Utilizzo del monitoraggio SNMP

StorageGRID

NetApp
October 03, 2025

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

Sommario

Utilizzo del monitoraggio SNMP

Se si desidera monitorare StorageGRID utilizzando il protocollo SNMP (Simple Network Management Protocol), è necessario configurare l'agente SNMP incluso in StorageGRID.

- "Configurazione dell'agente SNMP"
- "Aggiornamento dell'agente SNMP"

Funzionalità

Ogni nodo StorageGRID esegue un agente SNMP, o daemon, che fornisce una base di informazioni di gestione (MIB). Il MIB StorageGRID contiene definizioni di tabella e notifica per avvisi e allarmi. Il MIB contiene anche informazioni sulla descrizione del sistema, come il numero di piattaforma e il numero di modello per ciascun nodo. Ogni nodo StorageGRID supporta anche un sottoinsieme di oggetti MIB-II.

Inizialmente, SNMP viene disattivato su tutti i nodi. Quando si configura l'agente SNMP, tutti i nodi StorageGRID ricevono la stessa configurazione.

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

- **Trap** sono notifiche inviate dall'agente SNMP che non richiedono un riconoscimento da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che si è verificato qualcosa all'interno di StorageGRID, ad esempio un avviso attivato.

  I trap sono supportati in tutte e tre le versioni di SNMP.

- Le informazioni * sono simili alle trap, ma richiedono un riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, invia nuovamente l'informazione fino a quando non viene ricevuta una conferma o non viene raggiunto il valore massimo di ripetizione.

  Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche trap e inform vengono inviate nei seguenti casi:

- Viene attivato un avviso predefinito o personalizzato a qualsiasi livello di severità. Per eliminare le notifiche SNMP per un avviso, è necessario configurare un silenzio per l'avviso. Le notifiche di avviso vengono inviate da qualsiasi nodo amministrativo configurato come mittente preferito.
- Alcuni allarmi (sistema legacy) vengono attivati a livelli di severità specificati o superiori.

> Le notifiche SNMP non vengono inviate per ogni allarme o per ogni severità di allarme.

Supporto della versione SNMP

La tabella fornisce un riepilogo generale dei contenuti supportati per ciascuna versione SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Query	Query MIB di sola lettura	Query MIB di sola lettura	Query MIB di sola lettura
Autenticazione delle query	Stringa di comunità	Stringa di comunità	Utente del modello di sicurezza basato sull'utente (USM)
Notifiche	Solo trap	Trap e informa	Trap e informa
Autenticazione delle notifiche	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Utente USM per ciascuna destinazione trap

Limitazioni

- StorageGRID supporta l'accesso MIB di sola lettura. L'accesso in lettura/scrittura non è supportato.
- Tutti i nodi della griglia ricevono la stessa configurazione.
- SNMPv3: StorageGRID non supporta la modalità di supporto per il trasporto (TSM).
- SNMPv3: L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).
- SNMPv3: L'unico protocollo per la privacy supportato è AES.

Accesso al MIB

È possibile accedere al file di definizione MIB nella seguente posizione su qualsiasi nodo StorageGRID:

/Usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt

Informazioni correlate

"Riferimenti agli avvisi"

"Riferimento allarmi (sistema legacy)"

"Allarmi che generano notifiche SNMP (sistema legacy)"

"Tacitare le notifiche di avviso"

Configurazione dell'agente SNMP

È possibile configurare l'agente SNMP StorageGRID se si desidera utilizzare un sistema di gestione SNMP di terze parti per l'accesso MIB di sola lettura e le notifiche.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

L'agente SNMP StorageGRID supporta tutte e tre le versioni del protocollo SNMP. È possibile configurare l'agente per una o più versioni.

