



Metodo automatizzato

Install and maintain

NetApp
September 25, 2024

Sommario

- Metodo automatizzato 1
 - Flusso di lavoro per la sostituzione dei supporti di avvio - ASA A70 e ASA A90 1
 - Requisiti e considerazioni - ASA A70 e ASA A90 1
 - Spegnere il controller - ASA A70 e ASA A90 1
 - Sostituire i supporti di avvio - ASA A70 e ASA A90 2
 - Ripristino automatico dell'avvio - ASA A70 e ASA A90 5
 - Restituire il componente guasto a NetApp - ASA A70 e ASA A90 12

Metodo automatizzato

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

"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

"Ripristino dell'immagine sul supporto di avvio (ripristino automatico dell'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 e considerazioni - ASA A70 e ASA A90

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

- 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.
- Non devono essere presenti porte del quadro strumenti difettose sulla centralina guasta.

Spegnere il controller - ASA A70 e ASA A90

È necessario completare l'arresto del controller danneggiato. 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 <i>y</i> quando richiesto.
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 <i>Waiting for giveback...</i> (in attesa di giveback...), premere Ctrl-C e rispondere <i>y</i> .

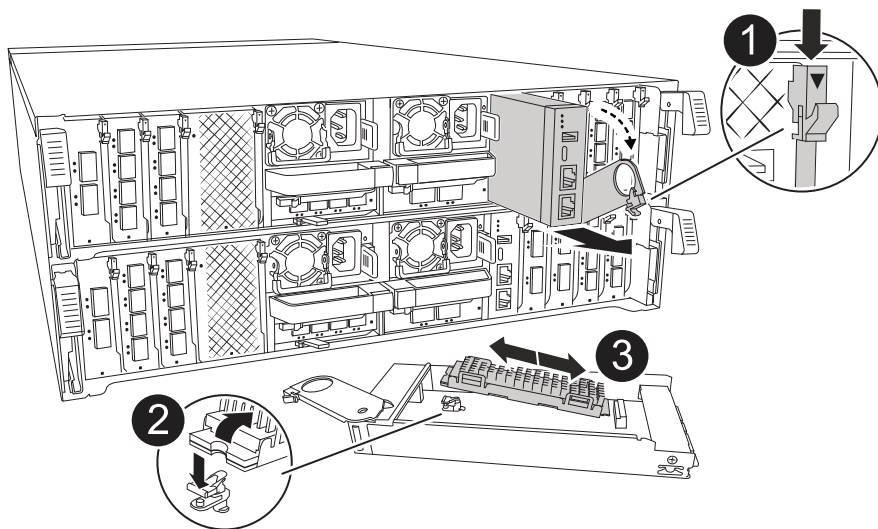
Sostituire i supporti di avvio - ASA A70 e ASA A90

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.

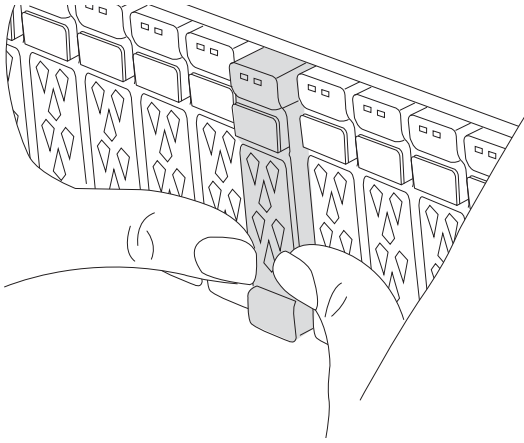
Fasi

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



	Dispositivo di chiusura della cappa del modulo di gestione del sistema
	Pulsante di blocco dei supporti di avvio
	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.

Ripristino automatico dell'avvio - ASA A70 e ASA A90

È possibile ripristinare l'immagine sul supporto di avvio dal controller partner utilizzando il processo di ripristino di avvio automatico.

Selezionare l'opzione di ripristino automatico a nodo singolo corrispondente alla configurazione in uso.

Opzione 1: Ripristino senza crittografia

È possibile ripristinare l'immagine ONTAP (boot media recovery) dal nodo partner utilizzando il `boot_recovery -partner` comando con le piattaforme ASA R2 che eseguono ONTAP 9.16,0 e versioni successive.

