



Ripristina dai guasti del nodo amministratore primario

StorageGRID software

NetApp
July 23, 2026

Sommario

- Ripristina dai guasti del nodo amministratore primario 1
 - Ripristina dai guasti del nodo amministratore primario di StorageGRID 1
 - Copia i log di controllo da un nodo di amministrazione StorageGRID primario non riuscito 1
 - Sostituire il nodo di amministrazione primario di StorageGRID 2
 - Configura un nodo Admin primario sostitutivo in StorageGRID 3
 - Determinare i requisiti di hotfix per il nodo amministratore primario in StorageGRID 5
 - Ripristina il registro di controllo sul nodo di amministrazione StorageGRID primario recuperato 5
 - Ripristina il database di StorageGRID Admin Node durante il recupero del nodo amministratore primario . . 6
 - Ripristina le metriche Prometheus durante il ripristino del nodo amministratore primario di StorageGRID. . . 8

Ripristina dai guasti del nodo amministratore primario

Ripristina dai guasti del nodo amministratore primario di StorageGRID

Per ripristinare il sistema in caso di errore del nodo di amministrazione primario, devi completare una serie specifica di attività. Il nodo di amministrazione primario ospita il servizio Configuration Management Node (CMN) per la grid.



Devi riparare o sostituire tempestivamente un nodo di amministrazione primario guasto, altrimenti potresti non riuscire a eseguire alcune procedure di manutenzione.

Segui questi high-level passaggi per ripristinare un nodo amministratore primario:

1. ["Copia i log di controllo dal nodo Admin primario guasto"](#)
2. ["Sostituisci il nodo Admin primario"](#)
3. ["Configura il nodo amministratore primario sostitutivo"](#)
4. ["Determina se è necessario un hotfix per il nodo di amministrazione primario ripristinato"](#)
5. ["Ripristina il registro di controllo sul nodo amministratore primario ripristinato"](#)
6. ["Ripristina il database Admin Node quando recuperi un nodo Admin Node primario"](#)
7. ["Ripristina le metriche Prometheus durante il ripristino di un nodo di amministrazione primario"](#)

Copia i log di controllo da un nodo di amministrazione StorageGRID primario non riuscito

Se puoi copiare i log di audit dal nodo Admin primario guasto, dovresti conservarli per mantenere la registrazione dell'attività e dell'utilizzo del grid. Puoi ripristinare i log di audit conservati sul nodo Admin primario recuperato dopo che è tornato operativo.

Informazioni su questa attività

Questa procedura copia i file di log di controllo dal nodo Admin guasto in una posizione temporanea su un nodo della griglia separato. Questi file di log di controllo conservati possono poi essere copiati sul nodo Admin sostitutivo. I file di log di controllo non vengono copiati automaticamente sul nuovo nodo Admin.

A seconda del tipo di errore, potresti non riuscire a copiare i log di audit da un Admin Node guasto. Se la distribuzione ha solo un Admin Node, l'Admin Node ripristinato inizia a registrare gli eventi nel file di log di audit in un nuovo file vuoto e i dati registrati in precedenza vengono persi. Se la distribuzione include più di un Admin Node, puoi recuperare i log di audit da un altro Admin Node.



Se al momento non puoi accedere ai log di controllo sul nodo Admin guasto, potresti riuscire ad accedervi più tardi, ad esempio dopo il ripristino dell'host.

Passaggi

1. Se possibile, accedi al nodo Admin primario non funzionante. Altrimenti, accedi a qualsiasi nodo Admin

disponibile.

- a. Inserisci il seguente comando: `ssh admin@grid_node_IP`
- b. Inserisci la password indicata nel file `Passwords.txt`.
- c. Inserisci il seguente comando per passare all'utente root: `su -`
- d. Inserisci la password indicata nel file `Passwords.txt`.

Quando sei connesso come root, il prompt cambia da `$` a `#`.

2. Interrompi il servizio AMS per impedirgli di creare un nuovo file di log: `service ams stop`
3. `${post_edited_translations.segment}`

```
cd /var/local/audit/export
```

(o `cd /var/local/log` sui sistemi precedenti)

4. Rinomina il file di log di origine con un nome file numerato univoco.



- Se il file di log si trova nella `/var/local/audit/export` directory, il suo nome è `audit.log`.
- Se il file di log si trova nella `/var/local/log` directory, il suo nome è `localaudit.log`.

