Panoramica dei messaggi di audit

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-115/audit/audit-message-flow-and-retention.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Panoramica dei messaggi di audit . . . 1
Controllare il flusso e la conservazione dei messaggi . . . 1
Controllare il flusso dei messaggi . . . 1
Modifica dei livelli dei messaggi di audit . . . 4
Accesso al file di log di audit . . . 6
Controllo della rotazione del file di log . . . 7

Panoramica dei messaggi di audit

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di audit e dei registri di audit di StorageGRID. È possibile utilizzare queste informazioni per leggere e analizzare il registro di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli amministratori responsabili della produzione di report sull'attività e sull'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID.

Si presume che si abbia una buona comprensione della natura delle attività controllate all'interno del sistema StorageGRID. Per utilizzare il file di log di testo, è necessario disporre dell'accesso alla condivisione di audit configurata nel nodo di amministrazione.

Informazioni correlate

"Amministrare StorageGRID"

Controllare il flusso e la conservazione dei messaggi

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. È necessario comprendere in che modo questi messaggi di audit vengono spostati nel sistema StorageGRID `audit.log` file.

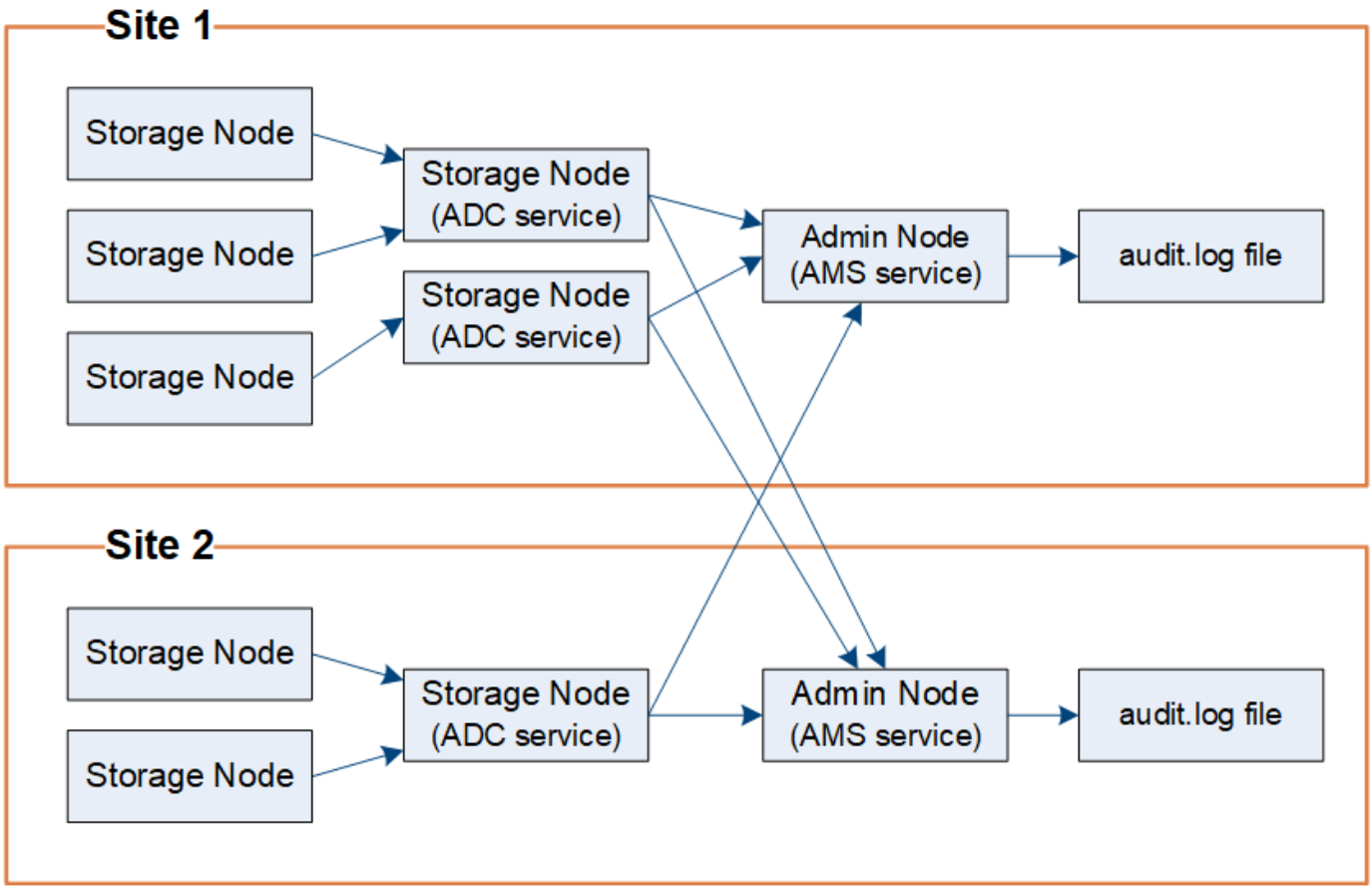
Controllare il flusso dei messaggi

I messaggi di audit vengono elaborati dai nodi di amministrazione e dai nodi di storage che dispongono di un servizio ADC (Administrative Domain Controller).

Come mostrato nel diagramma di flusso dei messaggi di audit, ciascun nodo StorageGRID invia i propri messaggi di audit a uno dei servizi ADC nel sito del data center. Il servizio ADC viene attivato automaticamente per i primi tre nodi di storage installati in ogni sito.

A sua volta, ogni servizio ADC agisce come un relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID, che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

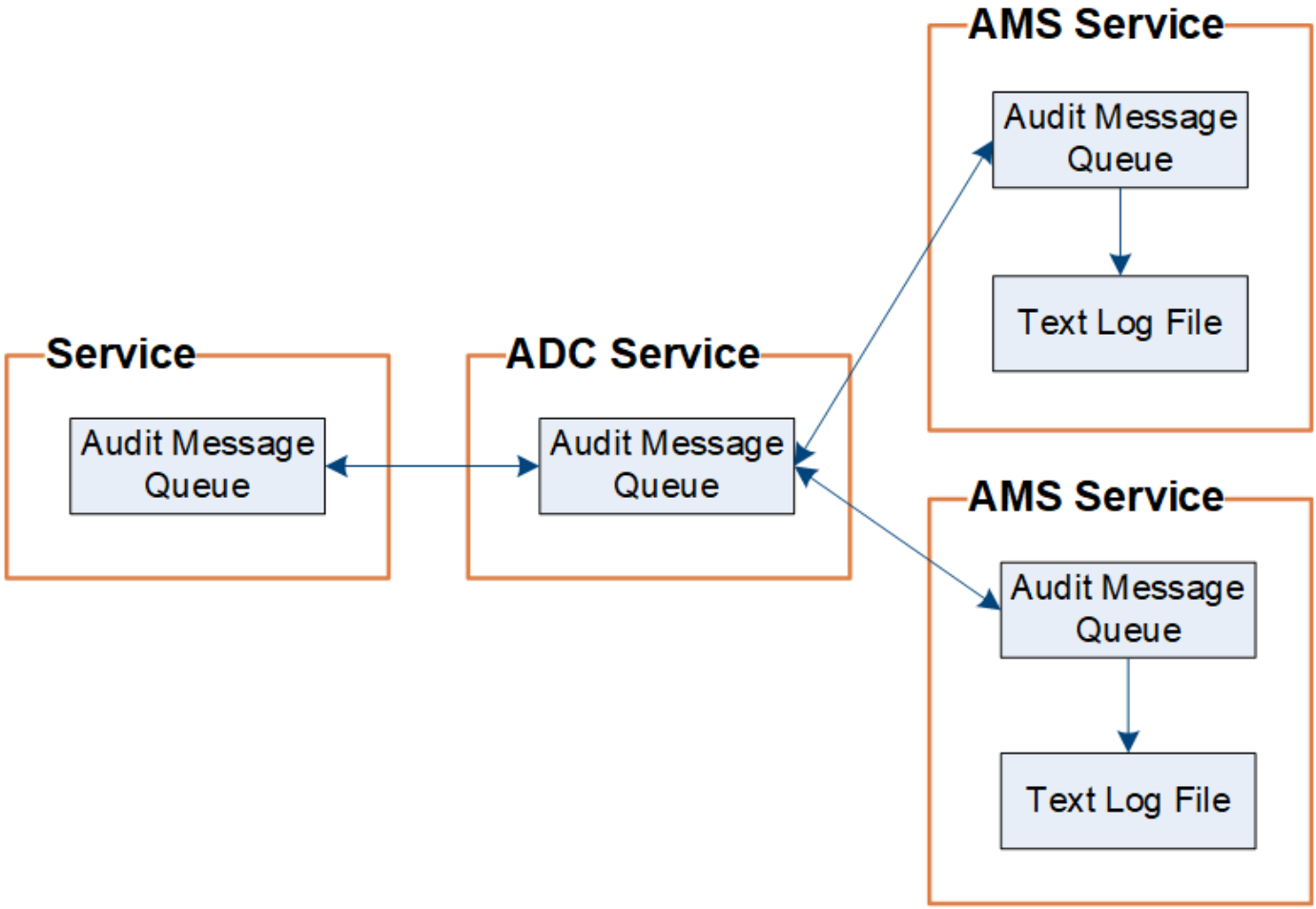
Ogni nodo amministrativo memorizza i messaggi di audit in file di log di testo; il file di log attivo viene denominato `audit.log`.



