Configurazione dei client di audit per CIFS

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-115/admin/configuring-audit-clients-for-workgroup.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Configurazione dei client di audit per CIFS . . . 1
Configurazione dei client di audit per Workgroup . . . 1
Configurazione dei client di audit per Active Directory . . . 4
Aggiunta di un utente o di un gruppo a una condivisione di audit CIFS . . . 7
Rimozione di un utente o di un gruppo da una condivisione di audit CIFS . . . 9
Modifica del nome di un utente o di un gruppo di condivisione dell’audit CIFS . . . 11
Verifica dell’integrazione dell’audit CIFS . . . 11

Configurazione dei client di audit per CIFS

La procedura utilizzata per configurare un client di audit dipende dal metodo di autenticazione: Windows Workgroup o Windows Active Directory (ad). Una volta aggiunta, la condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Informazioni correlate

"Aggiornare il software"

Configurazione dei client di audit per Workgroup

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato: `storagegrid-status`

   Se tutti i servizi non sono in esecuzione o verificati, risolvere i problemi prima di continuare.
3. Tornare alla riga di comando, premere **Ctrl+C**.
4. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

```
-------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------------
```

5. Impostare l'autenticazione per Windows Workgroup:

   Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

   a. Inserire: `set-authentication`
   b. Quando viene richiesto di installare Windows Workgroup o Active Directory, immettere: `workgroup`
   c. Quando richiesto, immettere un nome per il gruppo di lavoro: *`workgroup_name`*
   d. Quando richiesto, creare un nome NetBIOS significativo: *`netbios_name`*

      oppure

      Premere **Invio** per utilizzare il nome host del nodo di amministrazione come nome NetBIOS.

   Lo script riavvia il server Samba e le modifiche vengono applicate. Questa operazione dovrebbe richiedere meno di un minuto. Dopo aver impostato l'autenticazione, aggiungere un client di audit.

   a. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

6. Aggiungere un client di audit:

   a. Inserire: `add-audit-share`

      La condivisione viene aggiunta automaticamente in sola lettura.

   b. Quando richiesto, aggiungere un utente o un gruppo: *`user`*
   c. Quando richiesto, inserire il nome utente per l'audit: *`audit_user_name`*
   d. Quando richiesto, inserire una password per l'utente di controllo: *`password`*
   e. Quando richiesto, immettere nuovamente la stessa password per confermarla: *`password`*
   f. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

Non è necessario inserire una directory. Il nome della directory di controllo è predefinito.

7. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere gli utenti aggiuntivi:
   a. Inserire: `add-user-to-share`

      Viene visualizzato un elenco numerato di condivisioni abilitate.

   b. Quando richiesto, inserire il numero della condivisione audit-export: *`share_number`*
   c. Quando richiesto, aggiungere un utente o un gruppo: `user`

      oppure `group`

   d. Quando richiesto, inserire il nome dell'utente o del gruppo di controllo: *`audit_user or audit_group`*
   e. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

   f. Ripetere questi passaggi secondari per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.
8. In alternativa, verificare la configurazione: `validate-config`

   I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

   ```
   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
   (16384)
   ```

   a. Quando richiesto, premere **Invio**.

      Viene visualizzata la configurazione del client di audit.

   b. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.
9. Chiudere l'utilità di configurazione CIFS: `exit`
10. Avviare il servizio Samba: `service smbd start`
11. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

    oppure

    Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare questa condivisione di controllo come richiesto:

a. Accedere in remoto al nodo di amministrazione di un sito:
   i. Immettere il seguente comando: `ssh admin@grid_node_IP`
   ii. Immettere la password elencata in `Passwords.txt` file.
   iii. Immettere il seguente comando per passare a root: `su -`
   iv. Immettere la password elencata in `Passwords.txt` file.
b. Ripetere la procedura per configurare la condivisione di controllo per ogni nodo amministrativo aggiuntivo.
c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`

12. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

"Aggiornare il software"

Configurazione dei client di audit per Active Directory

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre del nome utente e della password di CIFS Active Directory.
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

> L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

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

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato: `storagegrid-status`

   Se tutti i servizi non sono in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando, premere **Ctrl**+**C**.
4. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. Impostare l'autenticazione per Active Directory: `set-authentication`

   Nella maggior parte delle implementazioni, è necessario impostare l'autenticazione prima di aggiungere il client di audit. Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

   a. Quando viene richiesto di installare Workgroup o Active Directory: `ad`
   b. Quando richiesto, inserire il nome del dominio ad (nome di dominio breve).
   c. Quando richiesto, inserire l'indirizzo IP o il nome host DNS del controller di dominio.
   d. Quando richiesto, inserire il nome completo del dominio.