Ad esempio, rinomina il file `localaudit.log` in `2025-10-22.txt.1`.

```
ls -l
mv localaudit.log 2025-10-22.txt.1
```

5. Riavvia il servizio AMS: `service ams start`
6. Crea la directory in cui copiare tutti i file di log di audit in una posizione temporanea su un nodo della griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando richiesto, inserisci la password per admin.

7. Copia tutti i file di log di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando richiesto, inserisci la password per admin.

8. Disconnettiti come root: `exit`

Sostituire il nodo di amministrazione primario di StorageGRID

Per ripristinare un nodo di amministrazione primario, devi prima sostituire l'hardware fisico o virtuale.

Puoi sostituire un nodo di amministrazione primario guasto con un nodo di amministrazione primario in esecuzione sulla stessa piattaforma, oppure puoi sostituire un nodo di amministrazione primario in esecuzione su VMware o su un host Linux con un nodo di amministrazione primario ospitato su un'appliance di servizi.

Usa la procedura che corrisponde alla piattaforma di sostituzione che scegli per il nodo. Dopo che hai completato la procedura di sostituzione del nodo (che va bene per tutti i tipi di nodo), quella procedura ti guiderà al passaggio successivo per il ripristino del nodo Admin primario.

Piattaforma di sostituzione	<code>\${post_edited_translations.segment}</code>
VMware	"Sostituisci un nodo VMware"
Linux	"Sostituisci un nodo Linux"
<code>\${post_edited_translations.segment}</code>	"Sostituisci un appliance di servizi"
OpenStack	I file del disco della macchina virtuale e gli script forniti da NetApp per OpenStack non sono più supportati per le operazioni di ripristino. Se devi ripristinare un nodo in esecuzione in una distribuzione OpenStack, scarica i file per il tuo sistema operativo Linux. Poi, segui la procedura per "sostituire un nodo Linux".

Configura un nodo Admin primario sostitutivo in StorageGRID

Il nodo sostitutivo deve essere configurato come nodo Admin primario per il tuo sistema StorageGRID.

Prima di iniziare

- Per i nodi di amministrazione primari ospitati su macchine virtuali, la macchina virtuale è stata distribuita, accesa e inizializzata.
- Per i nodi di amministrazione primari ospitati su un'appliance di servizi, hai sostituito l'appliance e hai installato il software. Vedi il "istruzioni di installazione per il tuo appliance".
- Hai il backup più recente del file del pacchetto di ripristino (`sgws-recovery-package-id-revision.zip`).
- `${post_edited_translations.segment}`