Prima di iniziare

Quando si avvia un nodo e il supporto di avvio su quel nodo è danneggiato, al prompt di Loader vengono visualizzati i seguenti messaggi e il processo di avvio con stop:

```
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>
```

Se viene visualizzato questo messaggio, è necessario ripristinare l'immagine ONTAP

Fasi

1. Dal prompt DI Loader, immettere il comando `boot_recovery -partner`.

La schermata visualizza il messaggio `Starting boot media recovery (BMR) process press Ctrl-C to abort...` e avvia i controlli iniziali.

2. Monitorare il processo mentre Loader configura le porte del cluster locale ed esegue netboot tramite `http://<remote-partner-IP>:65530/recoverydisk/image.tgz`.

Una volta eseguito netboot, `Starting BMR ...` viene visualizzato sullo schermo e il processo completa il processo di installazione.

- a. Se Key Manager non è configurato, viene visualizzato il seguente messaggio:

```
key manager is not configured. Exiting.
```


b. Se viene visualizzato il seguente messaggio, Onboard Key Manager (OKM) è configurato:

```
key manager is configured.  
Entering Bootmenu Option 10...  
  
This option must be used only in disaster recovery procedures.  
Are you sure? (y or n):
```

Andare a per completare il processo di ripristino.

c. Se viene visualizzato il seguente messaggio, EKM (External Key Manager) è configurato. Andare all'argomento EKM e completare il processo di ripristino:

```
Error when fetching key manager config from partner  
169.254.139.209: 28  
Has key manager been configured on this system? {y|n}
```

3. Monitorare il processo BMR mentre esegue il ripristino della configurazione di backup, del file env, di mdb e di rdb dal partner.

4. Il nodo si riavvia e il BMR è completo quando viene visualizzato quanto segue:

```
varfs_backup_restore: update checksum for varfs.tgz  
varfs_backup_restore: restore using /cfc card/x86_64/freebsd/oldvarfs.tgz  
varfs_backup_restore: attempting to restore /var/kmip to the boot  
device  
varfs_backup_restore: failed to restore /var/kmip to the boot device  
varfs_backup_restore: Rebooting to load the new varfs  
.  
Terminated  
varfs_backup_restore: bootarg.abandon_varfs is set! Skipping /var  
backup.
```

Opzione 2: Recupero con Key Manager integrato presente

È possibile ripristinare l'immagine ONTAP (recupero supporti di avvio) dal nodo partner utilizzando `boot_recovery -partner` con le piattaforme ASA R2 che eseguono ONTAP 9.16,0 e versioni successive.

Prima di iniziare

Quando si avvia un nodo e il supporto di avvio su quel nodo è danneggiato, al prompt di Loader vengono visualizzati i seguenti messaggi e il processo di avvio con stop:

```
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>
```

Se viene visualizzato questo messaggio, è necessario ripristinare l'immagine ONTAP

Fasi

1. Dal prompt DI Loader, immettere il comando *boot_recovery -partner*.

La schermata visualizza il messaggio Starting boot media recovery (BMR) process press Ctrl-C to abort... e inizia i controlli iniziali e l'installazione dei file di ripristino di avvio.

- a. Se è configurato Onboard Key Manager (OKM), viene visualizzato quanto segue:

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

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

2. Immettere y quando richiesto.
3. Immettere la passphrase per il gestore delle chiavi integrato quando viene visualizzato Enter the passphrase for onboard key management:
4. Quando viene richiesto di confermare la password, immettere nuovamente la password per il gestore delle chiavi integrato.

```
Enter the passphrase for onboard key management:
Enter the passphrase again to confirm:
Enter the backup data:
TmV0QXBwIEtleSBCbG9iAAECAAAEAAAACAEAAAAAAAAA3yR6UAAAAACEAAAAAAAAAA
QAAAAAAAAACJz1u2AAAAAPX84XY5AU0p4Jcb9t8wiwOZoqyJPJ4L6/j5FHJ9yj/w
RVDO1sZB1E4HO79/zYc82nBwtiHaSPWCbkCrMWuQQDsiAAAAAAAAACgAAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAGAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAAGAAAAAAAAABHVfpxAAAAAHUgdVq0EKNp
.
.
.
.
```

Al termine del processo di ripristino, viene visualizzato quanto segue:

```
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.
```

5. Monitorare il processo BMR mentre esegue il ripristino della configurazione di backup, del file env, di mdb e di rdb dal partner.

Al termine del ripristino, il nodo viene riavviato per completare il processo.