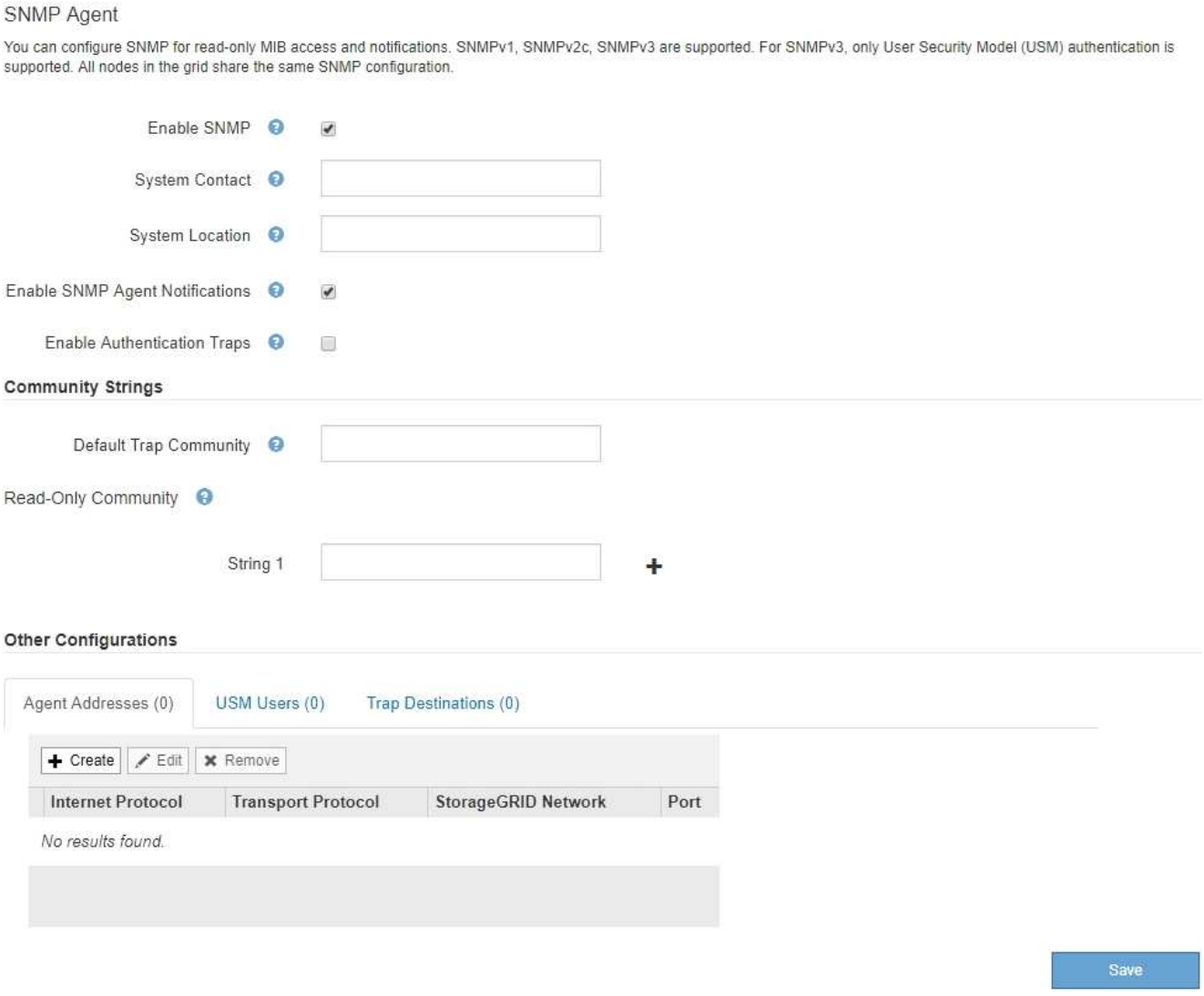
Fasi

1. Selezionare **Configuration Monitoring SNMP Agent**.

   Viene visualizzata la pagina SNMP Agent.

2. Per attivare l'agente SNMP su tutti i nodi della griglia, selezionare la casella di controllo **Enable SNMP** (attiva SNMP).

   Vengono visualizzati i campi per la configurazione di un agente SNMP.



3. Nel campo **contatto di sistema**, immettere il valore che StorageGRID deve fornire nei messaggi SNMP per sysContact.

   Il contatto di sistema in genere è un indirizzo e-mail. Il valore fornito si applica a tutti i nodi nel sistema StorageGRID. **Il campo System Contact** può contenere al massimo 255 caratteri.

4. Nel campo **posizione sistema**, immettere il valore che si desidera che StorageGRID fornisca nei messaggi SNMP per sysLocation.

   La posizione del sistema può essere qualsiasi informazione utile per identificare la posizione del sistema StorageGRID. Ad esempio, è possibile utilizzare l'indirizzo di una struttura. Il valore fornito si applica a tutti i nodi nel sistema StorageGRID. **System Location** può contenere un massimo di 255 caratteri.

5. Mantenere selezionata la casella di controllo **attiva notifiche agente SNMP** se si desidera che l'agente SNMP StorageGRID invii messaggi trap e avvisi.

   Se questa casella di controllo non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.

6. Selezionare la casella di controllo **attiva trap di autenticazione** se si desidera che l'agente SNMP di StorageGRID invii una trap di autenticazione se riceve un messaggio di protocollo autenticato in modo errato.
7. Se si utilizza SNMPv1 o SNMPv2c, completare la sezione Community Strings.

   I campi di questa sezione vengono utilizzati per l'autenticazione basata sulla community in SNMPv1 o SNMPv2c. Questi campi non si applicano a SNMPv3.

   a. Nel campo **Default Trap Community** (Comunità trap predefinita), immettere facoltativamente la stringa di comunità predefinita che si desidera utilizzare per le destinazioni trap.

      Se necessario, è possibile fornire una stringa di community diversa ("custom") definire una destinazione trap specifica.

      Default Trap Community può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

   b. Per **Read-only Community**, immettere una o più stringhe di comunità per consentire l'accesso MIB di sola lettura sugli indirizzi degli agenti IPv4 e IPv6. Fare clic sul segno più ➕ per aggiungere più stringhe.

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

      Ogni stringa di comunità può contenere un massimo di 32 caratteri e non può contenere spazi vuoti. Sono consentite fino a cinque stringhe.

      > ⓘ Per garantire la sicurezza del sistema StorageGRID, non utilizzare "public" come stringa di community. Se non si immette una stringa di comunità, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa di comunità.

