



Fase 3. Fare il boot node1 con i moduli di sistema sostitutivi

Upgrade controllers

NetApp

February 22, 2024

Sommario

- Fase 3. Fare il boot node1 con i moduli di sistema sostitutivi 1
 - Panoramica 1
 - Fare il boot node1 con i moduli di sistema sostitutivi 1
 - Verificare l'installazione di node1 6
 - Ripristinare la configurazione del gestore delle chiavi sul nodo aggiornato 1 10
 - Spostare gli aggregati non root e le LIF di dati NAS di proprietà del node1 dal node2 al node1 aggiornato. 11

Fase 3. Fare il boot node1 con i moduli di sistema sostitutivi

Panoramica

Durante la fase 3, si avvia node1 con i moduli di sistema aggiornati e si verifica l'installazione aggiornata node1. Se si utilizza NetApp Volume Encryption (NVE), viene ripristinata la configurazione del gestore delle chiavi. È inoltre possibile spostare gli aggregati non root node1 e le LIF dei dati NAS da node2 al node1 aggiornato e verificare che le LIF SAN esistano sul node1.

Fasi

1. "Fare il boot node1 con i moduli di sistema sostitutivi"
2. "Verificare l'installazione di node1"
3. "Ripristinare la configurazione del gestore delle chiavi sul nodo aggiornato 1"
4. "Spostare gli aggregati non root e le LIF di dati NAS di proprietà del node1 dal node2 al node1 aggiornato"

Fare il boot node1 con i moduli di sistema sostitutivi

Node1 con i moduli sostitutivi è ora pronto per l'avvio. Questa sezione fornisce i passaggi necessari per eseguire l'avvio del nodo 1 con i moduli sostitutivi per le seguenti configurazioni di aggiornamento:

Vecchio controller node1	Moduli di sistema node1 sostitutivi
AFF A220 configurato come ASA	Modulo controller AFF A150 ¹
AFF A220 AFF A200 AFF C190	Modulo controller AFF A150 ¹
FAS2620 FAS2720	Modulo controller FAS2820 ¹
AFF A700 configurato come ASA	Controller ASA A900 e moduli NVRAM ²
AFF A700	Controller AFF A900 e moduli NVRAM ²
FAS9000	Controller FAS9500 e moduli NVRAM ²

¹ quando si sostituiscono i moduli controller, si spostano tutte le connessioni dal vecchio al modulo controller sostitutivo.

² quando si sostituiscono il controller e i moduli NVRAM, vengono spostate solo le connessioni della console e di gestione.

Fasi

1. se sono installate unità di crittografia storage NetApp (NSE), procedere come segue.



Se la procedura non è stata ancora eseguita, consultare l'articolo della Knowledge base ["Come verificare se un disco è certificato FIPS"](#) per determinare il tipo di unità con crittografia automatica in uso.

a. Impostare `bootarg.storageencryption.support` a `true` oppure `false`:

Se i seguenti dischi sono in uso...	Quindi...
Unità NSE conformi ai requisiti di crittografia automatica FIPS 140-2 livello 2	<code>setenv bootarg.storageencryption.support true</code>
SED non FIPS di NetApp	<code>setenv bootarg.storageencryption.support false</code>



Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha. È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

b. Accedere al menu di avvio speciale e selezionare l'opzione (10) Set Onboard Key Manager recovery secrets.

Inserire la passphrase e le informazioni di backup registrate in precedenza. Vedere ["Gestire la crittografia dello storage utilizzando Onboard Key Manager"](#).

2. Avviare il nodo nel menu di boot:

```
boot_ontap menu
```

3. Riassegnare i vecchi dischi node1 al nodo sostituzione1 immettendo "22/7" e selezionando l'opzione nascosta `boot_after_controller_replacement` quando il nodo si arresta nel menu di boot.

Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.



