Utilizzare il monitoraggio SNMP

StorageGRID

NetApp
March 12, 2025

Sommario

Utilizzare il monitoraggio SNMP

USA monitoraggio SNMP: Panoramica

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

- "Configurare l'agente SNMP"
- "Aggiornare l'agente SNMP"

Funzionalità

Ogni nodo StorageGRID esegue un agente SNMP, o daemon, che fornisce un 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.

Vedere "Accedere ai file MIB" Se si desidera scaricare i file MIB sui nodi della griglia.

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:

Trappole

I 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.

Informa

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 tentativi.

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 "Nodo Admin mittente preferito".

  Ogni avviso viene associato 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 questi trap, vedere "Riferimenti agli avvisi".

- Certo "allarmi (sistema legacy)" vengono attivati a livelli di gravità 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 (GET e GETNEXT)	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 (INTRAPPOLARE e INFORMARE)	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.

Configurare l'agente SNMP

È possibile configurare l'agente SNMP StorageGRID in modo che utilizzi un sistema di gestione SNMP di terze parti per l'accesso MIB di sola lettura e le notifiche.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

L'agente SNMP di StorageGRID supporta SNMPv1, SNMPv2c e SNMPv3. È possibile configurare l'agente per

una o più versioni. Per SNMPv3, è supportata solo l'autenticazione del modello di sicurezza utente (USM).

Tutti i nodi nella griglia utilizzano la stessa configurazione SNMP.

Specificare la configurazione di base

Come prima fase, attivare l'agente SMNP StorageGRID e fornire informazioni di base.

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).
3. Inserire le seguenti informazioni nella sezione Configurazione di base.

Campo	Descrizione
Contatto per il sistema	Opzionale. Il contatto principale per il sistema StorageGRID, che viene restituito nei messaggi SNMP come sysContact. In genere, il contatto di sistema è un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID. **Il contatto di sistema** può contenere al massimo 255 caratteri.
Ubicazione del sistema	Opzionale. La posizione del sistema StorageGRID, che viene restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere una qualsiasi informazione utile per identificare la posizione del sistema StorageGRID. Ad esempio, è possibile utilizzare l'indirizzo di una struttura. Questo valore si applica a tutti i nodi nel sistema StorageGRID. **La posizione del sistema** può contenere al massimo 255 caratteri.
Attivare le notifiche dell'agente SNMP	• Se selezionata, l'agente SNMP StorageGRID invia notifiche trap e inform. • Se questa opzione non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.
Abilita trap di autenticazione	Se selezionata, l'agente SNMP StorageGRID invia trap di autenticazione se riceve messaggi di protocollo autenticati in modo errato.

Immettere le stringhe di comunità

Se si utilizza SNMPv1 o SNMPv2c, completare la sezione Community Strings (stringhe comunità).

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.

Fasi

1. Per **comunità di sola lettura**, è possibile immettere una stringa di comunità per consentire l'accesso MIB di sola lettura agli indirizzi di agenti IPv4 e IPv6.

   Per garantire la sicurezza del sistema StorageGRID, non utilizzare "public" come stringa di comunità. Se questo campo viene lasciato vuoto, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa di comunità.

   Ogni stringa di community può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

2. Selezionare **Aggiungi un'altra stringa di comunità** per aggiungere altre stringhe.

   Sono consentite fino a cinque stringhe.

creare destinazioni trap

Utilizzare la scheda destinazioni trap nella sezione altre configurazioni per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

Fasi

1. Per il campo **Comunità trap predefinita**, è possibile immettere la stringa di comunità predefinita che si desidera utilizzare per le destinazioni trap SNMPv1 o SNMPv2.

   Se necessario, è possibile fornire una stringa di comunità diversa ("personalizzata") quando si definisce una destinazione trap specifica.

   La comunità trap predefinita può contenere al massimo 32 caratteri e non può contenere spazi vuoti.

2. Per aggiungere una destinazione trap, selezionare **Crea**.
3. Selezionare la versione SNMP che verrà utilizzata per la destinazione trap.
4. Completare il modulo Crea destinazione trap per la versione selezionata.

SNMPv1

Se si seleziona SNMPv1 come versione, completare questi campi.

