



Usa il monitoraggio SNMP

StorageGRID software

NetApp
July 23, 2026

Sommario

- Usa il monitoraggio SNMP 1
 - Utilizza il monitoraggio SNMP in StorageGRID 1
 - Capacità 1
 - Supporto versioni SNMP 2
 - Limitazioni 2
 - Configura l'agente SNMP in StorageGRID 2
 - Specifica la configurazione di base 3
 - Inserisci le stringhe della community 3
 - Crea destinazioni trap 4
 - Crea indirizzi agente 6
 - Crea utenti USM 7
 - Aggiorna l'agente SNMP di StorageGRID 9
- Accedere ai file MIB di StorageGRID 11
 - Accedi ai file MIB 11
 - Contenuto del file MIB 11
 - oggetti MIB 12

Usa il monitoraggio SNMP

Utilizza il monitoraggio SNMP in StorageGRID

Se vuoi monitorare StorageGRID utilizzando il Simple Network Management Protocol (SNMP), devi configurare l'agente SNMP incluso in StorageGRID.

- ["Configura l'agente SNMP"](#)
- ["Aggiorna l'agente SNMP"](#)

Capacità

Ogni nodo StorageGRID esegue un agente SNMP, o demone, che fornisce una MIB. La MIB di StorageGRID contiene le definizioni di tabelle e notifiche per gli avvisi. La MIB contiene anche informazioni di descrizione del sistema, come la piattaforma e il numero di modello per ciascun nodo. Ogni nodo StorageGRID supporta inoltre un sottoinsieme di oggetti MIB-II.



Vedi ["Accedi ai file MIB"](#) se vuoi scaricare i file MIB sui nodi della tua griglia.

Inizialmente, SNMP è disabilitato su tutti i nodi. Quando configuri l'agente SNMP, tutti i nodi StorageGRID ricevono la stessa configurazione.

L'agente SNMP di StorageGRID supporta tutte e tre le versioni del protocollo SNMP. Fornisce accesso MIB in sola lettura per le query e può inviare due tipi di notifiche basate su eventi a un sistema di gestione:

Trappole

Le trap sono notifiche inviate dall'agente SNMP che non richiedono una conferma da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che è successo qualcosa all'interno di StorageGRID, come ad esempio l'attivazione di un avviso.

Le trap sono supportate in tutte e tre le versioni di SNMP.

Informa

Gli inform sono simili ai trap, ma richiedono una conferma da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, reinvia l'inform finché non riceve una conferma o viene raggiunto il valore massimo di tentativi.

Gli inform sono supportati in SNMPv2c e SNMPv3.

Le notifiche di intercettazione e informazione vengono inviate nei seguenti casi:

- Un avviso predefinito o personalizzato viene attivato a qualsiasi livello di gravità. Per sopprimere le notifiche SNMP per un avviso, devi ["configura un silenzio"](#) per l'avviso. Le notifiche di avviso vengono inviate dal ["Nodo amministratore mittente preferito"](#).

Ogni avviso è mappato a uno dei tre tipi di trap in base al livello di gravità dell'avviso: activeMinorAlert, activeMajorAlert e activeCriticalAlert. Per un elenco degli avvisi che possono attivare queste trap, vedi il ["Riferimento agli avvisi"](#).

Supporto versioni SNMP

La tabella fornisce un riepilogo high-level di ciò che è supportato per ciascuna versione di SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Query (GET e GETNEXT)	Query MIB di sola lettura	Query MIB di sola lettura	Query MIB di sola lettura
Autenticazione della query	Stringa community	Stringa community	Utente del modello di sicurezza basato sull'utente (USM)
Notifiche (TRAP e INFORM)	Solo trap	Trappole e informa	Trappole e informa
Autenticazione della notifica	Comunità di trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Comunità di trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Utente USM per ogni destinazione trap

Limitazioni

- StorageGRID supporta l'accesso MIB in sola lettura. L'accesso in lettura e scrittura non è supportato.
- Tutti i nodi della grid ricevono la stessa configurazione.
- SNMPv3: StorageGRID non supporta il Transport Support Mode (TSM).
- SNMPv3: L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).
- SNMPv3: L'unico protocollo di privacy supportato è AES.