      Utilizzare lettere maiuscole.

   e. Quando viene richiesto di attivare il supporto winbind, digitare **y**.

      Winbind viene utilizzato per risolvere le informazioni di utenti e gruppi dai server ad.

   f. Quando richiesto, inserire il nome NetBIOS.
   g. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

6. Unirsi al dominio:

   a. Se non è già stato avviato, avviare l'utility di configurazione CIFS: `config_cifs.rb`
   b. Unirsi al dominio: `join-domain`
   c. Viene richiesto di verificare se l'Admin Node è attualmente un membro valido del dominio. Se questo nodo di amministrazione non ha precedentemente aderito al dominio, immettere: `no`
   d. Quando richiesto, fornire il nome utente dell'amministratore: *`administrator_username`*

      dove *`administrator_username`* È il nome utente di CIFS Active Directory, non il nome utente di StorageGRID.

   e. Quando richiesto, fornire la password dell'amministratore: *`administrator_password`*

      erano *`administrator_password`* È il nome utente di CIFS Active Directory, non la password di

StorageGRID.

f. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

7. Verificare di aver inserito correttamente il dominio:
   a. Unirsi al dominio: `join-domain`
   b. Quando viene richiesto di verificare se il server è attualmente un membro valido del dominio, immettere: `y`

      Se viene visualizzato il messaggio "Join is OK," significa che l'accesso al dominio è stato eseguito correttamente. Se non si ottiene questa risposta, provare a impostare nuovamente l'autenticazione e ad accedere al dominio.

   c. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

8. Aggiungere un client di audit: `add-audit-share`
   a. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `user`
   b. Quando viene richiesto di inserire il nome utente per l'audit, inserire il nome utente per l'audit.
   c. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

9. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere altri utenti: `add-user-to-share`

   Viene visualizzato un elenco numerato di condivisioni abilitate.

   a. Inserire il numero della condivisione audit-export.
   b. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `group`

      Viene richiesto il nome del gruppo di audit.

   c. Quando viene richiesto il nome del gruppo di audit, immettere il nome del gruppo di utenti di audit.
   d. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

   e. Ripetere questo passaggio per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.

10. In alternativa, verificare la configurazione: `validate-config`

    I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

    - Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
    - Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-filesystem.inc`

- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-custom-config.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-shares.inc`
- Rlimit_max: Aumento di rlimit_max (1024) al limite minimo di Windows (16384)

> Non combinare l'impostazione 'security=ads' con il parametro 'password server'. (Per impostazione predefinita, Samba rileverà automaticamente il DC corretto da contattare).

i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.

ii. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

11. Chiudere l'utilità di configurazione CIFS: `exit`
12. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

    oppure

    Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:

    a. Accedere in remoto al nodo di amministrazione di un sito:
        i. Immettere il seguente comando: `ssh admin@grid_node_IP`
        ii. Immettere la password elencata in `Passwords.txt` file.
        iii. Immettere il seguente comando per passare a root: `su -`
        iv. Immettere la password elencata in `Passwords.txt` file.
    b. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
    c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione: `exit`
13. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

"Aggiornare il software"

Aggiunta di un utente o di un gruppo a una condivisione di audit CIFS

È possibile aggiungere un utente o un gruppo a una condivisione di audit CIFS integrata con l'autenticazione ad.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

La seguente procedura riguarda una condivisione di controllo integrata con l'autenticazione ad.

> L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

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

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato. Inserire: `storagegrid-status`

   Se tutti i servizi non sono in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando, premere **Ctrl+C**.
4. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Iniziare ad aggiungere un utente o un gruppo: `add-user-to-share`

   Viene visualizzato un elenco numerato di condivisioni di controllo configurate.

