Verwenden Sie SNMP-Überwachung

StorageGRID 11.8

NetApp
March 19, 2024

Inhalt

Verwenden Sie SNMP-Überwachung 1
Verwenden Sie SNMP-Überwachung: Übersicht 1
Konfigurieren Sie den SNMP-Agent 2
Aktualisieren Sie den SNMP-Agent 9
Zugriff auf MIB-Dateien 11

Verwenden Sie SNMP-Überwachung

Verwenden Sie SNMP-Überwachung: Übersicht

Wenn Sie StorageGRID mit dem Simple Network Management Protocol (SNMP) überwachen möchten, müssen Sie den SNMP-Agent konfigurieren, der in StorageGRID enthalten ist.

- "Konfigurieren Sie den SNMP-Agent"
- "Aktualisieren Sie den SNMP-Agent"

Sorgen

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder -Daemon ausgeführt, der eine MIB bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Alarme und Alarme. Die MIB enthält auch Informationen zur Systembeschreibung wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID-Knoten unterstützt auch eine Untergruppe von MIB-II-Objekten.

Siehe "Zugriff auf MIB-Dateien" Wenn Sie die MIB-Dateien auf Ihrem Grid-Knoten herunterladen möchten.

Zunächst ist SNMP auf allen Knoten deaktiviert. Wenn Sie den SNMP-Agent konfigurieren, erhalten alle StorageGRID-Knoten die gleiche Konfiguration.

Der StorageGRID SNMP Agent unterstützt alle drei Versionen des SNMP-Protokolls. Es bietet schreibgeschützten MIB-Zugriff für Abfragen, und es kann zwei Arten von ereignisgesteuerten Benachrichtigungen an ein Verwaltungssystem senden:

Traps

Traps sind Benachrichtigungen, die vom SNMP-Agenten gesendet werden und keine Bestätigung durch das Managementsystem erfordern. Traps dienen dazu, das Managementsystem über etwas innerhalb von StorageGRID zu informieren, wie z. B. eine Warnung, die ausgelöst wird.

Traps werden in allen drei Versionen von SNMP unterstützt.

Informiert

Informationen sind ähnlich wie Traps, aber sie erfordern eine Bestätigung durch das Management-System. Wenn der SNMP-Agent innerhalb einer bestimmten Zeit keine Bestätigung erhält, wird die Benachrichtigung erneut gesendet, bis eine Bestätigung empfangen oder der maximale Wiederholungswert erreicht wurde.

Die Informationsunterstützung wird in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden in folgenden Fällen versendet:

- Eine Standardwarnung oder eine benutzerdefinierte Meldung wird für jeden Schweregrad ausgelöst. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, müssen Sie "Konfigurieren Sie eine Stille" Für den Alarm. Warnmeldungen werden vom gesendet "Administratorknoten des bevorzugten Absenders".

  Jeder Alarm wird einem von drei Trap-Typen basierend auf dem Schweregrad des Alarms zugeordnet: ActiveMinorAlert, activeMajorAlert und activeCriticalAlert. Eine Liste der Warnmeldungen, mit denen diese

Traps ausgelöst werden können, finden Sie im "Alerts Referenz".

- Sicher "Alarme (Altsystem)" Werden bei einem bestimmten oder höheren Schweregrad ausgelöst.

> SNMP-Benachrichtigungen werden nicht für jeden Alarm oder für jeden Schweregrad des Alarms gesendet.

Unterstützung von SNMP-Versionen

Die Tabelle bietet eine allgemeine Zusammenfassung der unterstützten SNMP-Versionen.

	SNMPv1	SNMPv2c	SNMPv3
Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-Zeichenfolge	Community-Zeichenfolge	Benutzer des benutzerbasierten Sicherheitsmodells (USM)
Benachrichtigungen	Nur Traps	Traps und informiert	Traps und informiert
Benachrichtigungsauthentifizierung	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	USM-Benutzer für jedes Trap-Ziel

Einschränkungen

- StorageGRID unterstützt schreibgeschützten MIB-Zugriff. Lese-Schreibzugriff wird nicht unterstützt.
- Alle Nodes im Grid erhalten dieselbe Konfiguration.
- SNMPv3: StorageGRID unterstützt den Transport Support Mode (TSM) nicht.
- SNMPv3: Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).
- SNMPv3: Das einzige unterstützte Datenschutzprotokoll ist AES.