Configura l'agente SNMP in StorageGRID

Puoi configurare l'agente SNMP di StorageGRID per utilizzare un sistema di gestione SNMP di terze parti per l'accesso MIB in sola lettura e le notifiche.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["Permesso di accesso root"](#).

Informazioni su questa attività

L'agente SNMP di StorageGRID supporta SNMPv1, SNMPv2c e SNMPv3. Puoi configurare l'agente per una o più versioni. Per SNMPv3, è supportata solo l'autenticazione User Security Model (USM).

Tutti i nodi della griglia utilizzano la stessa configurazione SNMP.

Specifica la configurazione di base

Come primo passo, abilita l'agente SNMP di StorageGRID e fornisci le informazioni di base.

Passaggi

1. Seleziona **Configurazione > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina dell'agente SNMP.

2. Per abilitare l'agente SNMP su tutti i nodi della griglia, seleziona la casella di controllo **Abilita SNMP**.
3. Inserisci le seguenti informazioni nella sezione Configurazione di base.

Campo	Descrizione
Contatto di sistema	Opzionale. Il contatto principale per il sistema StorageGRID, che viene restituito nei messaggi SNMP come sysContact. Il contatto di sistema è in genere un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID. System contact può contenere un massimo di 255 caratteri.
Posizione del sistema	Opzionale. La posizione del sistema StorageGRID, che viene restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere qualsiasi informazione utile per identificare dove si trova il tuo sistema StorageGRID. Ad esempio, puoi usare l'indirizzo della struttura. Questo valore si applica a tutti i nodi del sistema StorageGRID. System location può essere lungo al massimo 255 caratteri.
Abilita le notifiche dell'agente SNMP	• Se selezionato, l'agente SNMP di StorageGRID invia notifiche trap e inform. • Se non selezionato, l'agente SNMP supporta l'accesso MIB in sola lettura, ma non invia alcuna notifica SNMP.
Abilita le trap di autenticazione	Se selezioni questa opzione, l'agente SNMP di StorageGRID invia trap di autenticazione se riceve messaggi di protocollo non autenticati correttamente.

Inserisci le stringhe della community

Se usi SNMPv1 o SNMPv2c, completa la sezione delle stringhe della community.

Quando il sistema di gestione interroga la MIB di StorageGRID, invia una stringa di comunità. Se la stringa di comunità corrisponde a uno dei valori specificati qui, l'agente SNMP invia una risposta al sistema di gestione.

Passaggi

1. Per la **community di sola lettura**, puoi inserire facoltativamente una stringa di community per consentire l'accesso MIB in sola lettura agli indirizzi agente IPv4 e IPv6.



Per garantire la sicurezza del tuo sistema StorageGRID, non usare "public" come stringa di comunità. Se lasci questo campo vuoto, l'agente SNMP usa l'ID grid del tuo sistema StorageGRID come stringa di comunità.

Ogni stringa di comunità può contenere un massimo di 32 caratteri e non può contenere caratteri di spazio.

2. Seleziona **Aggiungi un'altra stringa della community** per aggiungere altre stringhe.

Sono consentite fino a cinque stringhe.

Crea destinazioni trap

Utilizza la scheda Destinazioni trap nella sezione Altre configurazioni per definire una o più destinazioni per le notifiche trap o inform di StorageGRID. Quando abiliti l'agente SNMP e selezioni **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inviate anche notifiche standard per le entità MIB-II supportate (ad esempio, ifDown e coldStart).

Passaggi

1. Per il campo **Community trap predefinita**, inserisci facoltativamente la stringa community predefinita che vuoi usare per le destinazioni trap SNMPv1 o SNMPv2.