8. Facoltativamente, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

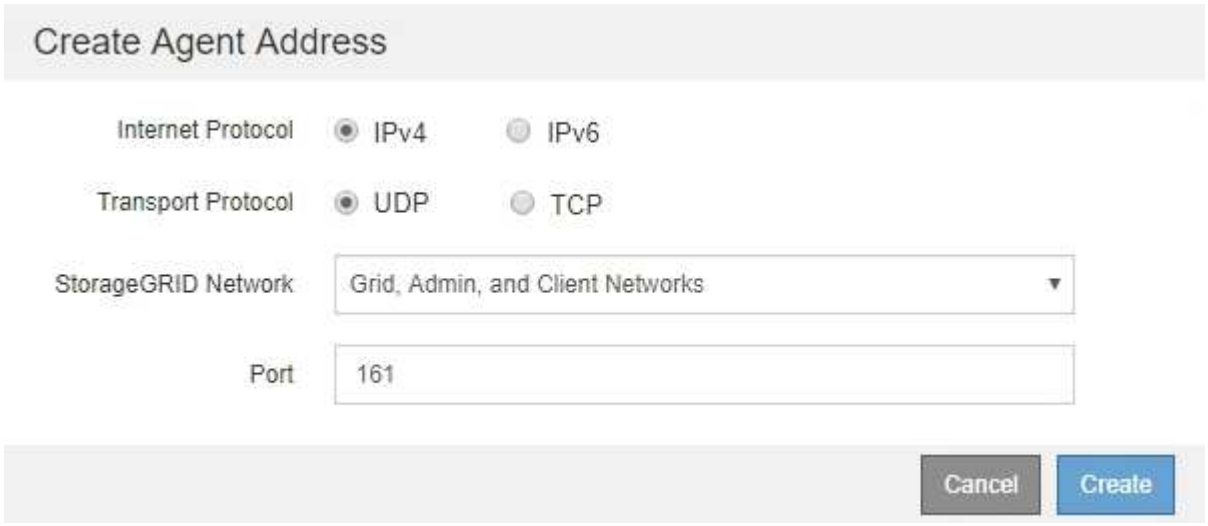
   Utilizzare questa scheda per specificare uno o più "indirizzi in attesa". Questi sono gli indirizzi StorageGRID sui quali l'agente SNMP può ricevere le query. Ogni indirizzo dell'agente include un

protocollo Internet, un protocollo di trasporto, una rete StorageGRID e, facoltativamente, una porta.

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

a. Fare clic su **Create** (Crea).

   Viene visualizzata la finestra di dialogo Create Agent Address (Crea indirizzo agente).



b. Per **Internet Protocol**, selezionare se questo indirizzo utilizzerà IPv4 o IPv6.

   Per impostazione predefinita, SNMP utilizza IPv4.

c. Per **Transport Protocol**, selezionare se questo indirizzo utilizzerà UDP o TCP.

   Per impostazione predefinita, SNMP utilizza UDP.

d. Nel campo **rete StorageGRID**, selezionare la rete StorageGRID su cui si desidera ricevere la query.

   - Reti griglia, amministratore e client: StorageGRID deve rimanere in attesa delle query SNMP su tutte e tre le reti.
   - Grid Network
   - Admin Network (rete amministrativa)
   - Rete client

   > Per garantire che le comunicazioni client con StorageGRID rimangano sicure, non creare un indirizzo agente per la rete client.

e. Nel campo **Port** (porta), immettere il numero di porta su cui l'agente SNMP deve rimanere in attesa.

   La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta inutilizzato.

   > Quando si salva l'agente SNMP, StorageGRID apre automaticamente le porte degli indirizzi dell'agente sul firewall interno. È necessario assicurarsi che tutti i firewall esterni consentano l'accesso a queste porte.

f. Fare clic su **Create** (Crea).