Konfigurieren Sie den SNMP-Agent

Sie können den StorageGRID SNMP-Agent so konfigurieren, dass ein SNMP-Verwaltungssystem eines Drittanbieters für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwendet wird.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

Der StorageGRID SNMP-Agent unterstützt SNMPv1, SNMPv2c und SNMPv3. Sie können den Agent für eine oder mehrere Versionen konfigurieren. Für SNMPv3 wird nur USM-Authentifizierung (User Security Model) unterstützt.

Alle Knoten im Grid verwenden dieselbe SNMP-Konfiguration.

Geben Sie die Grundkonfiguration an

Aktivieren Sie als ersten Schritt den StorageGRID-SMNP-Agent und geben Sie grundlegende Informationen an.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.

   Die Seite SNMP Agent wird angezeigt.

2. Um den SNMP-Agent auf allen Grid-Knoten zu aktivieren, aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.
3. Geben Sie im Abschnitt Grundkonfiguration die folgenden Informationen ein.

Feld	Beschreibung
Systemkontakt	Optional Der primäre Kontakt für das StorageGRID-System, der in SNMP-Nachrichten als sysContact zurückgegeben wird. Der Systemkontakt ist normalerweise eine E-Mail-Adresse. Dieser Wert gilt für alle Knoten im StorageGRID-System. **Systemkontakt** kann maximal 255 Zeichen lang sein.
Standort des Systems	Optional Der Speicherort des StorageGRID-Systems, der in SNMP-Nachrichten als sysLocation zurückgegeben wird. Der Systemstandort kann jede Information sein, die hilfreich ist, um zu ermitteln, wo sich das StorageGRID System befindet. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Dieser Wert gilt für alle Knoten im StorageGRID-System. **Systemstandort** kann maximal 255 Zeichen lang sein.
Aktivieren Sie SNMP-Agentenbenachrichtigungen	• Wenn diese Option ausgewählt ist, sendet der StorageGRID-SNMP-Agent Trap- und Inform-Benachrichtigungen. • Wenn diese Option nicht ausgewählt ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.
Aktivieren Sie Authentifizierungs-Traps	Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Authentifizierungs-Traps, wenn er falsch authentifizierte Protokollmeldungen empfängt.

Geben Sie Community-Strings ein

Wenn Sie SNMPv1 oder SNMPv2c verwenden, füllen Sie den Abschnitt Community Strings aus.

Wenn das Verwaltungssystem die StorageGRID-MIB abfragt, sendet es eine Community-Zeichenfolge. Wenn die Community-Zeichenfolge einem der hier angegebenen Werte entspricht, sendet der SNMP-Agent eine Antwort an das Managementsystem.

Schritte

1. Geben Sie für **Read-Only Community** optional eine Community-Zeichenfolge ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agent-Adressen zu ermöglichen.

   > Um die Sicherheit Ihres StorageGRID-Systems zu gewährleisten, verwenden Sie nicht „public“ als Community-String. Wenn Sie dieses Feld leer lassen, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID-Systems als Community-String.

   Jede Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.

2. Wählen Sie **Add another Community string**, um zusätzliche Strings hinzuzufügen.

   Es sind bis zu fünf Zeichenfolgen zulässig.

Trap-Ziele erstellen

Verwenden Sie die Registerkarte Trap-Ziele im Abschnitt andere Konfigurationen, um ein oder mehrere Ziele für StorageGRID-Trap- oder Inform-Benachrichtigungen zu definieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, wenn Warnungen ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

Schritte

1. Geben Sie für das Feld **Default Trap Community** optional den Standard-Community-String ein, den Sie für SNMPv1- oder SNMPv2-Trap-Ziele verwenden möchten.