Campo	Descrizione
Tipo	Deve essere trap per SNMPv1.
Host	Un indirizzo IPv4 o IPv6 o un nome di dominio completo (FQDN) per ricevere il trap.
Porta	Utilizzare 162, quale porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv2c

Se si seleziona SNMPv2c come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv3

Se si seleziona SNMPv3 come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Utente USM	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. • Se non viene visualizzato alcun utente: i. Creare e salvare la destinazione trap. ii. Passare a. Creare utenti USM e creare l'utente. iii. Tornare alla scheda Destinazioni trap, selezionare la destinazione salvata dalla tabella e selezionare **Modifica**. iv. Selezionare l'utente.

5. Selezionare **Crea**.

   La destinazione trap viene creata e aggiunta alla tabella.

Creare gli indirizzi degli agenti

Facoltativamente, utilizzare la scheda indirizzi agente nella sezione altre configurazioni per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

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

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

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

Campo	Descrizione
Protocollo di trasporto	Se questo indirizzo utilizza UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
Rete StorageGRID	La rete StorageGRID su cui l'agente ascolta. • Grid, Admin e Client Networks (reti Grid, Admin e Client): L'agente SNMP è in attesa di query su tutte e tre le reti. • Grid Network • Admin Network (rete amministrativa) • Rete client **Nota**: Se si utilizza la rete client per i dati non protetti e si crea un indirizzo agente per la rete client, tenere presente che anche il traffico SNMP non sarà sicuro.
Porta	Facoltativamente, il numero di porta su cui l'agente SNMP deve essere in attesa. La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta inutilizzato. **Nota**: 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.

3. Selezionare **Crea**.

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

creare utenti USM

Se si utilizza SNMPv3, utilizzare la scheda utenti USM nella sezione altre configurazioni per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

> SNMPv3 *inform* le destinazioni devono avere utenti con ID motore. SNMPv3 la destinazione *trap* non può avere utenti con ID motore.

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

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

Campo	Descrizione
Nome utente	Un nome univoco per questo utente USM. I nomi utente possono avere un massimo di 32 caratteri e non possono contenere spazi vuoti. Il nome utente non può essere modificato dopo la creazione dell'utente.
Accesso MIB di sola lettura	Se selezionata, l'opzione consente all'utente di accedere in sola lettura al MIB.
ID motore autorevole	Se l'utente verrà utilizzato in una destinazione inform, l'ID motore autorevole per questo utente. Inserire da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è necessario per gli utenti USM che verranno selezionati nelle destinazioni trap per gli informa. Questo valore non è consentito per gli utenti USM che verranno selezionati nelle destinazioni trap per trap. **Nota**: Questo campo non viene visualizzato se si seleziona **accesso MIB di sola lettura** perché gli utenti USM che hanno accesso MIB di sola lettura non possono avere ID motore.
Livello di sicurezza	Il 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.
Protocollo di autenticazione	Impostare sempre su SHA, che è l'unico protocollo supportato (HMAC-SHA-96).
Password	La password che l'utente utilizzerà per l'autenticazione.
Protocollo di privacy	Visualizzato solo se si seleziona **authviv** e si imposta sempre su AES, che è l'unico protocollo di privacy supportato.
Password	Visualizzato solo se è stato selezionato **authviv**. La password che l'utente utilizzerà per la privacy.

3. Selezionare **Crea**.

   L'utente USM viene creato e aggiunto alla tabella.

4. Una volta completata la configurazione dell'agente SNMP, selezionare **Salva**.

La nuova configurazione dell'agente SNMP diventa attiva.

Aggiornare l'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.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

Vedere "Configurare l'agente SNMP" Per informazioni dettagliate su ciascun campo nella pagina dell'agente SNMP. È necessario selezionare **Salva** nella parte inferiore della pagina per confermare le modifiche apportate in ciascuna scheda.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**.

   Viene visualizzata la pagina SNMP Agent.

2. Per disattivare l'agente SNMP su tutti i nodi della griglia, deselezionare la casella di controllo **attiva SNMP** e selezionare **Salva**.

   Se si riattiva l'agente SNMP, tutte le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Se si desidera, aggiornare le informazioni nella sezione Configurazione di base:
   a. Se necessario, aggiornare **System contact** e **System location**.
   b. In alternativa, selezionare o deselezionare la casella di controllo **attiva notifiche agente SNMP** per controllare se l'agente SNMP StorageGRID invia notifiche trap e inform.