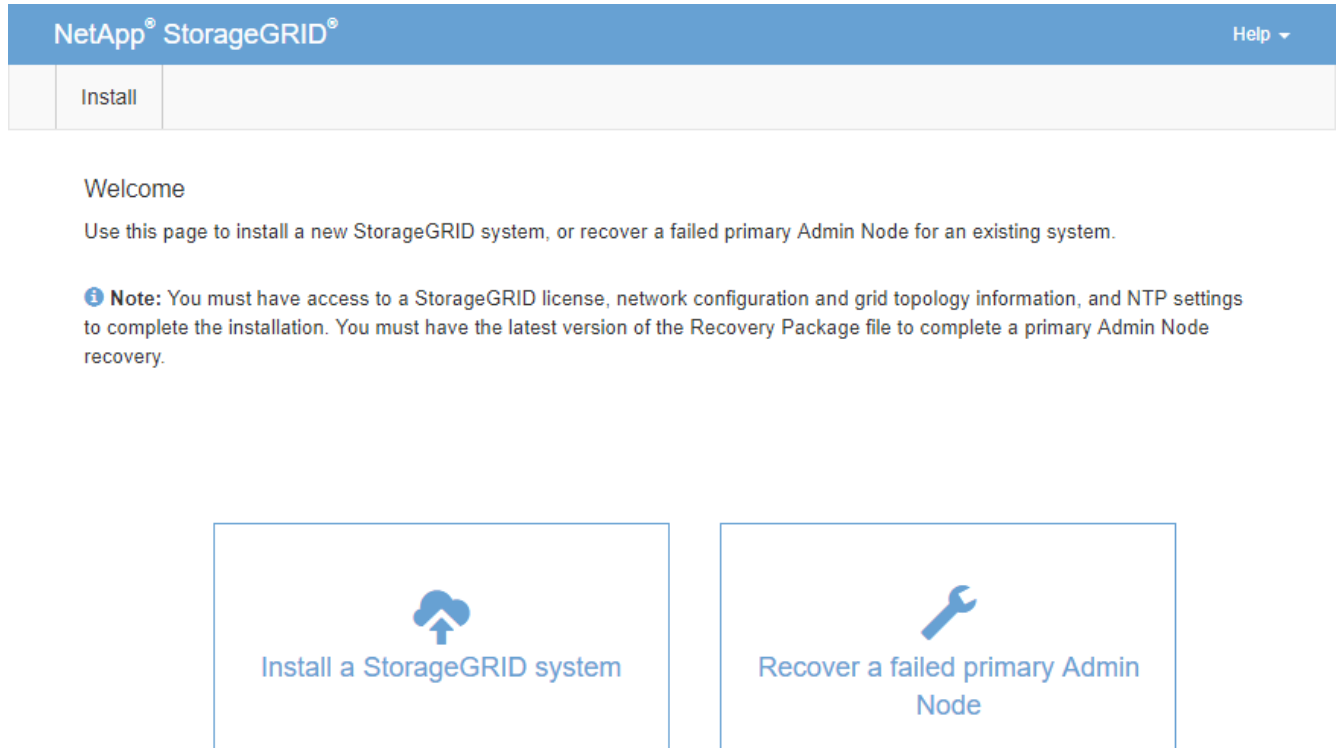
Passaggi

1. Apri il tuo browser web e vai a `https://primary_admin_node_ip`.
2. Gestisci una password di installazione temporanea all'occorrenza:
 - Se hai già impostato una password utilizzando uno di questi metodi, inseriscila per procedere.
 - Un utente ha impostato la password durante l'accesso al programma di installazione in precedenza
 - Per i sistemi bare metal, la password è stata importata automaticamente dal file di configurazione del nodo a `/etc/storagegrid/nodes/<node_name>.conf`
 - Per le macchine virtuali, la password SSH/console è stata importata automaticamente dalle

proprietà OVF

- Se non hai impostato una password, puoi impostarne una per proteggere l'installer di StorageGRID.

3. Fai clic su **Ripristina un nodo Admin primario non funzionante**.



4. Carica il backup più recente del pacchetto di ripristino:

- Fai clic su **Sfoggia**.
- Individua il file del pacchetto di ripristino più recente per il tuo sistema StorageGRID e fai clic su **Apri**.

5. \${post_edited_translations.segment}

6. Fai clic su **Avvia ripristino**.

Il processo di ripristino ha inizio. Il Grid Manager potrebbe risultare non disponibile per alcuni minuti mentre vengono avviati i servizi necessari. Quando il ripristino è completo, viene visualizzata la pagina di accesso.

7. Se il single sign-on (SSO) è abilitato per il tuo sistema StorageGRID e la relying party trust per l'Admin Node che hai ripristinato era configurata per usare il certificato predefinito dell'interfaccia di gestione, aggiorna (o elimina e ricrea) la relying party trust del nodo in Active Directory Federation Services (AD FS). Usa il nuovo certificato server predefinito che è stato generato durante il processo di ripristino dell'Admin Node.



Per configurare una relying party trust, vedi ["Configura single sign-on"](#). Per accedere al certificato server predefinito, accedi alla shell dei comandi dell'Admin Node. Vai alla directory `/var/local/mgmt-api` e seleziona il file `server.crt`.



Dopo aver ripristinato un nodo amministratore primario, ["determina se devi applicare una hotfix"](#).

Determinare i requisiti di hotfix per il nodo amministratore primario in StorageGRID

Dopo aver ripristinato un nodo amministratore primario, verifica se devi applicare una hotfix.

Prima di iniziare

Il ripristino del nodo amministratore primario è completo.

Passaggi

1. Accedi al Grid Manager utilizzando un ["browser web supportato"](#).
2. Selezionare **Nodi**.
3. Dall'elenco a sinistra, seleziona il nodo Admin principale.
4. Nella scheda Panoramica, prendi nota della versione visualizzata nel campo **Versione software**.
5. Seleziona un altro nodo della griglia.
6. Nella scheda Panoramica, prendi nota della versione visualizzata nel campo **Versione software**.
 - Se le versioni visualizzate nei campi **Versione software** sono identiche, non devi applicare un hotfix.
 - Se le versioni visualizzate nei campi **Versione software** sono diverse, devi ["applicare una hotfix"](#) aggiornare il nodo Admin primario ripristinato alla stessa versione.

Ripristina il registro di controllo sul nodo di amministrazione StorageGRID primario recuperato

Se sei riuscito a conservare il registro di controllo del nodo amministrativo primario guasto, puoi copiarlo sul nodo amministrativo primario che stai ripristinando.