Se necessario, puoi fornire una stringa di comunità diversa ("personalizzata") quando definisci una destinazione trap specifica.

La **trap community predefinita** può essere lunga al massimo 32 caratteri e non può contenere spazi.

2. Per aggiungere una destinazione trap, seleziona **Crea**.
3. Seleziona quale versione SNMP verrà utilizzata per questa destinazione trap.
4. Completa il modulo Crea destinazione trap per la versione che hai selezionato.

SNMPv1

Se hai selezionato SNMPv1 come versione, compila questi campi.

Campo	Descrizione
Tipo	Deve essere Trap per SNMPv1.
Host	Un indirizzo IPv4 o IPv6 oppure un domain name (FQDN) per ricevere la trap.
Porta	Utilizza 162, che è la porta standard per le trap SNMP, a meno che tu non debba utilizzare un valore diverso.
Protocollo	Utilizza UDP, che è il protocollo standard SNMP trap, a meno che tu non debba utilizzare TCP.
Stringa community	Utilizza la community di trap predefinita, se ne è stata specificata una, oppure inserisci una stringa di community personalizzata per questa destinazione di trap. La stringa della community personalizzata può essere lunga al massimo 32 caratteri e non può contenere spazi.

SNMPv2c

Se hai selezionato SNMPv2c come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o inform.
Host	Un indirizzo IPv4 o IPv6 oppure un FQDN per ricevere la trap.
Porta	Utilizza la 162, che è la porta standard per le trap SNMP, a meno che tu non debba usare un altro valore.
Protocollo	Utilizza UDP, che è il protocollo standard SNMP trap, a meno che tu non debba utilizzare TCP.
Stringa community	Utilizza la community di trap predefinita, se ne è stata specificata una, oppure inserisci una stringa di community personalizzata per questa destinazione di trap. La stringa della community personalizzata può essere lunga al massimo 32 caratteri e non può contenere spazi.

SNMPv3

Se hai selezionato SNMPv3 come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o inform.
Host	Un indirizzo IPv4 o IPv6 oppure un FQDN per ricevere la trap.
Porta	Utilizza la 162, che è la porta standard per le trap SNMP, a meno che tu non debba usare un altro valore.
Protocollo	Utilizza UDP, che è il protocollo standard SNMP trap, a meno che tu non debba utilizzare TCP.
utente USM	L'utente USM che userai per l'autenticazione. • Se hai selezionato Trap, vengono mostrati solo gli utenti USM senza ID motore autorevoli. • Se hai selezionato Inform, vengono mostrati solo gli utenti USM con engine ID autorevoli. • Se non vengono visualizzati utenti: i. Crea e salva la destinazione trap. ii. Vai su Crea utenti USM e crea l'utente. iii. Torna alla scheda Destinazioni Trap, seleziona la destinazione salvata dalla tabella e seleziona Modifica. iv. Seleziona l'utente.

5. Seleziona **Create**.

La destinazione trap viene creata e aggiunta alla tabella.

Crea indirizzi agente

Facoltativamente, usa la scheda Indirizzi agente nella sezione Altre configurazioni per specificare uno o più "indirizzi di ascolto". Questi sono gli indirizzi StorageGRID su cui l'agente SNMP può ricevere le query.

Se non configuri un indirizzo agente, l'indirizzo di ascolto predefinito è la porta UDP 161 su tutte le reti StorageGRID.

Passaggi

1. Seleziona **Create**.
2. Inserisci le seguenti informazioni.

Campo	Descrizione
Protocollo Internet	Indica se questo indirizzo utilizzerà IPv4 o IPv6. Per impostazione predefinita, SNMP utilizza IPv4.