Controllare la conservazione dei messaggi

StorageGRID utilizza un processo di copia e cancellazione per garantire che non vengano persi messaggi di controllo prima di poter essere scritti nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di audit, il messaggio viene memorizzato in una coda di messaggi di audit sul disco di sistema del nodo Grid. Una copia del messaggio viene sempre mantenuta in una coda di messaggi di audit fino a quando il messaggio non viene scritto nel file di log di audit nel nodo di amministrazione `/var/local/audit/export` directory. In questo modo si evita la perdita di un messaggio di audit durante il trasporto.



La coda dei messaggi di audit può aumentare temporaneamente a causa di problemi di connettività di rete o di capacità di audit insufficiente. Man mano che le code aumentano, consumano più spazio disponibile in ogni nodo `/var/local/` directory. Se il problema persiste e la directory dei messaggi di controllo di un nodo diventa troppo piena, i singoli nodi assegneranno la priorità all'elaborazione del proprio backlog e diventeranno temporaneamente non disponibili per i nuovi messaggi.

In particolare, potrebbero verificarsi i seguenti comportamenti:

- Se il `/var/local/audit/export` La directory utilizzata da un nodo amministratore diventa piena, il nodo amministratore viene contrassegnato come non disponibile per i nuovi messaggi di audit fino a quando la directory non è più piena. Le richieste dei client S3 e Swift non sono interessate. L'allarme XAMS (Unreachable Audit Repository) viene attivato quando un repository di audit non è raggiungibile.
- Se il `/var/local/` La directory utilizzata da un nodo di storage con il servizio ADC diventa piena al 92%, il nodo viene contrassegnato come non disponibile per i messaggi di controllo fino a quando la directory non è piena al 87%. Le richieste dei client S3 e Swift ad altri nodi non sono interessate. L'allarme NRLY (Available Audit Relay) viene attivato quando i relè di audit non sono raggiungibili.

> Se non sono disponibili nodi di storage con il servizio ADC, i nodi di storage memorizzano i messaggi di audit in locale.

- Se il `/var/local/` La directory utilizzata da un nodo di storage diventa piena al 85%, il nodo inizia a rifiutare le richieste dei client S3 e Swift con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare un aumento delle code dei messaggi di audit:

- Interruzione di un nodo amministrativo o di un nodo di storage con il servizio ADC. Se uno dei nodi del sistema non è attivo, i nodi rimanenti potrebbero diventare backlogged.
- Tasso di attività sostenuta che supera la capacità di audit del sistema.
- Il `/var/local/` Lo spazio su un nodo di storage ADC diventa pieno per motivi non correlati ai messaggi di audit. In questo caso, il nodo smette di accettare nuovi messaggi di audit e assegna la priorità al backlog corrente, che può causare backlog su altri nodi.

Avviso di coda di audit estesa e allarme di messaggi di audit in coda (AMQS)

Per facilitare il monitoraggio delle dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Large audit queue** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda Storage Node o Admin Node raggiunge determinate soglie.

Se viene attivato l'avviso **Large audit queue** o l'allarme AMQS legacy, iniziare controllando il carico sul sistema. Se si è verificato un numero significativo di transazioni recenti, l'avviso e l'allarme devono essere risolti nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di severità, visualizzare un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, il carico di audit ha probabilmente superato la capacità di audit del sistema. Ridurre la velocità di funzionamento del client o diminuire il numero di messaggi di audit registrati modificando il livello di audit per le scritture del client e le letture del client su Error (errore) o Off. Vedere "'Modifica dei livelli dei messaggi di audit"."

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto di rete o nodo. Per questo motivo, nel registro di controllo potrebbero essere presenti messaggi duplicati.