   Wenn Sie ein bestimmtes Trap-Ziel definieren, können Sie nach Bedarf eine andere (benutzerdefinierte) Community-Zeichenfolge bereitstellen.

   Default Trap Community kann maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.

2. Um ein Trap-Ziel hinzuzufügen, wählen Sie **Create**.
3. Wählen Sie aus, welche SNMP-Version für dieses Trap-Ziel verwendet werden soll.
4. Füllen Sie das Formular Trap-Ziel erstellen für die ausgewählte Version aus.

SNMPv1

Wenn Sie SNMPv1 als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Muss Trap für SNMPv1 sein.
Host	Eine IPv4- oder IPv6-Adresse oder ein vollständig qualifizierter Domänenname (FQDN) für den Empfang des Traps.
Port	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das das Standard-SNMP-Trap-Protokoll ist, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, falls eine angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.

SNMPv2c

Wenn Sie SNMPv2c als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Gibt an, ob das Ziel für Traps oder Informs verwendet wird.
Host	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Port	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das das Standard-SNMP-Trap-Protokoll ist, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, falls eine angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.

SNMPv3

Wenn Sie SNMPv3 als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Gibt an, ob das Ziel für Traps oder Informs verwendet wird.
Host	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Port	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das das Standard-SNMP-Trap-Protokoll ist, es sei denn, Sie müssen TCP verwenden.
USM-Benutzer	Der USM-Benutzer, der für die Authentifizierung verwendet wird. • Wenn Sie **Trap** ausgewählt haben, werden nur USM-Benutzer ohne maßgebliche Engine-IDs angezeigt. • Wenn Sie **Inform** ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt. • Wenn keine Benutzer angezeigt werden: i. Erstellen und speichern Sie das Trap-Ziel. ii. Gehen Sie zu USM-Benutzer erstellen Und erstellen Sie den Benutzer. iii. Kehren Sie zur Registerkarte Trap-Ziele zurück, wählen Sie das gespeicherte Ziel aus der Tabelle aus und wählen Sie **Bearbeiten**. iv. Wählen Sie den Benutzer aus.

5. Wählen Sie **Erstellen**.

   Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

Erstellen Sie Agentenadressen

Verwenden Sie optional die Registerkarte Agentenadressen im Abschnitt andere Konfigurationen, um eine oder mehrere „Listening-Adressen“ anzugeben. Dies sind die StorageGRID-Adressen, über die der SNMP-Agent Abfragen empfangen kann.

Wenn Sie keine Agentenadresse konfigurieren, ist die standardmäßige Abhöradresse in allen StorageGRID-Netzwerken UDP-Port 161.

Schritte

1. Wählen Sie **Erstellen**.
2. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Internetprotokoll	Gibt an, ob diese Adresse IPv4 oder IPv6 verwendet. Standardmäßig verwendet SNMP IPv4.
Transportprotokoll	Ob diese Adresse UDP oder TCP verwendet. Standardmäßig verwendet SNMP UDP.
StorageGRID-Netzwerk	Welches StorageGRID-Netzwerk der Agent abhört. • Grid-, Admin- und Client-Netzwerke: Der SNMP-Agent hört auf Abfragen in allen drei Netzwerken. • Grid-Netzwerk • Admin-Netzwerk • Client-Netzwerk **Hinweis**: Wenn Sie das Client-Netzwerk für unsichere Daten verwenden und eine Agentenadresse für das Client-Netzwerk erstellen, beachten Sie, dass der SNMP-Datenverkehr ebenfalls unsicher ist.
Port	Optional die Portnummer, die der SNMP-Agent abhören soll. Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch alle nicht verwendeten Portnummern eingeben. **Hinweis**: Wenn Sie den SNMP-Agent speichern, öffnet StorageGRID automatisch die Agentenadressen-Ports auf der internen Firewall. Sie müssen sicherstellen, dass alle externen Firewalls den Zugriff auf diese Ports zulassen.

