



# **Supporto di boot**

Install and maintain

NetApp  
April 19, 2024

This PDF was generated from [https://docs.netapp.com/it-it/ontap-systems/asa900/bootmedia\\_replace\\_overview.html](https://docs.netapp.com/it-it/ontap-systems/asa900/bootmedia_replace_overview.html) on April 19, 2024. Always check docs.netapp.com for the latest.

# Sommario

- Supporto di boot ..... 1
  - Sostituire il supporto di avvio - ASA A900 ..... 1
  - Pre-shutdown controlla le chiavi di crittografia integrate - ASA A900 ..... 1
  - Spegnere il controller compromesso - ASA A900 ..... 5
  - Sostituire il supporto di avvio - ASA A900 ..... 8
  - Avviare l'immagine di ripristino - ASA A900 ..... 13
  - Procedura di sostituzione dei supporti post-boot per OKM, NSE e NVE - ASA A900 ..... 16
  - Restituire il componente guasto a NetApp - ASA A900 ..... 20

# Supporto di boot

## Sostituire il supporto di avvio - ASA A900

Il supporto di avvio memorizza un set primario e secondario di file di sistema (immagine di avvio) che il sistema utilizza al momento dell'avvio. A seconda della configurazione di rete, è possibile eseguire una sostituzione senza interruzioni o senza interruzioni.

È necessario disporre di un'unità flash USB, formattata in FAT32, con la quantità di storage appropriata per contenere `image_XXX.tgz`.

È inoltre necessario copiare il `image_XXX.tgz` Sul disco flash USB per utilizzarlo successivamente in questa procedura.

- I metodi senza interruzioni e senza interruzioni per la sostituzione di un supporto di avvio richiedono entrambi il ripristino di `var` file system:
  - Per la sostituzione senza interruzioni, la coppia ha non richiede la connessione a una rete per ripristinare `var` file system. La coppia ha in un singolo chassis ha una connessione e0S interna, che viene utilizzata per il trasferimento `var` configurare tra loro.
  - Per la sostituzione delle interruzioni, non è necessaria una connessione di rete per ripristinare `var` file system, ma il processo richiede due riavvii.
- È necessario sostituire il componente guasto con un componente FRU sostitutivo ricevuto dal provider.
- È importante applicare i comandi 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.

## Pre-shutdown controlla le chiavi di crittografia integrate - ASA A900

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

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

### Fasi

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

2. Se AutoSupport è attivato, eliminare la creazione automatica del caso richiamando un messaggio

```
AutoSupport: system node autosupport invoke -node * -type all -message  
MAINT=number_of_hours_downh
```

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

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

## ONTAP 9.6 e versioni successive

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

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

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

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

## Verificare la configurazione NVE

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



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

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

- a. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
  - b. Immettere il comando per visualizzare le informazioni di gestione delle chiavi: `security key-manager onboard show-backup`
  - c. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
  - d. Tornare alla modalità admin: `set -priv admin`
  - e. Spegnerne il controller compromesso.
3. Se il Key Manager display dei tipi `external` e a. Restored la colonna visualizza un valore diverso da `yes`:

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

Se il comando non riesce, contattare il supporto NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Verificare che il Restored colonna uguale a. `yes` per tutte le chiavi di autenticazione: `security key-manager key query`
  - b. Spegnerne il controller compromesso.
4. Se il Key Manager display dei tipi `onboard` e a. Restored la colonna visualizza un valore diverso da `yes`:

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



Immettere la passphrase di gestione della chiave alfanumerica integrata a 32 caratteri del cliente al prompt. Se non è possibile fornire la passphrase, contattare il supporto NetApp. ["mysupport.netapp.com"](https://mysupport.netapp.com)