Modifica dei livelli dei messaggi di audit

È possibile regolare i livelli di audit per aumentare o diminuire il numero di messaggi di audit registrati nel registro di audit per ciascuna categoria di messaggi di audit.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

I messaggi di audit registrati nel log di audit vengono filtrati in base alle impostazioni della pagina **Configurazione** > **monitoraggio** > **controllo**.

È possibile impostare un livello di audit diverso per ciascuna delle seguenti categorie di messaggi:

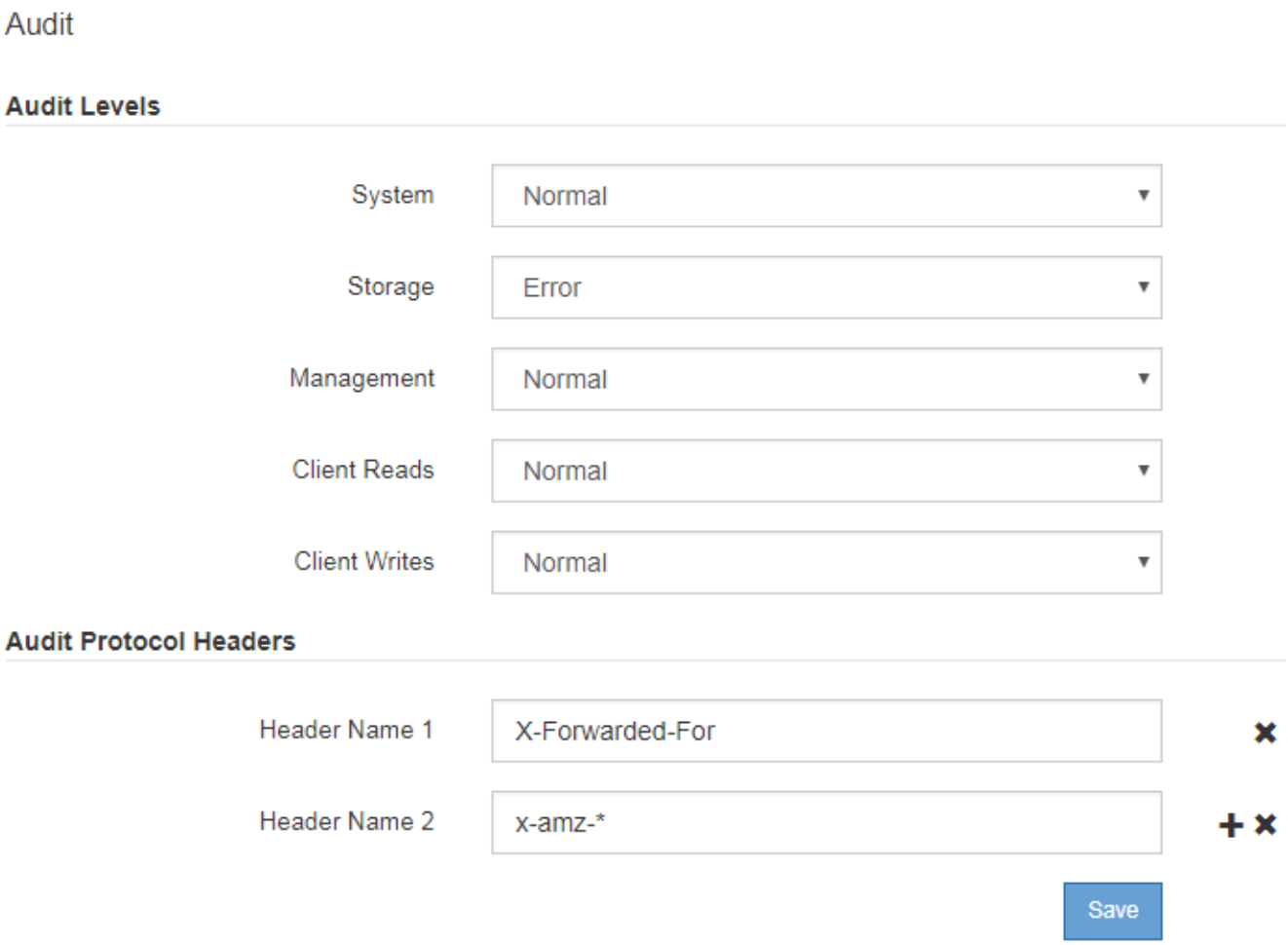
- **Sistema**: Per impostazione predefinita, questo livello è impostato su normale.
- **Storage**: Per impostazione predefinita, questo livello è impostato su Error.
- **Gestione**: Per impostazione predefinita, questo livello è impostato su normale.
- **Letture client**: Per impostazione predefinita, questo livello è impostato su normale.
- **Client Scritture**: Per impostazione predefinita, questo livello è impostato su Normal (normale).