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

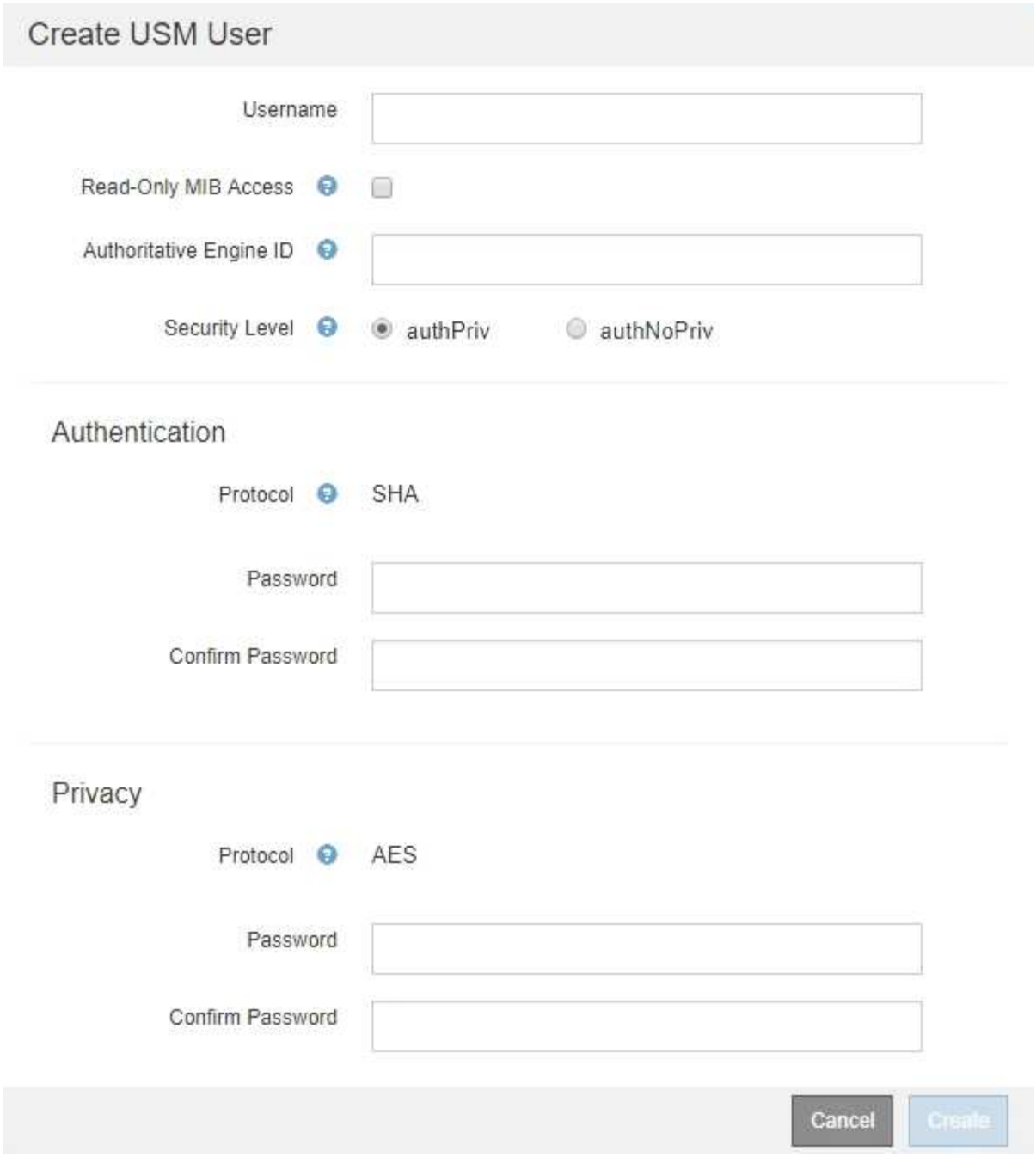
9. Se si utilizza SNMPv3, selezionare la scheda utenti USM nella sezione altre configurazioni.

Utilizzare questa scheda per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

Questo passaggio non è valido se si utilizza solo SNMPv1 o SNMPv2c.

a. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Create USM User (Crea utente USM).



b. Immettere un **Username** univoco per questo utente USM.

   I nomi utente hanno un massimo di 32 caratteri e non possono contenere spazi vuoti. Il nome utente non può essere modificato dopo la creazione dell'utente.

c. Selezionare la casella di controllo **Read-only MIB Access** (accesso MIB di sola lettura) se l'utente deve disporre dell'accesso di sola lettura al MIB.

   Se si seleziona **Read-only MIB Access** (accesso MIB di sola lettura), il campo **Authoritative Engine ID** (ID motore autorevole) viene disattivato.

   Gli utenti USM con accesso MIB di sola lettura non possono disporre di ID motore.

d. Se questo utente verrà utilizzato in una destinazione di tipo inform, immettere il **Authoritative Engine**

ID per questo utente.

> Le destinazioni SNMPv3 inform devono avere utenti con ID motore. La destinazione della trap SNMPv3 non può avere utenti con ID motore.

L'ID del motore autorevole può essere compreso tra 5 e 32 byte in formato esadecimale.

e. Selezionare un livello di sicurezza per l'utente USM.
   - **Authprim**: Questo utente comunica con autenticazione e privacy (crittografia). È necessario specificare un protocollo di autenticazione e una password, nonché un protocollo e una password per la privacy.
   - **AuthNoPriv**: Questo utente comunica con autenticazione e senza privacy (senza crittografia). Specificare un protocollo di autenticazione e una password.
f. Inserire e confermare la password che verrà utilizzata dall'utente per l'autenticazione.