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

## Verificare la configurazione NSE

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



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

- Se il Key Manager display dei tipi `external` e `a. Restored` viene visualizzata la colonna `yes`, è sicuro spegnere il controller compromesso.
  - Se il Key Manager display dei tipi `onboard` e `a. Restored` viene visualizzata la colonna `yes`, è necessario completare alcuni passaggi aggiuntivi.
  - Se il Key Manager display dei tipi `external` e `a. Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.
  - Se il Key Manager display dei tipi `external` e `a. Restored` la colonna visualizza un valore diverso da `yes`, è necessario completare alcuni passaggi aggiuntivi.
2. Se il Key Manager display dei tipi `onboard` e `a. Restored` viene visualizzata la colonna `yes`, Eseguire manualmente il backup delle informazioni OKM:
    - a. Accedere alla modalità avanzata dei privilegi e digitare `y` quando viene richiesto di continuare: `set -priv advanced`
    - b. Immettere il comando per visualizzare le informazioni di gestione delle chiavi: `security key-manager onboard show-backup`
    - c. Copiare il contenuto delle informazioni di backup in un file separato o nel file di log. Sarà necessario in situazioni di emergenza in cui potrebbe essere necessario ripristinare manualmente OKM.
    - d. Tornare alla modalità `admin`: `set -priv admin`
    - e. È possibile spegnere il controller in modo sicuro.
  3. Se il Key Manager display dei tipi `external` e `a. Restored` la colonna visualizza un valore diverso da `yes`:
    - a. Ripristinare le chiavi di autenticazione per la gestione delle chiavi esterne in tutti i nodi del cluster: `security key-manager external restore`  
  
Se il comando non riesce, contattare il supporto NetApp.  
  
["mysupport.netapp.com"](https://mysupport.netapp.com)
    - a. Verificare che il `Restored` colonna uguale `a. yes` per tutte le chiavi di autenticazione: `security key-manager key query`
    - b. È possibile spegnere il controller in modo sicuro.
  4. Se il Key Manager display dei tipi `onboard` e `a. Restored` la colonna visualizza un valore diverso da `yes`:
    - a. Immettere il comando di sincronizzazione del gestore delle chiavi di sicurezza integrato: `security key-manager onboard sync`

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

["mysupport.netapp.com"](https://mysupport.netapp.com)

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

## Spegnere il controller compromesso - ASA A900

Arrestare o sostituire il controller con problemi utilizzando la procedura appropriata per la configurazione.

## La maggior parte delle configurazioni

Dopo aver completato le attività NVE o NSE, è necessario completare l'arresto del 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 controllare i messaggi di evento `cluster kernel-service show`) Per blade SCSI del controller deteriorati. Il `cluster kernel-service show command` visualizza il nome del nodo, lo stato del quorum di quel nodo, lo stato di disponibilità di quel nodo e lo stato operativo di quel nodo.

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

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

### Fasi

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

Il seguente messaggio AutoSupport elimina la creazione automatica del caso per due ore:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disattivare il giveback automatico dalla console del controller integro: `storage failover modify -node local -auto-giveback false`



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

3. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza...	Quindi...
Il prompt DEL CARICATORE	Passare alla fase successiva.
In attesa di un giveback...	Premere Ctrl-C, quindi rispondere <i>y</i> quando richiesto.



Se il controller non utilizzato visualizza...	Quindi...
Prompt di sistema o prompt della password	Assumere il controllo o arrestare il controller compromesso dal controller integro: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code>  Quando il controller non utilizzato visualizza Waiting for giveback... (in attesa di giveback...), premere Ctrl-C e rispondere y.

## Il controller si trova in un MetroCluster

Dopo aver completato le attività NVE o NSE, è necessario completare l'arresto del controller compromesso.



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 y quando richiesto.