Queste impostazioni predefinite si applicano se StorageGRID è stato installato inizialmente utilizzando la versione 10.3 o successiva. Se è stato eseguito l'aggiornamento da una versione precedente di StorageGRID, l'impostazione predefinita per tutte le categorie è normale.

Durante gli aggiornamenti, le configurazioni a livello di audit non saranno effettive immediatamente.

Fasi

1. Selezionare **Configuration** > **Monitoring** > **Audit**.



2. Per ciascuna categoria di messaggi di audit, selezionare un livello di audit dall'elenco a discesa:

Livello di audit	Descrizione
Spento	Non vengono registrati messaggi di audit della categoria.
Errore	Vengono registrati solo messaggi di errore - messaggi di audit per i quali il codice risultato non è stato "riuscito" (SUCS).
Normale	Vengono registrati i messaggi transazionali standard, ovvero i messaggi elencati in queste istruzioni per la categoria.

Livello di audit	Descrizione
Debug	Obsoleto. Questo livello si comporta come il livello di audit normale.

I messaggi inclusi per qualsiasi livello specifico includono quelli che verrebbero registrati ai livelli superiori. Ad esempio, il livello normale include tutti i messaggi di errore.

3. In **Audit Protocol Headers**, inserire il nome delle intestazioni delle richieste HTTP da includere nei messaggi di controllo lettura client e scrittura client. Utilizzare un asterisco (**) come carattere jolly o la sequenza di escape (**) come asterisco letterale. Fare clic sul segno più per creare un elenco di campi relativi al nome dell'intestazione.

   Le intestazioni dei protocolli di audit si applicano solo alle richieste S3 e Swift.

   Quando tali intestazioni HTTP vengono trovate in una richiesta, vengono incluse nel messaggio di audit nel campo HTRH.

   Le intestazioni delle richieste del protocollo di audit vengono registrate solo se il livello di audit per **letture client** o **scritture client** non è **disattivato**.

4. Fare clic su **Save** (Salva).

Informazioni correlate

"Messaggi di audit del sistema"

"Messaggi di audit dello storage a oggetti"

"Messaggio di audit della gestione"

"Messaggi di audit in lettura del client"

"Amministrare StorageGRID"

Accesso al file di log di audit

La condivisione di audit contiene il attivo `audit.log` file ed eventuali file di log di audit compressi. Per un facile accesso ai log di audit, è possibile configurare l'accesso client per le condivisioni di audit sia per NFS che per CIFS (obsoleto). È inoltre possibile accedere ai file di log di audit direttamente dalla riga di comando del nodo di amministrazione.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`

b. Immettere la password elencata in `Passwords.txt` file.

2. Accedere alla directory contenente i file di log di controllo:

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

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

Informazioni correlate

"Amministrare StorageGRID"

Controllo della rotazione del file di log

I file di log di audit vengono salvati in un nodo di amministrazione `/var/local/audit/export` directory. I file di log di audit attivi sono denominati `audit.log`.

Una volta al giorno, il attivo `audit.log` il file viene salvato e viene visualizzato un nuovo `audit.log` il file viene avviato. Il nome del file salvato indica quando è stato salvato, nel formato *`yyyy-mm-dd.txt`*. Se in un singolo giorno vengono creati più log di audit, i nomi dei file utilizzano la data in cui il file è stato salvato, aggiunto da un numero, nel formato *`yyyy-mm-dd.txt.n`*. Ad esempio, `2018-04-15.txt` e. `2018-04-15.txt.1` Sono il primo e il secondo file di log creati e salvati il 15 aprile 2018.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato *`yyyy-mm-dd.txt.gz`*, che conserva la data originale. Con il passare del tempo, ciò comporta un consumo di storage allocato per i registri di controllo sul nodo di amministrazione. Uno script monitora il consumo di spazio nel registro di controllo ed elimina i file di registro in base alle necessità per liberare spazio in `/var/local/audit/export` directory. I registri di audit vengono cancellati in base alla data di creazione, con la data in cui sono stati cancellati per prima. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

In questo esempio viene visualizzato il valore attivo `audit.log` file del giorno precedente (`2018-04-15.txt`) e il file compresso per il giorno precedente (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.