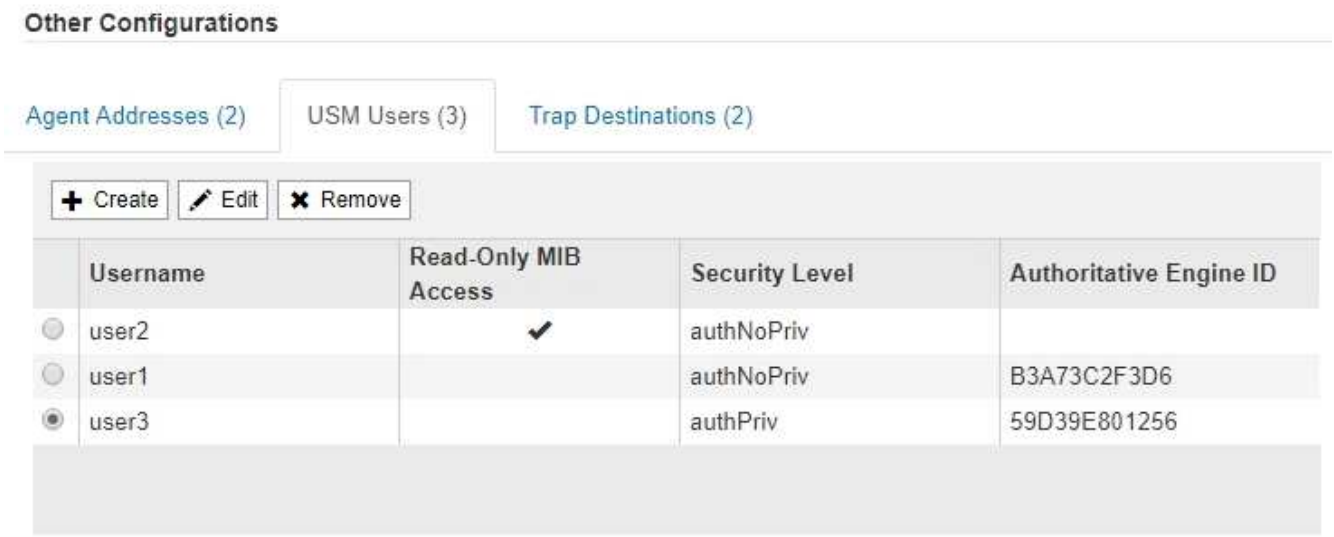
> L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).

g. Se si seleziona **authprim**, immettere e confermare la password che verrà utilizzata dall'utente per la privacy.

> L'unico protocollo per la privacy supportato è AES.

h. Fare clic su **Create** (Crea).

L'utente USM viene creato e aggiunto alla tabella.

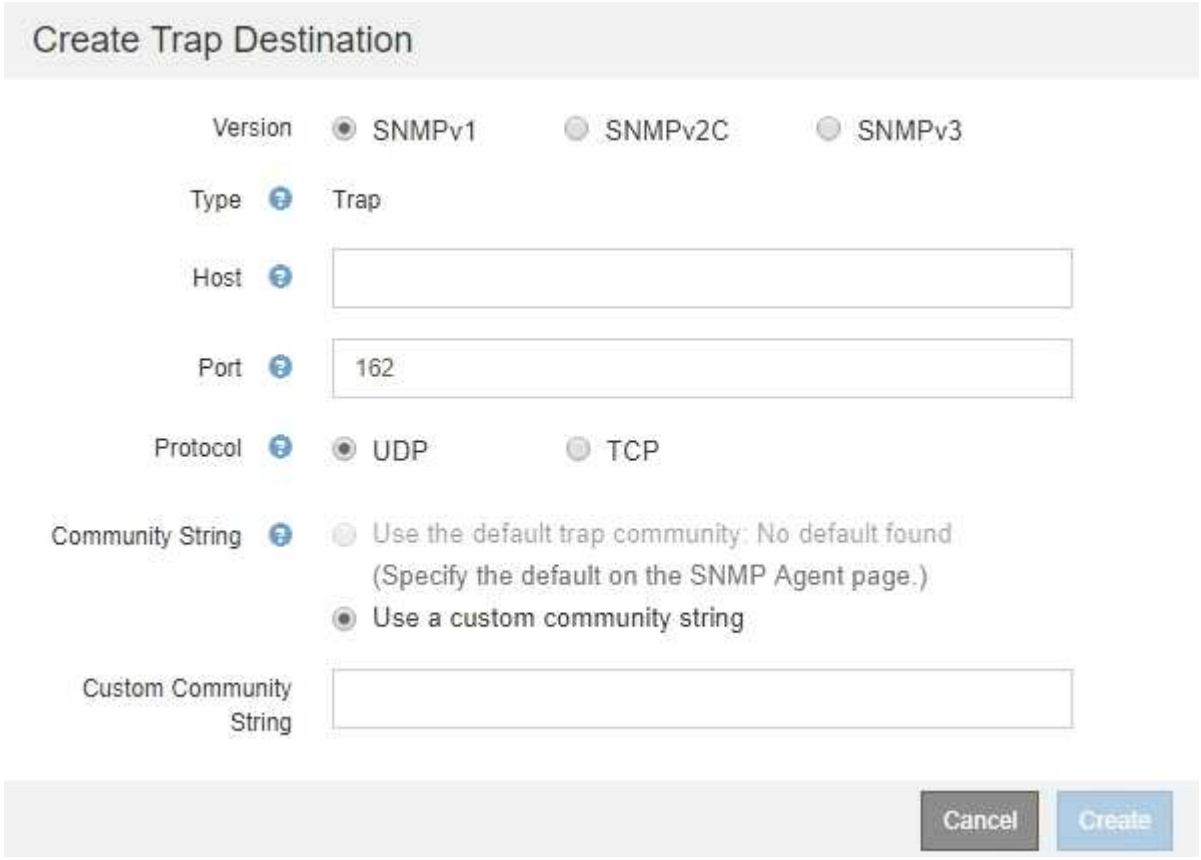


10. nella sezione altre configurazioni, selezionare la scheda Destinazioni trap.