**Se il controller non utilizzato visualizza...**

**Quindi...**

Prompt di sistema o prompt della password (inserire la password di sistema)

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 il supporto di avvio - ASA A900

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

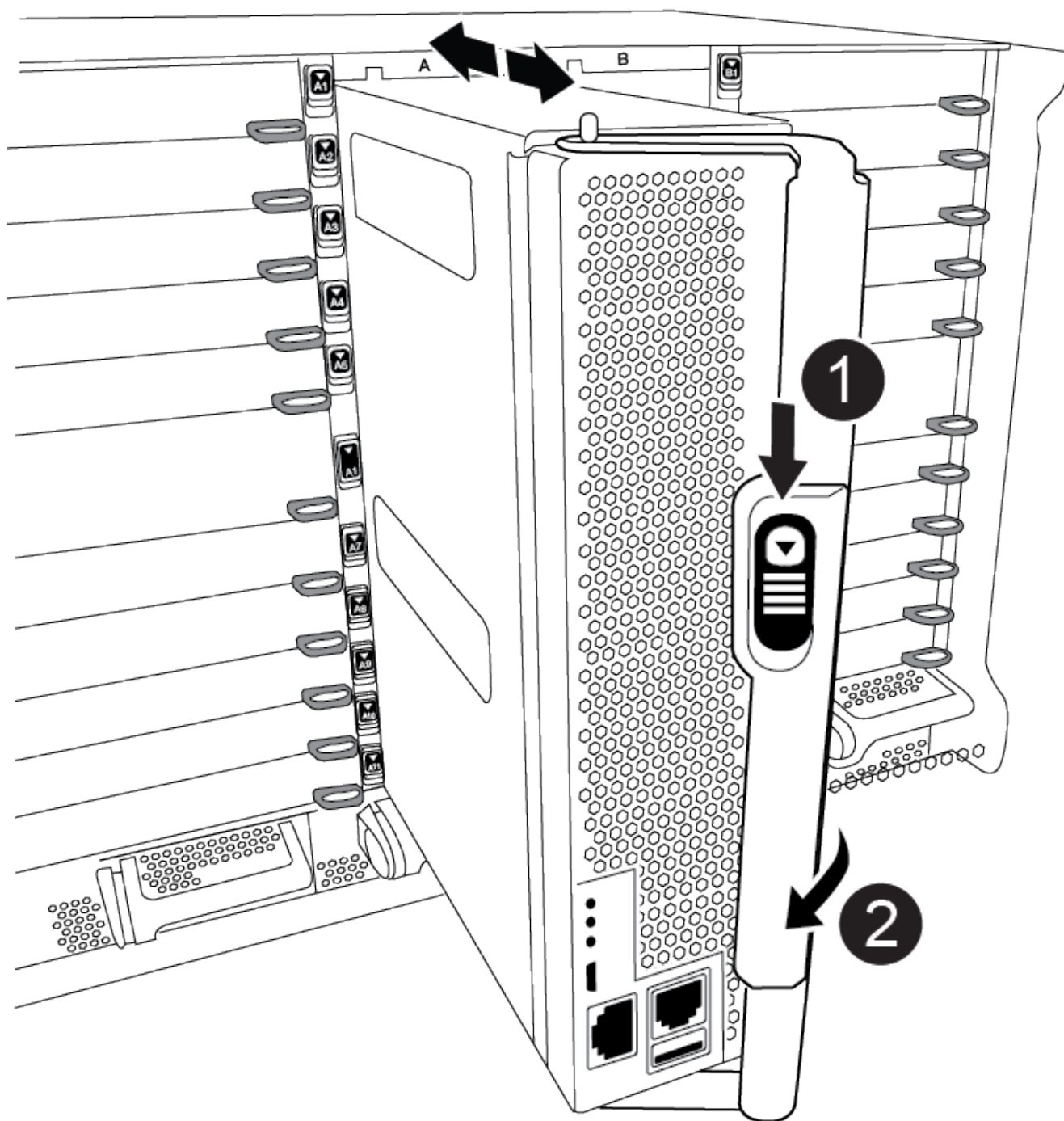
### Fase 1: Rimuovere il modulo controller