Prima di iniziare

- Il nodo di amministrazione ripristinato è installato e in esecuzione.
- Hai copiato i log di controllo in un'altra posizione dopo che l'Admin Node originale ha smesso di funzionare.

Informazioni su questa attività

Se un Admin Node si guasta, i log di audit salvati su quell'Admin Node potrebbero andare persi. Potresti riuscire a preservare i dati dalla perdita copiando i log di audit dall'Admin Node guasto e poi ripristinando questi log di audit sull'Admin Node recuperato. A seconda del tipo di guasto, potrebbe non essere possibile copiare i log di audit dall'Admin Node guasto. In tal caso, se il deployment ha più di un Admin Node, puoi recuperare i log di audit da un altro Admin Node, dato che i log di audit vengono replicati su tutti gli Admin Node.

Se è presente un solo nodo amministratore e non è possibile copiare il registro di controllo dal nodo guasto, il nodo amministratore ripristinato inizia a registrare gli eventi nel registro di controllo come se l'installazione fosse nuova.

Devi ripristinare un Admin Node il prima possibile per ripristinare la funzionalità di logging.

Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. Puoi saltare questi passaggi se si verifica una delle seguenti condizioni:



- Hai configurato un server syslog esterno e ora i log di controllo vengono inviati al server syslog invece che agli Admin Nodes.
- Hai specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.

Vedi ["Configura la gestione dei log e il server syslog esterno"](#) per dettagli.

Passaggi

1. Accedi al nodo di amministrazione ripristinato:

- a. Inserisci il seguente comando: `ssh admin@recovery_Admin_Node_IP`
- b. Inserisci la password indicata nel file `Passwords.txt`.
- c. Inserisci il seguente comando per passare all'utente root: `su -`
- d. Inserisci la password indicata nel file `Passwords.txt`.

Dopo aver effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Verifica quali file di audit sono stati conservati: `cd /var/local/audit/export`

3. Copia i file di registro di controllo conservati sul nodo amministratore ripristinato: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Quando richiesto, inserisci la password per admin.

4. Per motivi di sicurezza, elimina i log di controllo dal nodo della griglia guasto dopo aver verificato che siano stati copiati correttamente sul nodo di amministrazione ripristinato.

5. Aggiorna le impostazioni utente e di gruppo dei file di registro di controllo sul nodo amministratore ripristinato: `chown ams-user:bycast *`

6. Disconnettiti come root: `exit`

Ripristina il database di StorageGRID Admin Node durante il recupero del nodo amministratore primario

Se vuoi conservare le informazioni storiche relative ad attributi e avvisi su un nodo di amministrazione primario che ha riscontrato un errore, puoi ripristinare il database del nodo di amministrazione. Puoi ripristinare questo database solo se il tuo sistema StorageGRID include un altro nodo di amministrazione.

Prima di iniziare

- Il nodo di amministrazione ripristinato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Hai il file `Passwords.txt`.
- `${post_edited_translations.segment}`

Informazioni su questa attività

Se un Admin Node si guasta, le informazioni storiche memorizzate nel suo database Admin Node vengono perse. Questo database include le seguenti informazioni:

- `${post_edited_translations.segment}`
- Dati storici sugli attributi, utilizzati nei grafici in stile legacy nella pagina Nodes

Quando recuperi un nodo di amministrazione, il processo di installazione del software crea un database vuoto per il nodo di amministrazione sul nodo recuperato. Tuttavia, il nuovo database include solo le informazioni relative ai server e ai servizi attualmente presenti nel sistema o aggiunti in seguito.

Se hai ripristinato un nodo amministratore primario e il tuo sistema StorageGRID dispone di un altro nodo amministratore, puoi ripristinare le informazioni storiche copiando il database del nodo amministratore da un nodo amministratore non primario (il *nodo amministratore di origine*) al nodo amministratore primario ripristinato. Se il tuo sistema dispone solo di un nodo amministratore primario, non puoi ripristinare il database del nodo amministratore.



La copia del database dell'Admin Node potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi sono fermi sull'Admin Node di origine.