6. Quando richiesto, inserire il numero per la condivisione dell'audit (audit-export): *`audit_share_number`*

   Viene richiesto se si desidera concedere a un utente o a un gruppo l'accesso a questa condivisione di controllo.

7. Quando richiesto, aggiungere un utente o un gruppo: `user` oppure `group`
8. Quando viene richiesto il nome dell'utente o del gruppo per questa condivisione di audit ad, immettere il nome.

L'utente o il gruppo viene aggiunto in sola lettura per la condivisione di controllo sia nel sistema operativo del server che nel servizio CIFS. La configurazione di Samba viene ricaricata per consentire all'utente o al gruppo di accedere alla condivisione del client di audit.

9. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione CIFS.

10. Ripetere questa procedura per ogni utente o gruppo che ha accesso alla condivisione di controllo.
11. In alternativa, verificare la configurazione: `validate-config`

    I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

    - Impossibile trovare il file include /etc/samba/includes/cifs-interfaces.inc
    - Impossibile trovare il file include /etc/samba/includes/cifs-filesystem.inc
    - Impossibile trovare il file include /etc/samba/includes/cifs-custom-config.inc
    - Impossibile trovare il file include /etc/samba/includes/cifs-shares.inc
      i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.
      ii. Quando richiesto, premere **Invio**.
12. Chiudere l'utilità di configurazione CIFS: `exit`
13. Determinare se è necessario attivare ulteriori condivisioni di audit, come segue:
    - Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.
    - Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:
      i. Accedere in remoto al nodo di amministrazione di un sito:
         A. Immettere il seguente comando: `ssh admin@grid_node_IP`
         B. Immettere la password elencata in `Passwords.txt` file.
         C. Immettere il seguente comando per passare a root: `su -`
         D. Immettere la password elencata in `Passwords.txt` file.
      ii. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
      iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
14. Disconnettersi dalla shell dei comandi: `exit`

Rimozione di un utente o di un gruppo da una condivisione di audit CIFS

Non è possibile rimuovere l'ultimo utente o gruppo autorizzato ad accedere alla condivisione di controllo.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con le password dell'account root (disponibili in DETTO pacchetto).

- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

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

2. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. Iniziare a rimuovere un utente o un gruppo: `remove-user-from-share`

   Viene visualizzato un elenco numerato delle condivisioni di audit disponibili per il nodo di amministrazione. La condivisione dell'audit è etichettata audit-export.

4. Inserire il numero della condivisione di controllo: *`audit_share_number`*
5. Quando viene richiesto di rimuovere un utente o un gruppo: `user` oppure `group`

   Viene visualizzato un elenco numerato di utenti o gruppi per la condivisione dell'audit.

6. Inserire il numero corrispondente all'utente o al gruppo che si desidera rimuovere: *`number`*

   La condivisione di controllo viene aggiornata e l'utente o il gruppo non può più accedere alla condivisione di controllo. Ad esempio:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Chiudere l'utilità di configurazione CIFS: `exit`
8. Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, disattivare la condivisione di controllo in ciascun sito secondo necessità.
9. Disconnettersi da ogni shell dei comandi al termine della configurazione: `exit`

Informazioni correlate

"Aggiornare il software"

Modifica del nome di un utente o di un gruppo di condivisione dell'audit CIFS

È possibile modificare il nome di un utente o di un gruppo per una condivisione di audit CIFS aggiungendo un nuovo utente o gruppo ed eliminando quello precedente.

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Aggiungere un nuovo utente o gruppo con il nome aggiornato alla condivisione di controllo.
2. Eliminare il vecchio nome utente o gruppo.

Informazioni correlate

"Aggiornare il software"

"Aggiunta di un utente o di un gruppo a una condivisione di audit CIFS"

"Rimozione di un utente o di un gruppo da una condivisione di audit CIFS"

Verifica dell'integrazione dell'audit CIFS

La condivisione dell'audit è di sola lettura. I file di log devono essere letti dalle applicazioni del computer e la verifica non include l'apertura di un file. Si ritiene sufficiente

verificare che i file di registro di controllo vengano visualizzati in una finestra di Esplora risorse. Dopo la verifica della connessione, chiudere tutte le finestre.

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.