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

#### Fasi

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

[Animazione - rimuovere il controller](#)

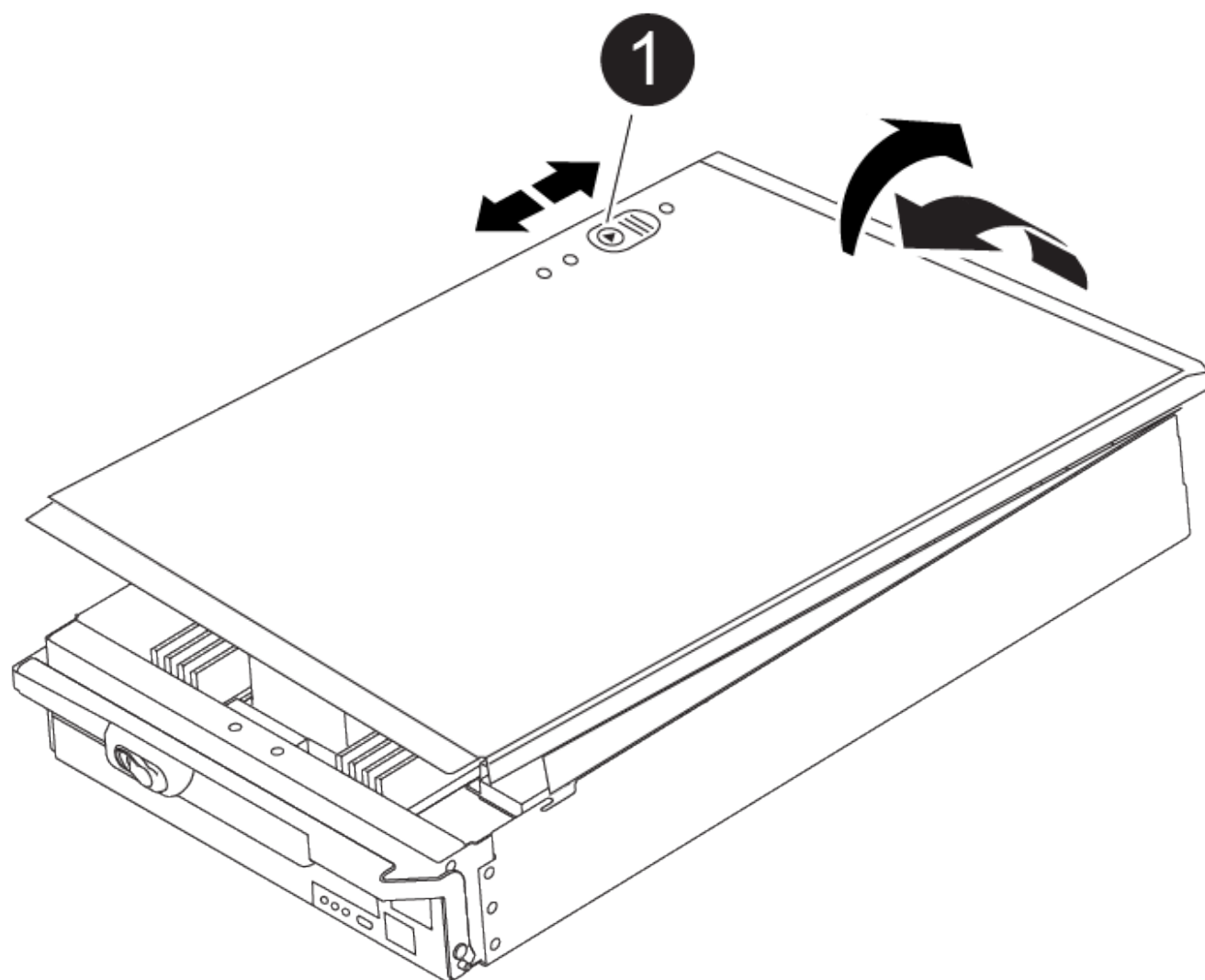


1	Pulsante di rilascio della maniglia della camma
2	Maniglia CAM

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

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

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



1	Pulsante di bloccaggio del coperchio del modulo controller
---	--

## Fase 2: Sostituire il supporto di avvio

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

### Fasi

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

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



1	Premere il tasto di rilascio Tab
2	Supporto di boot

2. Premere il pulsante blu sull'alloggiamento del supporto di avvio per rilasciare il supporto di avvio dall'alloggiamento, quindi estrarlo delicatamente dalla presa del supporto di avvio.