La scheda Destinazioni trap consente di definire una o più destinazioni per le trap StorageGRID o le notifiche di notifica. Quando si attiva l'agente SNMP e si fa clic su **Salva**, StorageGRID inizia a inviare notifiche a ciascuna destinazione definita. Le notifiche vengono inviate quando vengono attivati avvisi e allarmi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

a. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Create Trap Destination (Crea destinazione trap).



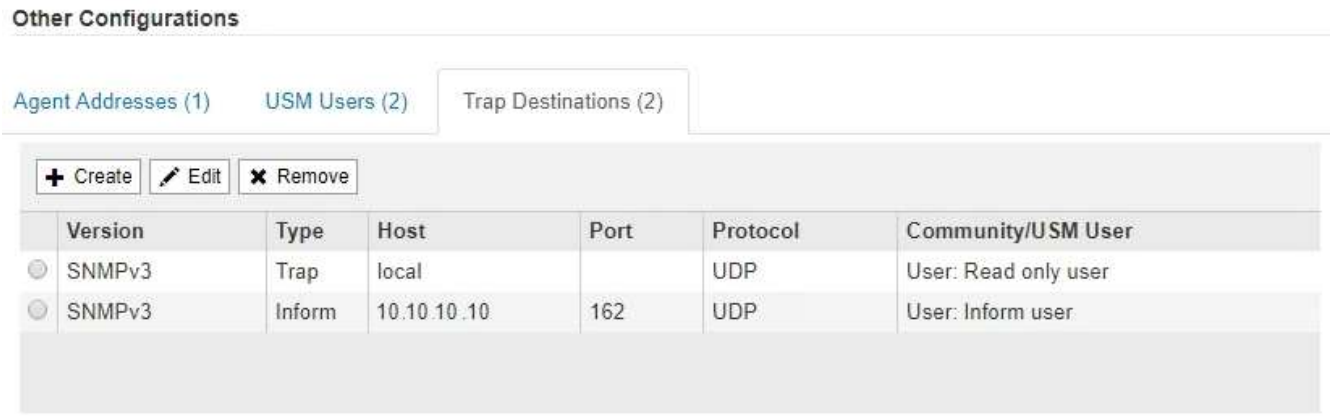
b. Nel campo **Version**, selezionare la versione SNMP da utilizzare per questa notifica.
c. Completare il modulo in base alla versione selezionata

Versione	Specificare queste informazioni
SNMPv1	**Nota:** per SNMPv1, l'agente SNMP può inviare solo trap. Le informazioni non sono supportate. i. Nel campo **host**, immettere un indirizzo IPv4 o IPv6 (o FQDN) per ricevere la trap. ii. Per **Port**, utilizzare il valore predefinito (162), a meno che non sia necessario utilizzare un altro valore. (162 è la porta standard per i trap SNMP). iii. Per **Protocol** (protocollo), utilizzare il valore predefinito (UDP). È supportato anche il protocollo TCP. (UDP è il protocollo SNMP trap standard). iv. Utilizzare la community trap predefinita, se specificata nella pagina SNMP Agent, oppure immettere una stringa di community personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.
SNMPv2c	i. Selezionare se la destinazione deve essere utilizzata per trap o informazioni. ii. Nel campo **host**, immettere un indirizzo IPv4 o IPv6 (o FQDN) per ricevere la trap. iii. Per **Port**, utilizzare il valore predefinito (162), a meno che non sia necessario utilizzare un altro valore. (162 è la porta standard per i trap SNMP). iv. Per **Protocol** (protocollo), utilizzare il valore predefinito (UDP). È supportato anche il protocollo TCP. (UDP è il protocollo SNMP trap standard). v. Utilizzare la community trap predefinita, se specificata nella pagina SNMP Agent, oppure immettere una stringa di community personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

Versione	Specificare queste informazioni
SNMPv3	i. Selezionare se la destinazione deve essere utilizzata per trap o informazioni. ii. Nel campo **host**, immettere un indirizzo IPv4 o IPv6 (o FQDN) per ricevere la trap. iii. Per **Port**, utilizzare il valore predefinito (162), a meno che non sia necessario utilizzare un altro valore. (162 è la porta standard per i trap SNMP). iv. Per **Protocol** (protocollo), utilizzare il valore predefinito (UDP). È supportato anche il protocollo TCP. (UDP è il protocollo SNMP trap standard). v. Selezionare l'utente USM che verrà utilizzato per l'autenticazione. ◦ Se si seleziona **Trap**, vengono visualizzati solo gli utenti USM senza ID motore autorevoli. ◦ Se si seleziona **inform**, vengono visualizzati solo gli utenti USM con ID motore autorevoli.

d. Fare clic su **Create** (Crea).

La destinazione trap viene creata e aggiunta alla tabella.