3. Wählen Sie **Erstellen**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

Erstellen Sie USM-Benutzer

Wenn Sie SNMPv3 verwenden, definieren Sie auf der Registerkarte USM-Benutzer im Abschnitt andere Konfigurationen die USM-Benutzer, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

SNMPv3 *Inform* Ziele müssen Benutzer mit Engine-IDs haben. SNMPv3 *Trap* Ziel kann keine Benutzer mit Engine-IDs haben.

Diese Schritte gelten nicht, wenn Sie nur SNMPv1 oder SNMPv2c verwenden.

Schritte

1. Wählen Sie **Erstellen**.
2. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Benutzername	Ein eindeutiger Name für diesen USM-Benutzer. Benutzernamen dürfen maximal 32 Zeichen enthalten und dürfen keine Leerzeichen enthalten. Der Benutzername kann nach dem Erstellen des Benutzers nicht mehr geändert werden.
Schreibgeschützter MIB-Zugriff	Wenn diese Option ausgewählt ist, sollte dieser Benutzer Lesezugriff auf die MIB haben.
Maßgeblicher Engine-ID	Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, ist die ID der autorisierenden Engine für diesen Benutzer. Geben Sie 10 bis 64 Hex-Zeichen (5 bis 32 Byte) ohne Leerzeichen ein. Dieser Wert ist für USM-Benutzer erforderlich, die in Trap-Zielen für Informationen ausgewählt werden. Dieser Wert ist für USM-Benutzer, die in Trap-Zielen für Traps ausgewählt werden, nicht zulässig. **Hinweis**: Dieses Feld wird nicht angezeigt, wenn Sie **schreibgeschützter MIB-Zugriff** ausgewählt haben, da USM-Benutzer, die schreibgeschützten MIB-Zugriff haben, keine Engine-IDs haben können.
Sicherheitsstufe	Die Sicherheitsstufe für den USM-Benutzer: • **AuthPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort sowie ein Datenschutzprotokoll und ein Passwort angeben. • **AuthNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort angeben.
Authentifizierungsprotokoll	Stellen Sie immer SHA ein, welches das einzige unterstützte Protokoll ist (HMAC-SHA-96).
Passwort	Das Kennwort, das dieser Benutzer zur Authentifizierung verwendet.
Datenschutzprotokoll	Wird nur angezeigt, wenn Sie **authpriv** ausgewählt und immer auf AES gesetzt haben, das einzige unterstützte Datenschutzprotokoll.
Passwort	Wird nur angezeigt, wenn Sie **authpriv** ausgewählt haben. Das Passwort, das dieser Benutzer für den Datenschutz verwendet.

3. Wählen Sie **Erstellen**.

Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

4. Wenn Sie die SNMP-Agent-Konfiguration abgeschlossen haben, wählen Sie **Speichern**.

   Die neue SNMP-Agent-Konfiguration wird aktiv.

Aktualisieren Sie den SNMP-Agent

Sie können SNMP-Benachrichtigungen deaktivieren, Community-Strings aktualisieren oder Agent-Adressen, USM-Benutzer und Trap-Ziele hinzufügen oder entfernen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

Siehe "Konfigurieren Sie den SNMP-Agent" Für Details zu den einzelnen Feldern auf der Seite SNMP-Agent. Sie müssen unten auf der Seite **Speichern** auswählen, um alle Änderungen zu übernehmen, die Sie auf jeder Registerkarte vornehmen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.

   Die Seite SNMP Agent wird angezeigt.

2. Um den SNMP-Agent auf allen Grid-Knoten zu deaktivieren, deaktivieren Sie das Kontrollkästchen **SNMP aktivieren**, und wählen Sie **Speichern** aus.

   Wenn Sie den SNMP-Agent erneut aktivieren, bleiben alle früheren SNMP-Konfigurationseinstellungen erhalten.