Non attorcigliare o tirare il supporto di avvio verso l'alto, in quanto potrebbe danneggiare la presa o il supporto di avvio.

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

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

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

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

È possibile installare l'immagine di sistema sul supporto di avvio sostitutivo utilizzando un'unità flash USB su cui è installata l'immagine. Tuttavia, è necessario ripristinare il file system var durante questa procedura.

#### Prima di iniziare

- È necessario disporre di un'unità flash USB, formattata con FAT32, con almeno 4 GB di capacità.
- Una copia della stessa versione dell'immagine di ONTAP utilizzata dal controller compromesso. È possibile scaricare l'immagine appropriata dalla sezione Download sul sito del supporto NetApp
  - Se NVE è attivato, scaricare l'immagine con NetApp Volume Encryption, come indicato nel pulsante download.
  - Se NVE non è attivato, scaricare l'immagine senza NetApp Volume Encryption, come indicato nel pulsante download.
- Se il sistema è autonomo, non è necessaria una connessione di rete, ma è necessario eseguire un ulteriore riavvio durante il ripristino del file system var.

#### Fasi

1. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
2. Se necessario, è possibile ricable il modulo controller.
3. Inserire l'unità flash USB nello slot USB del modulo controller.

Assicurarsi di installare l'unità flash USB nello slot contrassegnato per i dispositivi USB e non nella porta della console USB.

4. Inserire completamente il modulo controller nel sistema, assicurandosi che la maniglia della camma si allontani dall'unità flash USB, spingere con decisione la maniglia della camma per terminare l'inserimento del modulo controller, quindi spingere la maniglia della camma in posizione chiusa.

Il controller inizia ad avviarsi non appena viene installato completamente nello chassis.

5. Interrompere il processo di avvio per interrompere il CARICAMENTO premendo Ctrl-C quando viene visualizzato Avvio DI AUTOBOOT premere Ctrl-C per interrompere....

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

6. Impostare il tipo di connessione di rete al prompt DEL CARICATORE:

- Se si sta configurando DHCP: `ifconfig e0a -auto`



La porta di destinazione configurata è la porta di destinazione utilizzata per comunicare con il 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 e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`

- Filer\_addr è l'indirizzo IP del sistema di storage.
- Netmask è la maschera di rete della rete di gestione connessa al partner ha.
- gateway è il gateway per la rete.
- dns\_addr è l'indirizzo IP di un name server sulla rete.
- dns\_domain è il nome di dominio DNS (Domain Name System).

Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot. È necessario solo il nome host del server.



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

7. 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 - ASA A900

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

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

L'immagine viene scaricata dall'unità flash USB.