Se `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive e`, oppure `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` in caso di errori, attenersi alla seguente procedura:

- Arrestare il nodo al prompt DEL CARICATORE.
- Controllare e ripristinare i bootargs di crittografia dello storage indicati nella [Fase 1](#).
- Al prompt del caricatore, avviare:

```
boot_ontap
```

È possibile utilizzare il seguente esempio come riferimento:

Espandere l'esempio di output della console

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
.
<output truncated>
.
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)? 22/7

(22/7)                                Print this secret List
(25/6)                                Force boot with multiple filesystem
disks missing.
(25/7)                                Boot w/ disk labels forced to clean.
(29/7)                                Bypass media errors.
(44/4a)                               Zero disks if needed and create new
flexible root volume.
(44/7)                                Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                          Clean all configuration on boot
```

```

device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)          Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.

```

The boot device has changed. System configuration information could be lost. Use option (6) to restore the system configuration, or option (4) to initialize all disks and setup a new system. Normal Boot is prohibited.

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)? boot_after_controller_replacement

```

This will replace all flash-based configuration with the last backup to disks. Are you sure you want to continue?: yes

```

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id

```

```

= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.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: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...

.
System rebooting...

.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:

```



Gli ID di sistema mostrati nell'esempio precedente sono ID di esempio. Gli ID di sistema effettivi dei nodi che si stanno aggiornando saranno diversi.

Tra l'immissione dei nomi dei nodi al prompt e il prompt di accesso, il nodo viene riavviato alcune volte per ripristinare le variabili di ambiente, aggiornare il firmware sulle schede del sistema e per altri aggiornamenti del ONTAP.

Verificare l'installazione di node1

È necessario verificare l'installazione node1 con i moduli di sistema sostitutivi. Poiché non sono state apportate modifiche alle porte fisiche, non è necessario mappare le porte fisiche dal vecchio nodo 1 al nodo sostituito.

A proposito di questa attività

Dopo aver avviato il nodo 1 con il modulo controller sostitutivo, verificare che sia installato correttamente. È necessario attendere che il nodo 1 si unisca al quorum, quindi riprendere l'operazione di sostituzione del controller.

A questo punto della procedura, l'operazione di aggiornamento del controller dovrebbe essere stata sospesa poiché node1 tenta di unirsi automaticamente al quorum.

Fasi

1. Verificare che node1 si sia Unito al quorum:

```
cluster show -node node1 -fields health
```

L'output di health il campo deve essere true.

2. Verificare che node1 faccia parte dello stesso cluster di node2 e che sia integro:

```
cluster show
```

3. Passare alla modalità avanzata dei privilegi:

```
set advanced
```

4. Controllare lo stato dell'operazione di sostituzione del controller e verificare che sia in stato di pausa e nello stesso stato in cui si trovava prima dell'arresto del node1 per eseguire le attività fisiche di installazione di nuovi controller e cavi in movimento:

```
system controller replace show
```

```
system controller replace show-details
```

5. Riprendere l'operazione di sostituzione del controller:

```
system controller replace resume
```

6. L'operazione di sostituzione del controller viene interrotta per l'intervento con il seguente messaggio:


```
Cluster::*> system controller replace show
```

Node	Status	Error-Action
Node1	Paused-for-intervention	Follow the instructions given in
Node2	None	Step Details

Step Details:

To complete the Network Reachability task, the ONTAP network configuration must be manually adjusted to match the new physical network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For detailed commands and instructions, refer to the "Re-creating VLANs, ifgrps, and broadcast domains" section of the upgrade controller hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-replacement network displaced-vlans restore" to restore the VLAN on the desired port.

2 entries were displayed.



In questa procedura, la sezione *creazione di VLAN, ifgrps e domini di trasmissione* è stata rinominata *Ripristino configurazione di rete su node1*.

7. Con la sostituzione del controller in stato di pausa, passare a. [Ripristinare la configurazione di rete sul nodo 1](#).

Ripristinare la configurazione di rete sul nodo 1

Dopo aver confermato che node1 è in quorum e può comunicare con node2, verificare che le VLAN, i gruppi di interfacce e i domini di broadcast di node1 siano visibili sul node1. Inoltre, verificare che tutte le porte di rete node1 siano configurate nei domini di trasmissione corretti.

A proposito di questa attività

Per ulteriori informazioni sulla creazione e la ricreazione di VLAN, gruppi di interfacce e domini di trasmissione, fare riferimento a. ["Riferimenti"](#) Per collegarsi al contenuto di *Network Management*.

Fasi

1. Elencare tutte le porte fisiche sul nodo aggiornato1:

```
network port show -node node1
```

Vengono visualizzate tutte le porte di rete fisiche, le porte VLAN e le porte del gruppo di interfacce sul nodo. Da questo output, è possibile visualizzare le porte fisiche spostate in `Cluster` Dominio di broadcast di ONTAP. È possibile utilizzare questo output per agevolare la scelta delle porte da utilizzare come porte membro del gruppo di interfacce, porte di base VLAN o porte fisiche standalone per l'hosting di LIF.