3. Aktualisieren Sie optional die Informationen im Abschnitt Grundkonfiguration:
   a. Aktualisieren Sie bei Bedarf den * Systemkontakt* und **Systemstandort**.
   b. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Enable SNMP Agent notifications**, um zu steuern, ob der StorageGRID SNMP Agent Trap- und Inform-Benachrichtigungen sendet.

      Wenn dieses Kontrollkästchen deaktiviert ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.

   c. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Enable Authentication Traps**, um zu steuern, ob der StorageGRID-SNMP-Agent Authentifizierungs-Traps sendet, wenn er falsch authentifizierte Protokollmeldungen empfängt.
4. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren oder fügen Sie optional eine **schreibgeschützte Community** im Abschnitt Community Strings hinzu.
5. Um Trap-Ziele zu aktualisieren, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte Trap-Ziele aus.

   Auf dieser Registerkarte können Sie ein oder mehrere Ziele für StorageGRID-Trap- oder Informationsbenachrichtigungen definieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, wenn Warnungen ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B.

ifdown und coldstart).

Einzelheiten dazu, was Sie eingeben müssen, finden Sie unter "Erstellen Sie Trap-Ziele".

- Optional können Sie die Standard-Trap-Community aktualisieren oder entfernen.

  Wenn Sie die Standard-Trap-Community entfernen, müssen Sie zunächst sicherstellen, dass alle vorhandenen Trap-Ziele eine benutzerdefinierte Community-Zeichenfolge verwenden.

- Um ein Trap-Ziel hinzuzufügen, wählen Sie **Create**.
- Um ein Trap-Ziel zu bearbeiten, aktivieren Sie das Optionsfeld und wählen **Bearbeiten**.
- Um ein Trap-Ziel zu entfernen, aktivieren Sie das Optionsfeld und wählen Sie **Entfernen** aus.
- Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der Seite.

6. Um die Agentenadressen zu aktualisieren, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte Agentenadressen aus.

   Verwenden Sie diese Registerkarte, um eine oder mehrere „Listening-Adressen“ anzugeben. Dies sind die StorageGRID-Adressen, über die der SNMP-Agent Abfragen empfangen kann.

   Einzelheiten dazu, was Sie eingeben müssen, finden Sie unter "Erstellen Sie Agentenadressen".

   - Um eine Agentenadresse hinzuzufügen, wählen Sie **Create**.
   - Um eine Agentenadresse zu bearbeiten, aktivieren Sie das Optionsfeld und wählen **Bearbeiten**.
   - Um eine Agentenadresse zu entfernen, aktivieren Sie das Optionsfeld, und wählen Sie **Entfernen** aus.
   - Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der Seite.

7. Um USM-Benutzer zu aktualisieren, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

   Über diese Registerkarte können Sie USM-Benutzer definieren, die berechtigt sind, die MIB abzufragen oder Traps zu empfangen und zu informieren.

   Einzelheiten dazu, was Sie eingeben müssen, finden Sie unter "USM-Benutzer erstellen".

   - Um einen USM-Benutzer hinzuzufügen, wählen Sie **Create**.
   - Um einen USM-Benutzer zu bearbeiten, wählen Sie das Optionsfeld und dann **Bearbeiten** aus.

     Der Benutzername eines vorhandenen USM-Benutzers kann nicht geändert werden. Wenn Sie einen Benutzernamen ändern müssen, müssen Sie den Benutzer entfernen und einen neuen erstellen.

     > Wenn Sie die ID der autorisierenden Engine eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

   - Um einen USM-Benutzer zu entfernen, wählen Sie das Optionsfeld und dann **Entfernen** aus.

     > Wenn der Benutzer, den Sie entfernt haben, derzeit für ein Trap-Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

- Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der Seite.

8. Wenn Sie die SNMP-Agent-Konfiguration aktualisiert haben, wählen Sie **Speichern**.

Zugriff auf MIB-Dateien

MIB-Dateien enthalten Definitionen und Informationen über die Eigenschaften der verwalteten Ressourcen und Dienste für die Knoten in der Tabelle. Sie können auf MIB-Dateien zugreifen, die die Objekte und Benachrichtigungen für StorageGRID definieren. Diese Dateien können für die Überwachung Ihres Grids nützlich sein.