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

3. Ripristinare il file system var:

Se il sistema dispone di...	Quindi...
Una connessione di rete	<ul style="list-style-type: none"> <li>a. Premere <code>y</code> quando viene richiesto di ripristinare la configurazione di backup.</li> <li>b. Premere <code>y</code> quando viene richiesto di sovrascrivere <code>/etc/ssh/ssh_host_ecdsa_key</code>.</li> <li>c. Premere <code>y</code> quando viene richiesto di confermare se il backup di ripristino è stato eseguito correttamente.</li> <li>d. Premere <code>y</code> quando viene richiesto di ripristinare la copia della configurazione.</li> <li>e. Impostare il controller compromesso sul livello di privilegio avanzato: <code>set -privilege advanced</code></li> <li>f. Eseguire il comando di ripristino del backup: <code>system node restore-backup -node local -target-address impaired_node_IP_address</code></li> <li>g. Riportare il controller compromesso al livello di amministrazione: <code>set -privilege admin</code></li> <li>h. Premere <code>y</code> quando viene richiesto di utilizzare la configurazione ripristinata.</li> <li>i. Premere <code>y</code> quando viene richiesto di riavviare il controller compromesso.</li> </ul>
Nessuna connessione di rete	<ul style="list-style-type: none"> <li>a. Premere <code>n</code> quando viene richiesto di ripristinare la configurazione di backup.</li> <li>b. Riavviare il sistema quando richiesto dal sistema.</li> <li>c. Selezionare l'opzione <b>Update flash from backup config</b> (Sync flash) dal menu visualizzato.</li> </ul> <p>Se viene richiesto di continuare con l'aggiornamento, premere <code>y</code>.</p>



Se il sistema dispone di...	Quindi...
Nessuna connessione di rete e si trova in una configurazione MetroCluster IP	<p>a. Premere <b>n</b> quando viene richiesto di ripristinare la configurazione di backup.</p> <p>b. Riavviare il sistema quando richiesto dal sistema.</p> <p>c. Attendere che le connessioni dello storage iSCSI si connettano.</p> <p>È possibile procedere dopo aver visualizzato i seguenti messaggi:</p> <pre> date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).</pre> <p>d. Selezionare l'opzione <b>Update flash from backup config</b> (Sync flash) dal menu visualizzato.</p> <p>Se viene richiesto di continuare con l'aggiornamento, premere <b>y</b>.</p>

4. Assicurarsi che le variabili ambientali siano impostate come previsto:
  - a. Portare la centralina danneggiata al prompt DEL CARICATORE.
  - b. Controllare le impostazioni delle variabili di ambiente con il comando `printenv`.
  - c. Se una variabile di ambiente non è impostata come previsto, modificarla con il comando `setenv variable_name changed_value`.
  - d. Salvare le modifiche utilizzando il comando `saveenv`.
5. Il successivo dipende dalla configurazione del sistema:
  - Se il sistema dispone di onboard keymanager, NSE o NVE configurati, visitare il sito [Fasi di sostituzione dei supporti post-boot per OKM, NSE e NVE](#)

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

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

Se viene visualizzato...	Quindi...
Prompt di login	Passare alla fase successiva.
In attesa di un giveback...	a. Accedere al controller partner. b. Verificare che il destinatario sia pronto per il giveback con <code>storage failover show</code> comando.

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

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

10. Spostare il cavo della console sul dispositivo riparato spegnere o sostituire il controller con problemi utilizzando la procedura appropriata per la configurazione. Ed eseguire il comando `version -v` per controllare le versioni di ONTAP.
11. Ripristinare il giveback automatico se è stato disattivato utilizzando il comando `storage failover modify -node local -auto-giveback true`.

## Procedura di sostituzione dei supporti post-boot per OKM, NSE e NVE - ASA A900

Dopo aver controllato le variabili di ambiente, è necessario completare la procedura specifica per ripristinare il gestore delle chiavi integrato (OKM), la crittografia dello storage NetApp (NSE) e la crittografia del volume NetApp (NVE).

Determinare la sezione da utilizzare per ripristinare le configurazioni OKM, NSE o NVE: Se NSE o NVE sono attivati insieme a Onboard Key Manager, è necessario ripristinare le impostazioni acquisite all'inizio di questa procedura.

- Se NSE o NVE sono attivati e Onboard Key Manager è attivato, passare a. [Restore NVE or NSE \(Ripristina NVE o NSE\) quando Onboard Key Manager è attivato](#).
- Se NSE o NVE sono abilitati per ONTAP 9.6, passare a. [Ripristinare NSE/NVE nei sistemi che eseguono ONTAP 9.6 e versioni successive](#).