11. Una volta completata la configurazione dell'agente SNMP, fare clic su **Save** (Salva)

La nuova configurazione dell'agente SNMP diventa attiva.

Informazioni correlate

"Tacitare le notifiche di avviso"

Aggiornamento dell'agente SNMP

È possibile disattivare le notifiche SNMP, aggiornare le stringhe di comunità o aggiungere o rimuovere indirizzi di agenti, utenti USM e destinazioni trap.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

Ogni volta che si aggiorna la configurazione dell'agente SNMP, fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent per confermare le modifiche apportate in ciascuna scheda.

Fasi

1. Selezionare **Configuration Monitoring SNMP Agent**.

   Viene visualizzata la pagina SNMP Agent.

2. Se si desidera disattivare l'agente SNMP su tutti i nodi della griglia, deselezionare la casella di controllo **Enable SNMP** (attiva SNMP) e fare clic su **Save** (Salva).

   L'agente SNMP è disattivato per tutti i nodi della griglia. Se in seguito si riattiva l'agente, vengono mantenute le impostazioni di configurazione SNMP precedenti.

3. In alternativa, aggiornare i valori immessi per **contatto di sistema** e **posizione di sistema**.
4. Facoltativamente, deselezionare la casella di controllo **attiva notifiche agente SNMP** se non si desidera più che l'agente SNMP StorageGRID invii messaggi trap e avvisi.

   Se questa casella di controllo non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.

5. Facoltativamente, deselezionare la casella di controllo **attiva trap di autenticazione** se non si desidera più che l'agente SNMP di StorageGRID invii una trap di autenticazione quando riceve un messaggio di protocollo autenticato in modo errato.
6. Se si utilizza SNMPv1 o SNMPv2c, aggiornare la sezione Community Strings (stringhe di comunità).

   I campi di questa sezione vengono utilizzati per l'autenticazione basata sulla community in SNMPv1 o SNMPv2c. Questi campi non si applicano a SNMPv3.

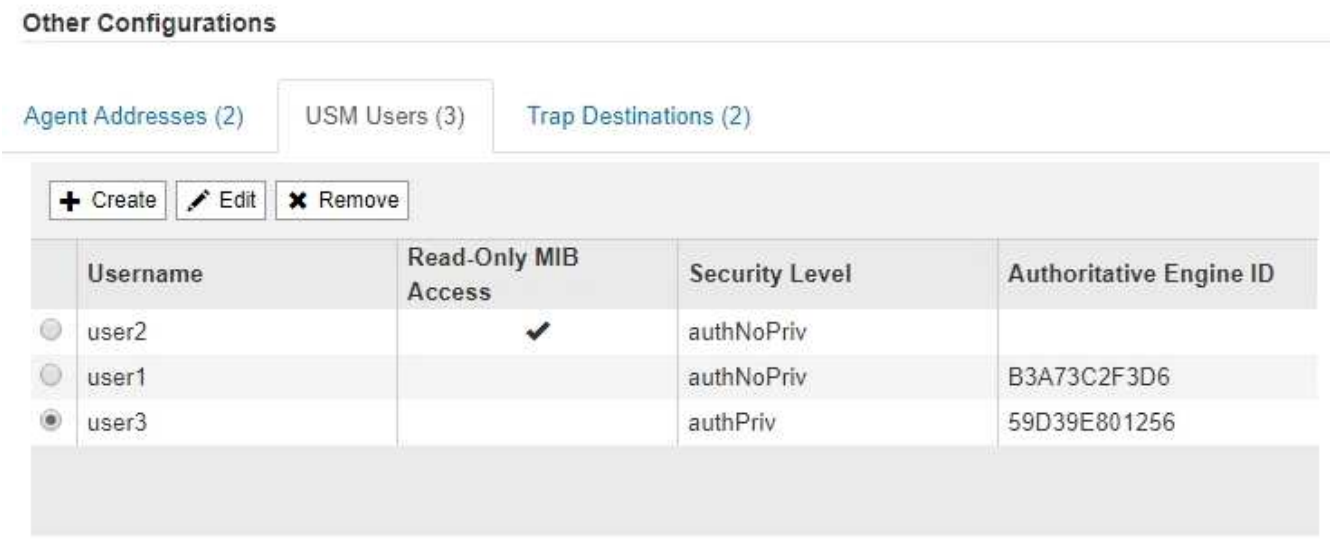
   > Se si desidera rimuovere la stringa di comunità predefinita, assicurarsi innanzitutto che tutte le destinazioni trap utilizzino una stringa di comunità personalizzata.

7. Se si desidera aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agenti nella sezione altre configurazioni.

Utilizzare questa scheda per specificare uno o più “indirizzi in attesa”. Questi sono gli indirizzi StorageGRID sui quali l’agente SNMP può ricevere le query. Ogni indirizzo dell’agente include un protocollo Internet, un protocollo di trasporto, una rete StorageGRID e una porta.

a. Per aggiungere un indirizzo agente, fare clic su **Crea**. Quindi, fare riferimento alla fase relativa agli indirizzi degli agenti nelle istruzioni per la configurazione dell’agente SNMP.
b. Per modificare l’indirizzo di un agente, selezionare il pulsante di opzione corrispondente all’indirizzo e fare clic su **Modifica**. Quindi, fare riferimento alla fase relativa agli indirizzi degli agenti nelle istruzioni per la configurazione dell’agente SNMP.
c. Per rimuovere un indirizzo dell’agente, selezionare il pulsante di opzione corrispondente all’indirizzo e fare clic su **Remove** (Rimuovi). Quindi, fare clic su **OK** per confermare che si desidera rimuovere questo indirizzo.
d. Per confermare le modifiche, fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent.