Opzione 3: Ripristino con gestore chiavi esterno presente

È possibile ripristinare l'immagine ONTAP (recupero supporti di avvio) dal nodo partner utilizzando `boot_recovery -partner` con le piattaforme ASA R2 che eseguono ONTAP 9.16,0 e versioni successive.

Quando si avvia un nodo e il supporto di avvio su quel nodo è danneggiato, al prompt di Loader vengono visualizzati i seguenti messaggi e il processo di avvio con stop:

```
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/imagel/kernel:Device not
found

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

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

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

Se viene visualizzato questo messaggio, è necessario ripristinare l'immagine ONTAP.

Fasi

1. Dal prompt DI Loader, immettere il comando *boot_recovery -partner*.

La schermata visualizza il messaggio Starting boot media recovery (BMR) process press Ctrl-C to abort... e inizia i controlli iniziali e l'installazione dei file di ripristino di avvio.

- a. Se EKM (External Key Manager) è configurato, viene visualizzato quanto segue:

```
Error when fetching key manager config from partner
169.254.139.209: 28
Has key manager been configured on this system? {y|n}
```

- b. Immettere *y* se è stato configurato un gestore delle chiavi.

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

L'opzione 11 del menu di avvio richiede all'utente tutte le informazioni di configurazione EKM in modo che i file di configurazione possano essere ricostruiti.

2. Immettere la configurazione EKM ad ogni richiesta.

NOTA: la maggior parte di queste informazioni è stata immessa quando EKM era originariamente

abilitato. È necessario immettere le stesse informazioni immesse durante la configurazione EKM iniziale.

3. Controllare che le `Keystore UUID` e `Cluster UUID` siano corrette.
 - a. Sul nodo partner recuperare l'UUID cluster con il ``cluster identity show`` comando.
 - b. Sul nodo partner recuperare l'UUID keystore con il `vserver show -type admin` comando e il `key-manager keystore show -vserver <nodename>` comando.
 - c. Immettere i valori per UUID keystore e UUID cluster quando richiesto.

NOTA: se il nodo partner non è disponibile, l'UUID keystore e l'UUID cluster possono essere ottenuti dalla chiave Mroot-AK situata sul server chiavi configurato.

Verificare `x-NETAPP-ClusterName: <cluster name>` `x-NETAPP-KeyUsage: "MROOT-AK"` che gli attributi UUID del cluster e UID del keystore siano corretti.

4. Monitorare il recupero e il ripristino di Mroot-AK nel nodo ONTAP.
5. Se il processo non riesce a ripristinare la chiave, verrà visualizzato il seguente messaggio e sarà necessario configurare e0M dalla shell del sistema di menu:

```
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>
```

- a. Eseguire il `boot_recovery -partner` comando sul nodo di recupero.
- b. Quando viene richiesto di eseguire (y o n) le opzioni per EKM, selezionare *n* per tutti.

Dopo aver selezionato l'opzione *n* per i prompt 8, il sistema si arresta al menu di avvio.
- c. Raccogliere le informazioni del file `/cfcard/kmip/servers.cfg` da un altro nodo del cluster. L'utente raccoglierà le seguenti informazioni:
 - L'indirizzo del server KMIP.
 - Porta KMIP.
 - UUID keystore.

- Una copia del certificato client dal file /cfcard/kmip/certs/client.crt.
 - Una copia della chiave client dal file /cfcard/kmip/certs/client.key.
 - Una copia delle CA del server KMIP dal file /cfcard/kmip/certs/CA.pem.
- d. Immettere `systemshell` dal menu di avvio digitando `systemshell` al prompt.
- e. Configurare la rete dal menu della shell del sistema per `e0M`, `netmask` e `gateway`.
- f. Uscire dalla shell del menu con il comando `exit`.
- g. Viene visualizzato il menu di avvio. Selezionare l'opzione 11 per continuare il ripristino EKM.
- h. Rispondere `y` alle seguenti domande e inserire le informazioni richieste precedentemente raccolte quando richiesto:
- Si dispone di una copia del file /cfcard/kmip/certs/client.crt? {y/n}
 - Avete una copia del file /cfcard/kmip/certs/client.key? {y/n}
 - Si dispone di una copia del file /cfcard/kmip/certs/CA.pem? {y/n}
 - Si dispone di una copia del file /cfcard/kmip/servers.cfg? {y/n}
6. Se la chiave viene ripristinata correttamente, il processo di ripristino continua e riavvia il nodo.

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

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.