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

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

Se la console visualizza...	Quindi...
Il prompt DEL CARICATORE	Avviare il controller dal menu di avvio: <code>boot_ontap menu</code>
In attesa di un giveback	<ol style="list-style-type: none"> <li>Invio <code>Ctrl-C</code> quando richiesto</li> <li>Quando viene visualizzato il messaggio: Interrompere questo nodo invece di attendere <code>[y/n]?</code> , inserire: <code>y</code></li> <li>Al prompt DEL CARICATORE, immettere <code>boot_ontap menu</code> comando.</li> </ol>

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



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

Esempio di dati di backup:

Inserire i dati di backup:

```

----- INIZIA IL BACKUP-----
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----- FINE BACKUP-----

```

- Nel menu di avvio, selezionare l'opzione Normal Boot (Avvio normale).  
Il sistema si avvia in attesa di giveback... prompt.
- Spostare il cavo della console sul controller partner e accedere come admin.
- Verificare che il controller di destinazione sia pronto per il giveback con `storage failover show` comando.
- Restituire solo gli aggregati CFO con `storage failover giveback -fromnode local -only-cfo -aggregates true` comando.
  - Se il comando non riesce a causa di un disco guasto, disinnestare fisicamente il disco guasto, ma lasciare il disco nello slot fino a quando non viene ricevuto un disco sostitutivo.
  - Se il comando non riesce a causa di una sessione CIFS aperta, verificare con il cliente come chiudere

le sessioni CIFS.



La chiusura di CIFS può causare la perdita di dati.

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

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

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

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



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

- c. Attendere 10 minuti per la sincronizzazione della chiave nel cluster.

13. Spostare il cavo della console sul controller partner.
14. Restituire il controller di destinazione utilizzando `storage failover giveback -fromnode local` comando.
15. Controllare lo stato del giveback, tre minuti dopo il completamento del report, utilizzando `storage failover show` comando.

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

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

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

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

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

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

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

4. Spostare il cavo della console sul controller partner e restituire lo storage del controller di destinazione utilizzando il comando `giveback di failover dello storage -fromnode local -only-cfo-aggregates true local`.

- Se il comando non riesce a causa di un disco guasto, disinnestare fisicamente il disco guasto, ma lasciare il disco nello slot fino a quando non viene ricevuto un disco sostitutivo.
- Se il comando non riesce a causa di sessioni CIFS aperte, verificare con il cliente come chiudere le sessioni CIFS.



La chiusura di CIFS può causare la perdita di dati.

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

5. Attendere 3 minuti e controllare lo stato di failover con il comando `show di failover dello storage`.

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

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

7. Spostare il cavo della console sul controller di destinazione ed eseguire `version -v` Per controllare le versioni di ONTAP.

8. Ripristinare il giveback automatico se è stato disattivato utilizzando `storage failover modify -node local -auto-giveback true` comando.

9. Utilizzare `storage encryption disk show` al prompt di `clustershell`, per rivedere l'output.

10. Utilizzare `security key-manager key-query` per visualizzare le chiavi di crittografia e autenticazione memorizzate nei server di gestione delle chiavi.

- Se il `Restored colonna = yes/true`, è possibile completare il processo di sostituzione.
- Se il `Key Manager type = external` e a. `Restored column (colonna) = qualsiasi altro elemento diverso da yes/true`, Utilizzare il comando di ripristino esterno del gestore delle chiavi di protezione per ripristinare gli ID delle chiavi di autenticazione.



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

- Se il `Key Manager type = onboard` e a. `Restored column (colonna) = qualsiasi altro elemento diverso da yes/true`, Utilizzare il comando di sincronizzazione integrato del gestore delle chiavi di protezione per `resynchronize` il tipo di Gestore chiavi.

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

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

## Restituire il componente guasto a NetApp - ASA A900

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

## Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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.