Supporto di boot

Install and maintain

NetApp
February 28, 2025

Sommario

Supporto di boot . . . 1
Panoramica sul ripristino dei supporti di avvio - ASA A70 e ASA A90 . . . 1
Flusso di lavoro per la sostituzione dei supporti di avvio - ASA A70 e ASA A90 . . . 1
Requisiti di sostituzione dei supporti di avvio - ASA A70 e ASA A90 . . . 2
Spegnere il controller danneggiato - ASA A70 e ASA A90 . . . 2
Sostituire i supporti di avvio - ASA A70 e ASA A90 . . . 3
Ripristinare l’immagine ONTAP - ASA A70 e ASA A90 . . . 6
Restituire il componente guasto a NetApp - ASA A70 e ASA A90 . . . 16

Supporto di boot

Panoramica sul ripristino dei supporti di avvio - ASA A70 e ASA A90

Il ripristino del supporto di avvio utilizza l'immagine di avvio dal nodo partner ed esegue automaticamente l'opzione appropriata del menu di avvio per installare l'immagine di avvio sul supporto di avvio sostitutivo.

Quando si verificano messaggi di errore di avvio simili a quelli illustrati di seguito, è necessario sostituire il supporto di avvio e ripristinare l'immagine ONTAP dal nodo partner.

```
Can't find primary boot device u0a.0
Can't find backup boot device u0a.1
ACPI RSDP Found at 0x777fe014

Starting AUTOBOOT press Ctrl-C to abort...
Could not load fat://boot0/X86_64/freebsd/image1/kernel: Device not found

ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/Linux/image1/vmlinuz (boot0, fat)
ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/freebsd/image1/kernel (boot0, fat)

Autoboot of PRIMARY image failed. Device not found (-6)
LOADER-A>
```

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"**

Esaminare i requisiti per la sostituzione dei supporti di avvio.

2. **"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.

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

Rimuovere il supporto di avvio guasto dal modulo di gestione del sistema 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 di sostituzione dei supporti di avvio - ASA A70 e ASA A90

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

- È necessario sostituire il supporto di avvio guasto con un supporto di avvio sostitutivo ricevuto da NetApp.
- Non devono essere presenti porte del quadro strumenti difettose sulla centralina guasta.
- Determinare se OKM (Onboard Key Manager) o EKM (Eternal Key Manager) è configurato utilizzando uno dei seguenti metodi:
  - È possibile chiedere all'amministratore di sistema se OKM o EKM sono abilitati.
  - Per verificare se OKM è abilitato, è possibile utilizzare `security key-manager onboard show`.
  - Per verificare se EKM è abilitato, è possibile utilizzare `security key-manager external show`.
- Per OKM, è necessario il contenuto del file della passphrase OKM.
- 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.

Cosa succederà

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

Spegnere il controller danneggiato - ASA A70 e ASA A90

Spegnere o sostituire il controller danneggiato in modo da poter eseguire la manutenzione sul supporto di 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, 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`.

Cosa succederà

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

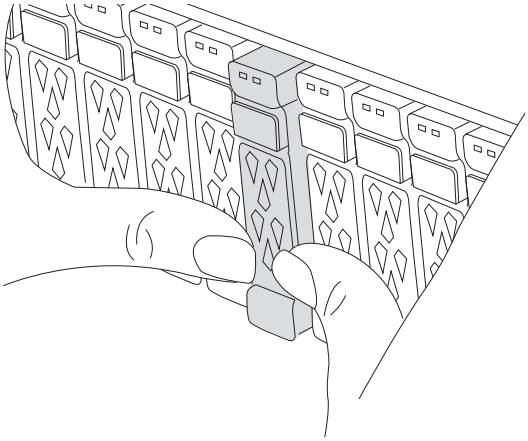
Sostituire i supporti di avvio - ASA A70 e ASA A90

Sostituire il supporto di avvio rimuovendo il modulo di gestione del sistema dal retro del sistema, rimuovendo il supporto di avvio danneggiato, installando il supporto di avvio sostitutivo nel modulo di gestione del sistema, quindi reinstallando il modulo di gestione del sistema.