Siehe "Verwenden Sie SNMP-Überwachung" Weitere Informationen zu SNMP- und MIB-Dateien.

Zugriff auf MIB-Dateien

Gehen Sie wie folgt vor, um auf die MIB-Dateien zuzugreifen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.
2. Wählen Sie auf der Seite des SNMP-Agenten die Datei aus, die Sie herunterladen möchten:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definiert die Alarmtabelle und Benachrichtigungen (Traps), auf die auf allen Admin-Knoten zugegriffen werden kann.
   - **Es-NETAPP-06-MIB.mib**: Definiert Objekte und Benachrichtigungen für E-Series-basierte Appliances.
   - **MIB_1_10.zip**: Definiert Objekte und Benachrichtigungen für Geräte mit BMC-Schnittstelle.

   > Sie können auch auf MIB-Dateien am folgenden Speicherort auf jedem StorageGRID-Knoten zugreifen: `/usr/share/snmp/mibs`

3. So extrahieren Sie die StorageGRID-OIDs aus der MIB-Datei:

   a. Erhalten Sie die OID des Stamms der StorageGRID MIB:

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

   Ergebnis: `.1.3.6.1.4.1.789.28669` (`28669` Ist immer die OID für StorageGRID)

   a. Grep für die StorageGRID-OID in der gesamten Struktur (mit `paste` Verbinden von Zeilen):

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

> Der `snmptranslate` Befehl hat viele Optionen, die nützlich sind, um die MIB zu erkunden. Dieser Befehl ist auf jedem StorageGRID-Node verfügbar.

MIB-Dateiinhalte

Alle Objekte befinden sich unter der StorageGRID-OID.

Objektname	Objekt-ID (OID)	Beschreibung
iso.org.dod.internet. Private.Unternehmen. netapp.storagegrid		Das MIB-Modul für NetApp StorageGRID-Einheiten.

MIB-Objekte

Objektname	Objekt-ID (OID)	Beschreibung
ActiveAlertCount	**1.3.6.1.4.1.** 789.28669.1.3	Die Anzahl der aktiven Warnungen in der activeAlertTable.
ActiveAlertTable	**1.3.6.1.4.1.** 789.28669.1.4	Eine Tabelle mit aktiven Warnmeldungen in StorageGRID.
ActiveAlertId	**1.3.6.1.4.1.** 789.28669.1.4.1.1	Die ID der Warnmeldung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
ActiveAlertName	**1.3.6.1.4.1.** 789.28669.1.4.1.2	Der Name der Warnmeldung.
ActiveAlertInstance	**1.3.6.1.4.1.** 789.28669.1.4.1.3	Der Name der Entität, die die Warnmeldung generiert hat, normalerweise der Knotenname.
ActiveAlertSchweregrad	**1.3.6.1.4.1.** 789.28669.1.4.1.4	Der Schweregrad der Meldung.
ActiveAlertStartTime	**1.3.6.1.4.1.** 789.28669.1.4.1.5	Das Datum und die Uhrzeit, zu der die Warnmeldung ausgelöst wurde.

Benachrichtigungstypen (Traps)

Alle Benachrichtigungen enthalten die folgenden Variablen als varbindes:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSchweregrad
- ActiveAlertStartTime

Benachrichtigungstyp	Objekt-ID (OID)	Beschreibung
ActiveMinorAlert	**1.3.6.1.4.1.** 789.28669.0.6	Ein Alarm mit geringem Schweregrad
ActiveMajorAlert	**1.3.6.1.4.1.** 789.28669.0.7	Ein Alarm mit dem Hauptschweregrad
ActiveCriticalAlert	**1.3.6.1.4.1.** 789.28669.0.8	Eine Meldung mit dem Schweregrad „kritisch“