Campo	Descrizione
Protocollo di trasporto	Se questo indirizzo utilizzerà UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
rete StorageGRID	Su quale rete StorageGRID l'agente rimarrà in ascolto. • Reti Grid, Admin e Client: l'agente SNMP ascolterà le query su tutte e tre le reti. • \${post_edited_translations.segment} • Rete di amministrazione • \${post_edited_translations.segment} Nota: Se usi la rete client per dati non protetti e crei un indirizzo agente per la rete client, sappi che anche il traffico SNMP sarà non protetto.
Porta	Facoltativamente, il numero di porta su cui l'agente SNMP deve ascoltare. La porta UDP predefinita per un agente SNMP è 161, ma puoi inserire qualsiasi numero di porta non utilizzato. Nota: Quando salvi l'agente SNMP, StorageGRID apre automaticamente le porte dell'indirizzo dell'agente sul firewall interno. Devi assicurarti che eventuali firewall esterni consentano l'accesso a queste porte.

3. Seleziona **Create**.

L'indirizzo dell'agente viene creato e aggiunto alla tabella.

Crea utenti USM

Se usi SNMPv3, usa la scheda Utenti USM nella sezione Altre configurazioni per definire gli utenti USM autorizzati a interrogare la MIB o a ricevere trap e inform.



Per le destinazioni SNMPv3 *trap*, si consiglia di creare un utente USM per ogni Admin Node. Se ogni Admin Node non dispone di un utente USM, il sistema di gestione potrebbe smettere di ricevere notifiche se il primary Admin Node va giù.



Le destinazioni SNMPv3 *inform* devono avere utenti con ID motore. Le destinazioni SNMPv3 *trap* non possono avere utenti con ID motore.

Questi passaggi non si applicano se usi solo SNMPv1 o SNMPv2c.

Passaggi

1. Seleziona **Create**.

2. Inserisci le seguenti informazioni.

Campo	Descrizione
Nome utente	Un nome univoco per questo utente USM. I nomi utente possono avere una lunghezza massima di 32 caratteri e non possono contenere spazi. Il nome utente non può essere modificato dopo la creazione dell'utente.
Accesso MIB in sola lettura	Se selezionato, questo utente dovrebbe avere accesso in sola lettura alla MIB.
ID motore autorevole	Se userai questo utente in una destinazione inform, l'ID del motore autorevole per questo utente. Inserisci da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è obbligatorio per gli utenti USM che verranno selezionati come destinazione delle trap per gli inform. Questo valore non è consentito per gli utenti USM che verranno selezionati come destinazione delle trap per le trap. Nota: Questo campo non viene visualizzato se hai selezionato Accesso MIB in sola lettura perché gli utenti USM con accesso MIB in sola lettura non possono avere engine ID.
Livello di sicurezza	Livello di sicurezza per l'utente USM: • authPriv: Questo utente comunica tramite autenticazione e privacy (crittografia). Devi specificare un protocollo di autenticazione e una password e un protocollo di privacy e una password. • authNoPriv: Questo utente comunica con autenticazione e senza riservatezza (nessuna crittografia). Devi specificare un protocollo di autenticazione e una password.
Protocollo di autenticazione	Imposta sempre su SHA, che è l'unico protocollo supportato (HMAC-SHA-96).
Password	La password che questo utente userà per l'autenticazione.
Protocollo sulla privacy	Mostrato solo se hai selezionato authPriv e sempre impostato su AES, che è l'unico protocollo di privacy supportato.
Password	Mostrato solo se hai selezionato authPriv. La password che questo utente utilizzerà per la privacy.

3. Seleziona **Create**.

L'utente USM viene creato e aggiunto alla tabella.

4. Quando hai completato la configurazione dell'agente SNMP, seleziona **Salva**.

La nuova configurazione dell'agente SNMP diventa attiva.

Aggiorna l'agente SNMP di StorageGRID

Puoi disabilitare le notifiche SNMP, aggiornare le stringhe di comunità o aggiungere o rimuovere indirizzi agente, utenti USM e destinazioni trap.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["Permesso di accesso root"](#).

