sul supporto di avvio sostitutivo.

Fase 1: Ripristinare il gestore delle chiavi integrato

È necessario completare i passaggi specifici per i sistemi con gestore delle chiavi integrato (OKM), crittografia storage NetApp (NSE) o crittografia del volume NetApp (NVE) abilitati utilizzando le impostazioni acquisite all'inizio di questa procedura.

Se NSE o NVE sono abilitati insieme a Onboard o External Key Manager, devi ripristinare le impostazioni acquisite all'inizio di questa procedura.

Fasi

1. Collegare il cavo della console al controller di destinazione.
2. Selezionare una delle seguenti opzioni per ripristinare la configurazione del gestore delle chiavi integrato dal menu di avvio ONATP.

Opzione 1: Sistemi con configurazione server gestore chiavi integrato

Ripristinare la configurazione del gestore delle chiavi integrato dal menu di avvio ONATP.

Prima di iniziare

Durante il ripristino della configurazione OKM sono necessarie le 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. Dal menu di avvio di ONTAP, selezionare l'opzione 10:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 10
```

2. Confermare la continuazione del processo. `This option must be used only in disaster recovery procedures. Are you sure? (y or n): y`
3. Inserire due volte la passphrase a livello di cluster.

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

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

4. Immettere le informazioni di backup. Incollare l'intero contenuto dalla riga DI BACKUP BEGIN attraverso la riga di BACKUP FINALE.

   Premere due volte il tasto invio alla fine dell'immissione.

```
Enter the backup data:

--------------------------BEGIN BACKUP--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---------------------------END BACKUP---------------------------
```

5. Il processo di ripristino verrà completato.

```
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.

```
*******************************************************************
***************
* 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 venga visualizzata `Waiting for giveback…(Press Ctrl-C to abort wait)`

8. Dal nodo partner, eseguire il giveback per il controller partner: *Storage failover giveback -fromnode local -only-cfo-Aggregates true*
9. Una volta avviato solo con l'aggregato CFO, eseguire il comando *Security key-manager onboard sync* :
10. Inserisci la passphrase a livello di cluster per Onboard Key Manager:

```
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.
```

11. Assicurarsi che tutte le chiavi siano sincronizzate: *Query chiave gestore chiavi di sicurezza -ripristinato false*

```
There are no entries matching your query.
```

> Nessun risultato dovrebbe comparire quando si filtra per false nel parametro ripristinato.

12. Giveback del nodo dal partner: *Storage failover giveback -fromnode local*

Opzione 2: Sistemi con configurazione server gestore chiavi esterno

Ripristinare la configurazione del gestore delle chiavi esterno dal menu di avvio ONATP.

Prima di iniziare

Per ripristinare la configurazione del gestore chiavi esterno (EKM) sono necessarie le seguenti informazioni:

- È necessaria una copia del file /cfcard/kmip/servers.cfg da un altro nodo del cluster, oppure le seguenti informazioni:
- L'indirizzo del server KMIP.
- Porta KMIP.
- Una copia del file /cfcard/kmip/certs/client.crt da un altro nodo del cluster o, il certificato del client.
- Una copia del file /cfcard/kmip/certs/client.key da un altro nodo del cluster o, la chiave del client.
- Una copia del file /cfcard/kmip/certs/CA.pem da un altro nodo del cluster o, le CA del server KMIP.

Fasi

1. Selezionare l'opzione 11 dal menu di avvio di ONTAP.

```
(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
```

2. Quando richiesto, confermare di aver raccolto le informazioni richieste:
   a. `Do you have a copy of the /cfcard/kmip/certs/client.crt file? {y/n}` *y*
   b. `Do you have a copy of the /cfcard/kmip/certs/client.key file? {y/n}` *y*
   c. `Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}` *y*
   d. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *y*

      In alternativa, è possibile anche visualizzare le seguenti istruzioni:

   e. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *n*
      i. `Do you know the KMIP server address? {y/n}` *y*
      ii. `Do you know the KMIP Port? {y/n}` *y*
3. Fornire le informazioni relative a ciascuna di queste richieste:
   a. `Enter the client certificate (client.crt) file contents:`
   b. `Enter the client key (client.key) file contents:`
   c. `Enter the KMIP server CA(s) (CA.pem) file contents:`
   d. `Enter the server configuration (servers.cfg) file contents:`

```
Example

Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAoU1eajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYlbkIb4bAgLztHEmUDOkGmXYAkblQ=
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

4. Il processo di ripristino verrà completato:

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Selezionare l'opzione 1 dal menu di avvio per continuare l'avvio in ONTAP.

```
**********************************************************************
***************
* 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
```

Passaggio 2: Completare la sostituzione del supporto di avvio

Completare il processo di sostituzione dei supporti di avvio dopo il normale avvio completando i controlli finali e restituendo spazio di archiviazione.

1. Controllare l'output della console:

Se la console visualizza…	**Quindi…**
Prompt di login	Passare alla fase 6.
In attesa di un giveback…	a. Accedere al controller partner. b. Verifica che il controller di destinazione sia pronto per il giveback con il comando *storage failover show*.

2. Spostare il cavo della console sul controller partner e restituire lo storage del controller di destinazione utilizzando il comando *storage failover giveback -fromnode local -only-cfo-Aggregates true*.
   - 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 perché il partner è "non pronto", attendere 5 minuti affinché il sottosistema ha si sincronizzi tra i partner.

- Se il comando non riesce a causa di un processo NDMP, SnapMirror o SnapVault, disattivare il processo. Per ulteriori informazioni, consultare il centro di documentazione appropriato.

3. Attendere 3 minuti e controllare lo stato di failover con il comando *storage failover show*.
4. Al prompt di clustershell, immettere il comando *network interface show -is-home false* per elencare le interfacce logiche che non si trovano sul controller e sulla porta home.

   Se alcune interfacce sono elencate come `false`, riportarle alla porta home utilizzando il comando *net int revert -vserver Cluster -lif _nodename*.

5. Spostare il cavo della console sul controller di destinazione ed eseguire il comando *version -v* per controllare le versioni di ONTAP.
6. Utilizzare `storage encryption disk show` per rivedere l'output.
7. Utilizzare il comando *Security key-manager key query* per visualizzare gli ID delle chiavi di autenticazione memorizzati nei server di gestione delle chiavi.
   - Se il `Restored` colonna = `yes/true`, è possibile completare il processo di sostituzione.
   - Se `Key Manager type` = `external` e la `Restored` colonna = qualcosa di diverso da `yes/true`, utilizzare il comando *Security key-manager external restore* per ripristinare gli ID delle chiavi di autenticazione.

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

   - Se il `Key Manager type` comando = `onboard` e la `Restored` colonna = qualcosa di diverso da `yes/true`, utilizzare il comando *Security key-manager onboard Sync* per sincronizzare le chiavi di bordo mancanti sul nodo riparato.

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

8. Collegare il cavo della console al controller partner.
9. Restituire il controller utilizzando `storage failover giveback -fromnode local` comando.
10. Ripristinare il giveback automatico se è stato disattivato utilizzando il comando *storage failover modify -node local -auto-giveback true*.
11. Se AutoSupport è abilitato, ripristinare/riattivare la creazione automatica dei casi utilizzando il comando *system node AutoSupport Invoke -node * -type all -message MAINT=END*.

Restituire il componente guasto a NetApp - ASA A70 e ASA A90

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

Informazioni sul copyright

Informazioni sul marchio commerciale