Passaggi

1. Accedi al nodo di amministrazione di origine:
 - a. Inserisci il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password indicata nel file `Passwords.txt`.
 - c. Inserisci il seguente comando per passare all'utente root: `su -`
 - d. Inserisci la password indicata nel file `Passwords.txt`.
2. Dal nodo di amministrazione di origine, arresta il servizio MI: `service mi stop`
3. Dal nodo Admin di origine, arresta il servizio Management Application Program Interface (mgmt-api):
`service mgmt-api stop`
4. Completa i seguenti passaggi sul nodo Admin ripristinato:
 - a. Accedi al nodo di amministrazione ripristinato:
 - i. Inserisci il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password indicata nel file `Passwords.txt`.
 - iii. Inserisci il seguente comando per passare all'utente root: `su -`
 - iv. Inserisci la password indicata nel file `Passwords.txt`.
 - b. Interrompi il servizio MI: `service mi stop`
 - c. Interrompi il servizio mgmt-api: `service mgmt-api stop`
 - d. Aggiungi la chiave privata SSH all'agente SSH. Inserisci: `ssh-add`
 - e. Inserisci la password di accesso SSH indicata nel file `Passwords.txt`.
 - f. Copia il database dal nodo amministratore di origine al nodo amministratore ripristinato:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Quando richiesto, conferma che vuoi sovrascrivere il database MI sul nodo Admin ripristinato.

Il database e i dati storici vengono copiati sul nodo di amministrazione ripristinato. Quando l'operazione di copia è terminata, lo script avvia il nodo di amministrazione ripristinato.

h. Quando non hai più bisogno dell'accesso senza password ad altri server, rimuovi la chiave privata dall'agente SSH. Inserisci:`ssh-add -D`

5. Riavvia i servizi sul nodo amministratore di origine: `service servermanager start`

Ripristina le metriche Prometheus durante il ripristino del nodo amministratore primario di StorageGRID

Facoltativamente, puoi conservare le metriche storiche gestite da Prometheus su un nodo di amministrazione primario che ha subito un errore. Le metriche di Prometheus possono essere ripristinate solo se il tuo sistema StorageGRID include un altro nodo di amministrazione.

Prima di iniziare

- Il nodo di amministrazione ripristinato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Hai il file `Passwords.txt`.
- `${post_edited_translations.segment}`

Informazioni su questa attività

Se un Admin Node si guasta, le metriche mantenute nel database Prometheus sull'Admin Node vengono perse. Quando recuperi l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Dopo l'avvio dell'Admin Node recuperato, registra le metriche come se avessi effettuato una nuova installazione del sistema StorageGRID.

Se hai ripristinato un nodo Admin primario e il tuo sistema StorageGRID dispone di un altro nodo Admin, puoi ripristinare le metriche storiche copiando il database Prometheus da un nodo Admin non primario (il *nodo Admin di origine*) al nodo Admin primario ripristinato. Se il tuo sistema dispone solo di un nodo Admin primario, non puoi ripristinare il database Prometheus.



La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi sono fermi sul nodo di amministrazione di origine.

Passaggi

1. Accedi al nodo di amministrazione di origine:
 - a. Inserisci il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password indicata nel file `Passwords.txt`.
 - c. Inserisci il seguente comando per passare all'utente root: `su -`
 - d. Inserisci la password indicata nel file `Passwords.txt`.
2. Dall'Admin Node di origine, arresta il servizio Prometheus: `service prometheus stop`
3. Completa i seguenti passaggi sul nodo Admin ripristinato:

a. Accedi al nodo di amministrazione ripristinato:

- i. Inserisci il seguente comando: `ssh admin@grid_node_IP`
- ii. Inserisci la password indicata nel file `Passwords.txt`.
- iii. Inserisci il seguente comando per passare all'utente root: `su -`
- iv. Inserisci la password indicata nel file `Passwords.txt`.

b. Interrompi il servizio Prometheus: `service prometheus stop`

c. Aggiungi la chiave privata SSH all'agente SSH. Inserisci: `ssh-add`

d. Inserisci la password di accesso SSH indicata nel file `Passwords.txt`.

e. Copia il database Prometheus dal nodo Admin di origine al nodo Admin ripristinato:

`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Quando richiesto, premi **Invio** per confermare che vuoi distruggere il nuovo database Prometheus sul nodo Admin ripristinato.

Il database Prometheus originale e i relativi dati storici vengono copiati sul nodo di amministrazione ripristinato. Quando l'operazione di copia è terminata, lo script avvia il nodo di amministrazione ripristinato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

a. Quando non hai più bisogno dell'accesso senza password ad altri server, rimuovi la chiave privata dall'agente SSH. Inserisci: `ssh-add -D`

4. Riavvia il servizio Prometheus sul nodo Admin di origine. `service prometheus start`

Informazioni sul copyright

Copyright © 2026 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.