Informazioni su questa attività

Vedi ["Configura l'agente SNMP"](#) per i dettagli su ciascun campo nella pagina dell'agente SNMP. Devi selezionare **Salva** in fondo alla pagina per confermare qualsiasi modifica apportata in ciascuna scheda.

Passaggi

1. Seleziona **Configurazione > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina dell'agente SNMP.

2. Per disabilitare l'agente SNMP su tutti i nodi della griglia, deseleziona la casella di controllo **Abilita SNMP** e seleziona **Salva**.

Se riattivi l'agente SNMP, le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Facoltativamente, aggiorna le informazioni nella sezione Configurazione di base:
 - a. Se necessario, aggiorna il **contatto di sistema** e la **posizione del sistema**.
 - b. Facoltativamente, seleziona o deseleziona la casella di controllo **Abilita notifiche agente SNMP** per controllare se l'agente SNMP di StorageGRID invia notifiche trap e inform.

Quando questa casella di controllo non è selezionata, l'agente SNMP supporta l'accesso MIB in sola lettura, ma non invia notifiche SNMP.

- c. Facoltativamente, seleziona o deseleziona la casella di controllo **Abilita trap di autenticazione** per controllare se l'agente SNMP di StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo non autenticati correttamente.
4. Se usi SNMPv1 o SNMPv2c, puoi aggiornare o aggiungere una **community di sola lettura** nella sezione Stringhe della community.
 5. Per aggiornare le destinazioni trap, seleziona la scheda Destinazioni trap nella sezione Altre configurazioni.

Utilizza questa scheda per definire una o più destinazioni per le notifiche trap o inform di StorageGRID. Quando abiliti l'agente SNMP e selezioni **Salva**, StorageGRID invia notifiche a ciascuna destinazione quando vengono attivati gli avvisi. Vengono inviate anche notifiche standard per le entità MIB-II supportate (ad esempio, ifDown e coldStart).

Per i dettagli su cosa inserire, vedi ["Crea destinazioni trap"](#).

- Facoltativamente, aggiorna o rimuovi la trap community predefinita.

Se rimuovi la community predefinita per le trap, devi prima assicurarti che tutte le destinazioni delle trap esistenti utilizzino una stringa di community personalizzata.

- Per aggiungere una destinazione trap, seleziona **Crea**.
- Per modificare una destinazione trap, seleziona il pulsante di opzione e seleziona **Modifica**.
- Per rimuovere una destinazione trap, seleziona il pulsante di opzione e seleziona **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

6. Per aggiornare gli indirizzi degli agenti, seleziona la scheda Indirizzi degli agenti nella sezione Altre configurazioni.

Utilizza questa scheda per specificare uno o più "indirizzi di ascolto". Questi sono gli indirizzi StorageGRID sui quali l'agente SNMP può ricevere query.

Per i dettagli su cosa inserire, vedi "[Crea indirizzi agente](#)".

- Per aggiungere un indirizzo agente, seleziona **Crea**.
- Per modificare l'indirizzo di un agente, seleziona il pulsante di opzione e seleziona **Modifica**.
- Per rimuovere un indirizzo agente, seleziona il pulsante di opzione e seleziona **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

7. Per aggiornare gli utenti USM, seleziona la scheda Utenti USM nella sezione Altre configurazioni.

Usa questa scheda per definire gli utenti USM autorizzati a interrogare la MIB o a ricevere trap e inform.

Per i dettagli su cosa inserire, vedi "[Crea utenti USM](#)".

- Per aggiungere un utente USM, seleziona **Crea**.
- Per modificare un utente USM, seleziona il pulsante di opzione e seleziona **Modifica**.

Il nome utente di un utente USM esistente non può essere cambiato. Se devi cambiare un nome utente, devi rimuovere l'utente e crearne uno nuovo.