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

   c. Facoltativamente, selezionare o deselezionare 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 autenticati in modo errato.
4. Se si utilizza SNMPv1 o SNMPv2c, è possibile aggiornare o aggiungere una comunità **di sola lettura** nella sezione Community Strings (stringhe comunità).
5. Per aggiornare le destinazioni trap, selezionare la scheda destinazioni trap nella sezione altre configurazioni.

   Utilizzare questa scheda per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

   Per informazioni dettagliate su cosa immettere, vedere "Creare destinazioni trap".

   - Facoltativamente, aggiornare o rimuovere la comunità trap predefinita.

Se si rimuove la comunità trap predefinita, è necessario innanzitutto verificare che tutte le destinazioni trap esistenti utilizzino una stringa di comunità personalizzata.

- Per aggiungere una destinazione trap, selezionare **Crea**.
- Per modificare una destinazione trap, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere una destinazione trap, selezionare il pulsante di opzione e selezionare **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

6. Per aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

   Utilizzare questa scheda per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

   Per informazioni dettagliate su cosa immettere, vedere "Creare gli indirizzi degli agenti".

   - Per aggiungere un indirizzo agente, selezionare **Crea**.
   - Per modificare l'indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Modifica**.
   - Per rimuovere un indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Rimuovi**.
   - Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

7. Per 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.

   Per informazioni dettagliate su cosa immettere, vedere "Creare utenti USM".

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

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

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

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

   - Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

8. Una volta aggiornata la configurazione dell'agente SNMP, selezionare **Salva**.

Accedere ai file MIB

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

Vedere "Utilizzare il monitoraggio SNMP" Per ulteriori informazioni sui file SNMP e MIB.

Accedere ai file MIB

Per accedere ai file MIB, procedere come segue.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**.
2. Nella pagina dell'agente SNMP, selezionare il file che si desidera 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 gli oggetti e le notifiche per le appliance basate su e-Series.
   - **MIB_1_10.zip**: Definisce gli oggetti e le notifiche per le appliance con un'interfaccia BMC.

   È inoltre possibile accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID StorageGRID dal file MIB:

   a. Ottenere l'OID della directory principale del MIB StorageGRID:

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

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

   a. Grep per l'OID di StorageGRID nell'intero albero (usando `paste` per unire le linee):

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

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

Contenuto del file MIB

Tutti gli oggetti si trovano sotto l'OID StorageGRID.

Nome dell'oggetto	ID oggetto (OID)	Descrizione
iso.org.dod.internet. private.enterprise. netapp.storagegrid		Il modulo MIB per le entità NetApp StorageGRID.

Oggetti MIB

Nome dell'oggetto	ID oggetto (OID)	Descrizione
ActiveAlertCount	**1.3.6.1.4.1.** 789.28669.1.3	Il numero di avvisi attivi in activeAlertTable.
ActiveAlertTable	**1.3.6.1.4.1.** 789.28669.1.4	Tabella degli avvisi attivi in StorageGRID.
ActiveAlertId	**1.3.6.1.4.1.** 789.28669.1.4.1.1	L'ID dell'avviso. Unico solo nel set corrente di avvisi attivi.
ActiveAlertName	**1.3.6.1.4.1.** 789.28669.1.4.1.2	Il nome dell'avviso.
ActiveAlertInstance	**1.3.6.1.4.1.** 789.28669.1.4.1.3	Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
ActiveAlertSeverity	**1.3.6.1.4.1.** 789.28669.1.4.1.4	La severità dell'avviso.
ActiveAlertStartTime	**1.3.6.1.4.1.** 789.28669.1.4.1.5	La data e l'ora di attivazione dell'avviso.

Tipi di notifica (trap)

Tutte le notifiche includono le seguenti variabili come varbind:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo di notifica	ID oggetto (OID)	Descrizione
ActiveMinorAlert	**1.3.6.1.4.1.** 789.28669.0.6	Un avviso con un livello di severità minore
ActiveMajorAlert	**1.3.6.1.4.1.** 789.28669.0.7	Un avviso con severità maggiore
ActiveCriticalAlert	**1.3.6.1.4.1.** 789.28669.0.8	Un avviso con severità critica

Informazioni sul copyright

Informazioni sul marchio commerciale