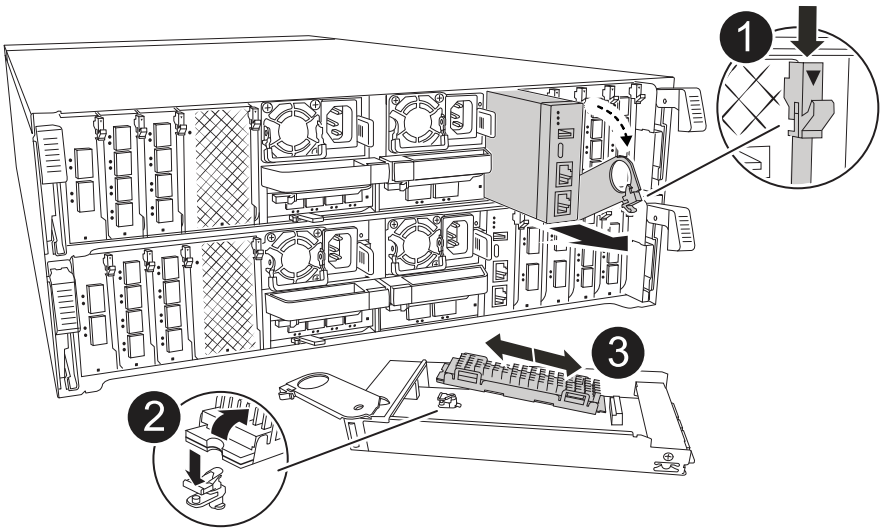
Fasi

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

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:



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

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.

7. Reinstallare la centralina e 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 viene inserito e l'alimentazione viene ripristinata.

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

Cosa succederà

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

Ripristinare l'immagine ONTAP - ASA A70 e ASA A90

Se il supporto di avvio nel sistema ASA A70 o ASA A90 è danneggiato, è possibile avviare l'immagine di ripristino e ripristinare la configurazione dal nodo partner.

Prima di iniziare

- Determinare se OKM (Onboard Key Manager) o EKM (Eternal Key Manager) è configurato utilizzando uno dei seguenti metodi:
  - È possibile chiedere al cliente o all'amministratore di sistema se OKM o EKM sono abilitati.
  - Per verificare se OKM è abilitato, è possibile utilizzare `security key-manager onboard show`.
  - Per verificare se EKM è abilitato, è possibile utilizzare `security key-manager external show`.
- Per OKM, è necessario il contenuto del file della passphrase OKM.
- 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.

Fasi

1. Al prompt di Loader, immettere il comando:

   ```
   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 controlla il tipo di crittografia e di crittografia e visualizza uno dei due messaggi. A seconda del messaggio visualizzato, eseguire una delle seguenti operazioni:

   A volte, il processo potrebbe non essere in grado di identificare se il gestore delle chiavi è configurato sul sistema. Viene visualizzato un messaggio di errore, viene chiesto se il gestore delle chiavi è configurato per il sistema e viene chiesto quale tipo di gestore delle chiavi è configurato. Il processo riprenderà dopo aver risolto il problema.

Mostrare un esempio di messaggi di errore di configurazione per la ricerca

```
Error when fetching key manager config from partner ${partner_ip}:
${status}

Has key manager been configured on this system

Is the key manager onboard
```

Se viene visualizzato questo messaggio…	Eseguire questa operazione…
`key manager is not configured. Exiting.`	La crittografia non è installata sul sistema. Attenersi alla seguente procedura: a. Accedere al nodo quando viene visualizzato il prompt di login e restituire lo spazio di archiviazione: `storage failover giveback -ofnode` *`impaired_node_name`* b. Andare al passaggio 5 per abilitare il giveback automatico se è stato disattivato.
`key manager is configured.`	Andare al passaggio 4 per ripristinare il gestore delle chiavi appropriato. Il nodo accede al menu di avvio ed esegue: • Opzione 10 per sistemi con Onboard Key Manager (OKM). • Opzione 11 per i sistemi con EKM (External Key Manager).

4. Selezionare il processo di ripristino del gestore delle chiavi appropriato.

Onboard Key Manager (OKM)

Se viene rilevato un OKM, il sistema visualizza il seguente messaggio e inizia a eseguire l'opzione 10 del menu di avvio.

```
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. Immettere `Y` quando richiesto per confermare che si desidera avviare il processo di ripristino OKM.

b. Immettere la passphrase per il gestore delle chiavi integrato quando richiesto, quindi immettere nuovamente la passphrase quando richiesto, per confermare.

Mostrare un esempio di prompt di passphrase

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

c. Continuare a monitorare il processo di ripristino durante il ripristino dei file appropriati dal nodo partner.

Al termine del processo di ripristino, il nodo viene riavviato. I seguenti messaggi indicano che il ripristino è stato eseguito correttamente:

```
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.
```

d. Quando il nodo viene riavviato, verificare che il ripristino del supporto di avvio sia stato eseguito correttamente confermando che il sistema è nuovamente in linea e operativo.

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

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

f. Una volta che il nodo partner è completamente attivo e fornisce i dati, sincronizzare le chiavi OKM nel cluster.

```
security key-manager onboard sync
```

Gestore chiavi esterno (EKM)

Se viene rilevato EKM, il sistema visualizza il seguente messaggio e inizia a eseguire l'opzione 11 del menu di avvio.