2. Elencare i domini di broadcast sul cluster:

```
network port broadcast-domain show
```

3. Elencare la raggiungibilità delle porte di rete di tutte le porte sul nodo 1:

```
network port reachability show -node node1
```

L'output dovrebbe essere simile al seguente esempio:

```
Cluster::> reachability show -node node1
(network port reachability show)
Node      Port      Expected Reachability      Reachability
Status
-----
Node1
    a0a      Default:Default      ok
    a0a-822   Default:822          ok
    a0a-823   Default:823          ok
    e0M       Default:Mgmt         ok
    e11a      -                    no-reachability
    e11b      -                    no-reachability
    e11c      -                    no-reachability
    e11d      -                    no-reachability
    e3a       -                    no-reachability
    e3b       -                    no-reachability
    e4a       Cluster:Cluster      ok
    e4e       Cluster:Cluster      ok
    e5a       -                    no-reachability
    e7a       -                    no-reachability
    e9a       Default:Default      ok
    e9a-822   Default:822          ok
    e9a-823   Default:823          ok
    e9b       Default:Default      ok
    e9b-822   Default:822          ok
    e9b-823   Default:823          ok
    e9c       Default:Default      ok
    e9d       Default:Default      ok
22 entries were displayed.
```

Nell'esempio precedente, node1 si è avviato dopo la sostituzione del controller. Alcune porte non hanno la

raggiungibilità perché non c'è connettività fisica. È necessario riparare le porte con uno stato di raggiungibilità diverso da `ok`.



Durante l'aggiornamento, le porte di rete e la relativa connettività non devono cambiare. Tutte le porte devono risiedere nei domini di trasmissione corretti e la raggiungibilità delle porte di rete non deve cambiare. Tuttavia, prima di spostare i file LIF da node2 a node1, è necessario verificare la raggiungibilità e lo stato di salute delle porte di rete.

4. riparare la raggiungibilità per ciascuna porta sul node1 con uno stato di raggiungibilità diverso da `ok` utilizzando il seguente comando, nel seguente ordine:

```
network port reachability repair -node node_name -port port_name
```

- a. Porte fisiche
- b. Porte VLAN

L'output dovrebbe essere simile al seguente esempio:

```
Cluster ::> reachability repair -node node1 -port e11b
```

```
Warning: Repairing port "node1:e11b" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Un messaggio di avviso, come mostrato nell'esempio precedente, è previsto per le porte con uno stato di raggiungibilità che potrebbe essere diverso dallo stato di raggiungibilità del dominio di broadcast in cui si trova attualmente. Esaminare la connettività della porta e rispondere `y` oppure `n` a seconda dei casi.

Verificare che tutte le porte fisiche abbiano la raggiungibilità prevista:

```
network port reachability show
```

Quando viene eseguita la riparazione della raggiungibilità, ONTAP tenta di posizionare le porte nei domini di trasmissione corretti. Tuttavia, se non è possibile determinare la raggiungibilità di una porta e non appartiene a nessuno dei domini di broadcast esistenti, ONTAP creerà nuovi domini di broadcast per queste porte.

5. Verificare la raggiungibilità delle porte:

```
network port reachability show
```

Quando tutte le porte sono configurate correttamente e aggiunte ai domini di trasmissione corretti, il `network port reachability show` il comando deve riportare lo stato di raggiungibilità come `ok` per tutte le porte connesse e lo stato come `no-reachability` per porte senza connettività fisica. Se una delle porte riporta uno stato diverso da questi due, eseguire la riparazione della raggiungibilità e aggiungere o rimuovere le porte dai propri domini di trasmissione come indicato nella [Fase 4](#).

6. Verificare che tutte le porte siano state inserite nei domini di broadcast:

```
network port show
```

7. Verificare che tutte le porte nei domini di trasmissione abbiano configurato la MTU (Maximum Transmission Unit) corretta:

```
network port broadcast-domain show
```

8. Ripristinare le porte LIF home, specificando le porte Vserver e LIF home, se presenti, che devono essere ripristinate seguendo questa procedura:

- a. Elencare eventuali LIF spostati:

```
displaced-interface show
```

- b. Ripristinare i nodi home LIF e le porte home:

```
displaced-interface restore-home-node -node node_name -vserver vserver_name  
-lif-name LIF_name
```

9. Verificare che tutte le LIF dispongano di una porta home e siano amministrativamente up:

```
network interface show -fields home-port,status-admin
```

Ripristinare la configurazione del gestore delle chiavi sul nodo aggiornato 1

Se si utilizza NetApp aggregate Encryption (NAE) o NetApp Volume Encryption (NVE) per crittografare i volumi sul sistema che si sta aggiornando, la configurazione della crittografia deve essere sincronizzata con i nuovi nodi. Se non si risincronizza il gestore delle chiavi, quando si trasferono gli aggregati node1 da node2 al node1 aggiornato utilizzando ARL, potrebbero verificarsi errori perché node1 non dispone delle chiavi di crittografia necessarie per portare online volumi e aggregati crittografati.

A proposito di questa attività

Sincronizzare la configurazione della crittografia con i nuovi nodi seguendo questa procedura:

Fasi

1. Eseguire il seguente comando da node1:

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

2. Prima di spostare gli aggregati di dati, verificare che la chiave SVM-KEK sia ripristinata su "true" in node1:

```
::> security key-manager key query -node node1 -fields restored -key  
-type SVM-KEK
```

Esempio

```
::> security key-manager key query -node node1 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node1	svml	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f0000000000000000

Spostare gli aggregati non root e le LIF di dati NAS di proprietà del node1 dal node2 al node1 aggiornato

Dopo aver verificato la configurazione di rete su node1 e prima di spostare gli aggregati da node2 a node1, verificare che i dati NAS LIF appartenenti a node1 che sono attualmente su node2 vengano ricollocati da node2 a node1. È inoltre necessario verificare che le LIF SAN esistano nel node1.

A proposito di questa attività

Le LIF remote gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Lo spostamento delle LIF SAN non è necessario per lo stato del cluster o del servizio durante l'aggiornamento. LE LIF SAN non vengono spostate a meno che non sia necessario mapparle su nuove porte. Dopo aver portato il node1 online, è necessario verificare che i LIF siano integri e posizionati sulle porte appropriate.

Fasi

1. Riprendere l'operazione di trasferimento:

```
system controller replace resume
```

Il sistema esegue le seguenti operazioni:

- Verifica del quorum del cluster
- Verifica dell'ID di sistema
- Controllo della versione dell'immagine
- Verifica della piattaforma di destinazione
- Verifica della raggiungibilità della rete

L'operazione viene interrotta in questa fase del controllo della raggiungibilità della rete.

2. Eseguire un controllo della raggiungibilità della rete:

```
network port reachability show -node node1
```

Verificare che tutte le porte connesse, inclusi il gruppo di interfacce e le porte VLAN, mostrino il loro stato

come OK.

3. Riprendere l'operazione di trasferimento:

```
system controller replace resume
```

Il sistema esegue i seguenti controlli:

- Controllo dello stato del cluster
- Controllo dello stato LIF del cluster

Dopo aver eseguito questi controlli, il sistema ricolloca gli aggregati non root e le LIF dei dati NAS di proprietà di node1 nel nuovo node1.

L'operazione di sostituzione del controller viene interrotta al termine del trasferimento delle risorse.

4. Controllare lo stato delle operazioni di trasferimento aggregato e LIF dei dati NAS:

```
system controller replace show-details
```

Se la procedura di sostituzione del controller è in pausa, controllare e correggere l'errore, se presente, quindi il problema `resume` per continuare l'operazione.

5. Se necessario, ripristinare e ripristinare eventuali LIF spostate. Elencare eventuali LIF spostate:

```
cluster controller-replacement network displaced-interface show
```

In caso di spostamento di LIF, ripristinare il nodo home al nodo node1:

```
cluster controller-replacement network displaced-interface restore-home-node
```

6. Riprendere l'operazione per richiedere al sistema di eseguire i controlli successivi richiesti:

```
system controller replace resume
```

Il sistema esegue i seguenti post-controlli:

- Verifica del quorum del cluster
- Controllo dello stato del cluster
- Controllo della ricostruzione degli aggregati
- Controllo dello stato dell'aggregato
- Controllo dello stato del disco
- Controllo dello stato LIF del cluster
- Controllo del volume

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.