8. Se si desidera aggiornare gli utenti USM, selezionare la scheda utenti USM nella sezione altre configurazioni.



Utilizzare questa scheda per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

a. Per aggiungere un utente USM, fare clic su **Crea**. Quindi, fare riferimento alla fase per gli utenti USM nelle istruzioni per la configurazione dell’agente SNMP.

b. Per modificare un utente USM, selezionare il pulsante di opzione dell'utente e fare clic su **Edit** (Modifica). Quindi, fare riferimento alla fase per gli utenti USM nelle istruzioni per la configurazione dell'agente SNMP.

   Il nome utente di un utente USM esistente non può essere modificato. Se è necessario modificare un nome utente, rimuovere l'utente e crearne uno nuovo.

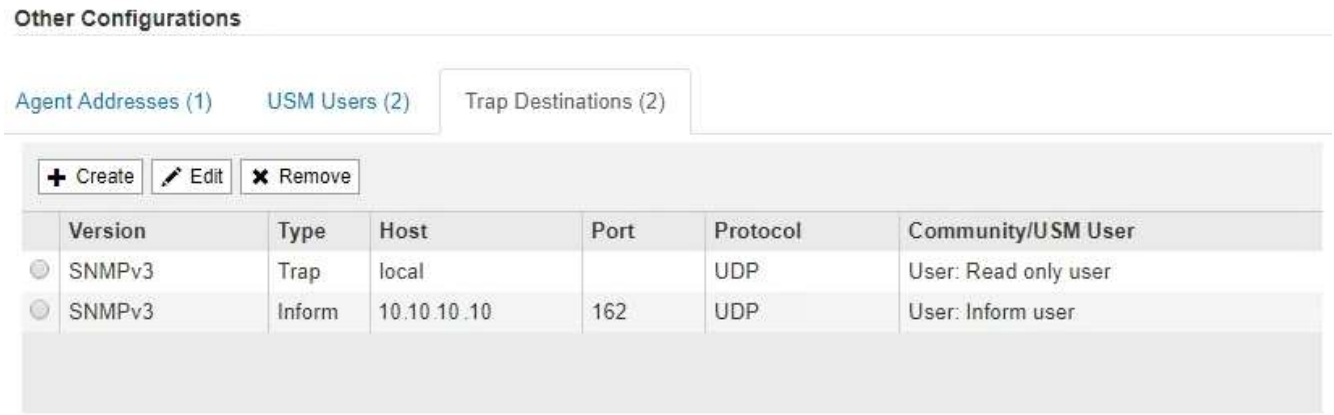
   Se si aggiunge o rimuove l'ID motore autorevole di un utente e tale utente è attualmente selezionato per una destinazione, è necessario modificare o rimuovere la destinazione, come descritto al punto Destinazione trap SNMP. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

c. Per rimuovere un utente USM, selezionare il pulsante di opzione dell'utente e fare clic su **Remove** (Rimuovi). Quindi, fare clic su **OK** per confermare che si desidera rimuovere l'utente.

   Se l'utente rimosso è attualmente selezionato per una destinazione trap, è necessario modificare o rimuovere la destinazione, come descritto al punto Destinazione trap SNMP. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

a. Per confermare le modifiche, fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent.

1. Se si desidera aggiornare le destinazioni trap, selezionare la scheda Destinations trap nella sezione Other Configurations (altre configurazioni).



La scheda Destinazioni trap consente di definire una o più destinazioni per le trap StorageGRID o le notifiche di notifica. Quando si attiva l'agente SNMP e si fa clic su **Salva**, StorageGRID inizia a inviare notifiche a ciascuna destinazione definita. Le notifiche vengono inviate quando vengono attivati avvisi e

allarmi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

a. Per aggiungere una destinazione trap, fare clic su **Create** (Crea). Quindi, fare riferimento alla fase relativa alle destinazioni trap nelle istruzioni per la configurazione dell'agente SNMP.
b. Per modificare una destinazione trap, selezionare il pulsante di opzione dell'utente e fare clic su **Edit** (Modifica). Quindi, fare riferimento alla fase relativa alle destinazioni trap nelle istruzioni per la configurazione dell'agente SNMP.
c. Per rimuovere una destinazione trap, selezionare il pulsante di opzione corrispondente alla destinazione e fare clic su **Remove** (Rimuovi). Quindi, fare clic su **OK** per confermare che si desidera rimuovere questa destinazione.
d. Per confermare le modifiche, fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent.

2. Una volta aggiornata la configurazione dell'agente SNMP, fare clic su **Save** (Salva).

Informazioni correlate

"Configurazione dell'agente SNMP"

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.