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

a. Il passaggio successivo dipende dalla versione di ONTAP in esecuzione sul sistema:

Se il sistema è in esecuzione…	Eseguire questa operazione…
ONTAP 9.16.0	i. Premere `Ctlr-C` per uscire dall'opzione 11 del menu di avvio. ii. Premere `Ctlr-C` per uscire dal processo di configurazione EKM e tornare al menu di avvio. iii. Selezionare l'opzione del menu di avvio 8. iv. Riavviare il nodo. Se `AUTOBOOT` è impostato, il nodo viene riavviato e utilizza i file di configurazione dal nodo partner. Se `AUTOBOOT` non è impostato, immettere il comando di avvio appropriato. Il nodo viene riavviato e utilizza i file di configurazione dal nodo partner. v. Riavviare il nodo in modo che EKM protegga la partizione dei supporti di avvio. vi. Passare alla fase c.
ONTAP 9.16.1	Passare alla fase successiva.

b. Quando richiesto, immettere le seguenti impostazioni di configurazione EKM:

Azione	Esempio

Immettere il contenuto del certificato client dal `/cfcard/kmip/certs/client.crt` file.	**Mostra un esempio di contenuto del certificato client**
	`-----BEGIN CERTIFICATE-----`
	`<certificate_value>`
	`-----END CERTIFICATE-----`

Immettere il contenuto del file della chiave client dal `/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-----`

Immettere il contenuto del file CA del server KMIP dal `/cfcard/kmip/certs/CA.pem` file.	**Mostra un esempio del contenuto del file del server KMIP**
	`-----BEGIN CERTIFICATE-----`
	`<KMIP_certificate_CA_value>`
	`-----END CERTIFICATE-----`

Azione	Esempio

Immettere il contenuto del file di configurazione del server dal `/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.crt`
	`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>`

Azione	Esempio

Se richiesto, immettere l'UUID cluster ONTAP dal partner.	**Mostra un esempio di UUID 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).`

Azione	Esempio

Se richiesto, inserire l'interfaccia di rete temporanea e le impostazioni per il nodo.	**Mostrare un esempio di impostazione di rete temporanea**
	`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=]`

c. A seconda che la chiave sia stata ripristinata correttamente, eseguire una delle seguenti operazioni:

   - Se la configurazione EKM è stata ripristinata correttamente, il processo tenta di ripristinare i file appropriati dal nodo partner e riavvia il nodo. Passare al punto d.

Mostrare un esempio di messaggi di ripristino 9.16.0 riusciti

```
kmip2_client: Importing keys from external key server:
xxx.xxx.xxx.xxx:5696
[Feb  6 04:57:43]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdUtils:
[locateMrootAkUuids]:420: Locating local cluster MROOT-AK
with keystore UUID: <uuid>
[Feb  6 04:57:43]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [doCmdImp]:79: Calling
KMIP Locate for the following attributes: [<x-NETAPP-
ClusterId, <uuid>>, <x-NETAPP-KeyUsage, MROOT-AK>, <x-
NETAPP-KeystoreUuid, <uuid>>, <x-NETAPP-Product, Data
ONTAP>]
[Feb  6 04:57:44]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [doCmdImp]:84: KMIP
Locate executed successfully!
[Feb  6 04:57:44]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [setUuidList]:50: UUID
returned: <uuid>
...
kmip2_client: Successfully imported the keys from external
key server: xxx.xxx.xxx.xxx:5696

GEOM_ELI: Device nvd0s4.eli created.
GEOM_ELI: Encryption: AES-XTS 256
GEOM_ELI:     Crypto: software
Feb 06 05:02:37 [_server-name_]: crypto_get_mroot_ak:140
MROOT-AK is requested.
Feb 06 05:02:37 [_server-name_]: crypto_get_mroot_ak:162
Returning MROOT-AK.
```

Mostrare un esempio di messaggi di ripristino 9.16.1 riusciti

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
...
kmip2_client: Successfully imported the keys from external
key server: xxx.xxx.xxx.xxx:xxxx
Successfully recovered keymanager secrets.
```

- Se la chiave non viene ripristinata correttamente, il sistema si arresta e indica che non è stato possibile ripristinarla. Vengono visualizzati i messaggi di errore e di avvertenza. Eseguire nuovamente il processo di ripristino immettendo `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>
```

d. Quando il nodo viene riavviato, verificare che il ripristino del supporto di avvio sia stato eseguito correttamente confermando che il sistema è nuovamente online e operativo.

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

`storage failover giveback -ofnode` *`impaired_node_name`*.

5. Se il giveback automatico è stato disattivato, riabilitarlo:

`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 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