Se aggiungi o rimuovi l'ID motore autorevole di un utente e quell'utente è attualmente selezionato per una destinazione, devi modificare o rimuovere la destinazione. Altrimenti, si verifica un errore di convalida quando salvi la configurazione dell'agente SNMP.

- Per rimuovere un utente USM, seleziona il pulsante di opzione e seleziona **Rimuovi**.



Se l'utente che hai rimosso è attualmente selezionato per una destinazione trap, devi modificare o rimuovere la destinazione. Altrimenti, si verifica un errore di convalida quando salvi la configurazione dell'agente SNMP.

- Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

8. Quando hai aggiornato la configurazione dell'agente SNMP, seleziona **Salva**.

Accedere ai file MIB di StorageGRID

I file MIB contengono definizioni e informazioni sulle proprietà delle risorse e dei servizi gestiti per i nodi della tua griglia. Puoi accedere ai file MIB che definiscono gli oggetti e le notifiche per StorageGRID. Questi file possono essere utili per monitorare la tua griglia.

Vedi ["Usa il monitoraggio SNMP"](#) per ulteriori informazioni su SNMP e sui file MIB.

Accedi ai file MIB

Segui questi passaggi per accedere ai file MIB.

Passaggi

1. Seleziona **Configurazione > Monitoraggio > Agente SNMP**.
2. Nella pagina dell'agente SNMP, seleziona il file che vuoi scaricare:
 - **NETAPP-STORAGEGRID-MIB.txt**: Definisce la tabella degli avvisi e le notifiche (trap) accessibili su tutti i nodi di amministrazione.
 - **ES-NETAPP-06-MIB.mib**: Definisce oggetti e notifiche per appliance basati su E-Series.
 - **MIB_1_10.zip**: Definisce oggetti e notifiche per dispositivi con interfaccia BMC.



Puoi anche accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID di StorageGRID dal file MIB:

- a. Ottieni l'OID della radice della MIB di StorageGRID:

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Risultato: `.1.3.6.1.4.1.789.28669` (28669 è sempre l'OID per StorageGRID)

- b. Cerca l'OID di StorageGRID nell'intero albero (utilizzando `paste` per unire le righe):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



Il comando `snmptranslate` offre molte opzioni utili per esplorare la MIB. Questo comando è disponibile su qualsiasi nodo StorageGRID.

Contenuto del file MIB

Tutti gli oggetti sono sotto l'OID di StorageGRID.

Nome oggetto	ID oggetto (OID)	Descrizione
		Il modulo MIB per le entità NetApp StorageGRID.

oggetti MIB

Nome oggetto	ID oggetto (OID)	Tipo	Accesso	Modulo MIB	Descrizione
activeAlertCount		Integer32	Sola lettura	NETAPP-STORAGEGR ID-MIB	Il numero di avvisi attivi nella activeAlertTable.
activeAlertTable		Sequenza di ActiveAlertEntry	Non accessibile	NETAPP-STORAGEGR ID-MIB	Una tabella degli avvisi attivi in StorageGRID.
activeAlertEntry		Sequenza	Non accessibile	NETAPP-STORAGEGR ID-MIB	Un singolo avviso StorageGRID, indicizzato tramite ID avviso.
activeAlertId		stringa di ottetto	Sola lettura	NETAPP-STORAGEGR ID-MIB	L'ID dell'avviso. Univoco solo nell'insieme corrente di avvisi attivi.
activeAlertName		stringa di ottetto	Sola lettura	NETAPP-STORAGEGR ID-MIB	Il nome dell'allerta.
activeAlertInstance		stringa di ottetto	Sola lettura	NETAPP-STORAGEGR ID-MIB	Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
activeAlertSeverity		stringa di ottetto	Sola lettura	NETAPP-STORAGEGR ID-MIB	La gravità dell'allerta.
activeAlertStartTime		Data e ora	Sola lettura	NETAPP-STORAGEGR ID-MIB	L'ora in cui è scattato l'allarme.

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.