Verwenden Sie die SNMP-Überwachung

StorageGRID software

NetApp
October 21, 2025

Inhalt

Verwenden Sie die SNMP-Überwachung

Verwenden Sie die SNMP-Überwachung

Wenn Sie StorageGRID mithilfe des Simple Network Management Protocol (SNMP) überwachen möchten, müssen Sie den in StorageGRID enthaltenen SNMP-Agenten konfigurieren.

- "Konfigurieren des SNMP-Agenten"
- "Aktualisieren Sie den SNMP-Agenten"

Funktionen

Auf jedem StorageGRID Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine MIB bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Warnungen. Die MIB enthält außerdem Systembeschreibungsinformationen wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID Knoten unterstützt auch eine Teilmenge von MIB-II-Objekten.

Sehen"Zugriff auf MIB-Dateien" wenn Sie die MIB-Dateien auf Ihre Grid-Knoten herunterladen möchten.

Zunächst ist SNMP auf allen Knoten deaktiviert. Wenn Sie den SNMP-Agenten konfigurieren, erhalten alle StorageGRID Knoten dieselbe Konfiguration.

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

Fallen

Traps sind vom SNMP-Agenten gesendete Benachrichtigungen, die keine Bestätigung durch das Verwaltungssystem erfordern. Traps dienen dazu, das Verwaltungssystem darüber zu informieren, dass in StorageGRID etwas passiert ist, beispielsweise dass ein Alarm ausgelöst wurde.

Traps werden in allen drei Versionen von SNMP unterstützt.

Informiert

Informs ähneln Traps, erfordern jedoch eine Bestätigung durch das Managementsystem. Wenn der SNMP-Agent innerhalb einer bestimmten Zeitspanne keine Bestätigung erhält, sendet er die Information erneut, bis eine Bestätigung eingeht oder der maximale Wiederholungswert erreicht ist.

Informs werden in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden in den folgenden Fällen gesendet:

- Bei jedem Schweregrad wird eine Standard- oder benutzerdefinierte Warnung ausgelöst. Um SNMP-Benachrichtigungen für einen Alarm zu unterdrücken, müssen Sie"Konfigurieren Sie eine Stille" für die Warnung. Warnmeldungen werden gesendet von"bevorzugter Absender-Admin-Knoten" .

  Jeder Alarm wird basierend auf seinem Schweregrad einem von drei Trap-Typen zugeordnet: activeMinorAlert, activeMajorAlert und activeCriticalAlert. Eine Liste der Warnungen, die diese Traps auslösen können, finden Sie im"Warnungsreferenz" .

SNMP-Versionsunterstützung

Die Tabelle bietet eine allgemeine Zusammenfassung der Unterstützung für jede SNMP-Version.

	SNMPv1	SNMPv2c	SNMPv3
Abfragen (GET und GETNEXT)	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-Zeichenfolge	Community-Zeichenfolge	Benutzer des benutzerbasierten Sicherheitsmodells (USM)
Benachrichtigungen (Falle und Inform)	Nur Fallen	Fallen und Informationen	Fallen und Informationen
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 Knoten im Grid erhalten die gleiche 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 des SNMP-Agenten

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

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

Alle Knoten im Grid verwenden dieselbe SNMP-Konfiguration.

Grundlegende Konfiguration festlegen

Aktivieren Sie als ersten Schritt den StorageGRID SMNP-Agenten und geben Sie grundlegende Informationen ein.

Schritte

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

   Die SNMP-Agent-Seite wird angezeigt.

2. Um den SNMP-Agenten 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** darf maximal 255 Zeichen lang sein.
Systemstandort	Optional. Der Standort des StorageGRID -Systems, der in SNMP-Nachrichten als sysLocation zurückgegeben wird. Der Systemstandort kann jede Information sein, die zur Identifizierung des Standorts Ihres StorageGRID Systems nützlich ist. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Dieser Wert gilt für alle Knoten im StorageGRID -System. **Systemstandort** darf maximal 255 Zeichen lang sein.
Aktivieren Sie SNMP-Agent-Benachrichtigungen	• 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.
Authentifizierungs-Traps aktivieren	Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Authentifizierungs-Traps, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.

Community-Strings eingeben

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 der Community-String mit einem der hier angegebenen Werte übereinstimmt, sendet der SNMP-Agent eine Antwort an das Verwaltungssystem.

Schritte

1. Geben Sie für **Nur-Lese-Community** optional eine Community-Zeichenfolge ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agentadressen zuzulassen.

   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.

   Jeder Community-String darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

2. Wählen Sie **Weitere Community-Zeichenfolge hinzufügen**, um zusätzliche Zeichenfolgen hinzuzufügen.

   Es sind bis zu fünf Zeichenfolgen zulässig.

Trap-Ziele erstellen

Verwenden Sie die Registerkarte „Trap-Ziele“ im Abschnitt „Weitere 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. Für die unterstützten MIB-II-Entitäten werden auch Standardbenachrichtigungen gesendet (z. B. ifDown und coldStart).

Schritte

1. Geben Sie im Feld **Standard-Trap-Community** optional die Standard-Community-Zeichenfolge ein, die Sie für SNMPv1- oder SNMPv2-Trap-Ziele verwenden möchten.

   Bei Bedarf können Sie bei der Definition eines bestimmten Trap-Ziels einen anderen („benutzerdefinierten“) Community-String angeben.

   Standard-Trap-Community darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

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

SNMPv1

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

Feld	Beschreibung
Typ	Muss Trap für SNMPv1 sein.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein vollqualifizierter Domänenname (FQDN) zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, sofern 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 keine Leerzeichen enthalten.

SNMPv2c

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

Feld	Beschreibung
Typ	Ob das Ziel für Fallen oder Informationen verwendet wird.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, sofern Sie nicht einen anderen Wert verwenden müssen.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, sofern 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 keine Leerzeichen enthalten.

SNMPv3

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

Feld	Beschreibung
Typ	Ob das Ziel für Fallen oder Informationen verwendet wird.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, sofern Sie nicht einen anderen Wert verwenden müssen.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, 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 autoritative Engine-IDs angezeigt. • Wenn Sie **Informieren** 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. Gehe zuErstellen von USM-Benutzern 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.

Agentenadressen erstellen

Optional können Sie auf der Registerkarte „Agentenadressen“ im Abschnitt „Weitere Konfigurationen“ eine oder mehrere „Abhöradressen“ angeben. Dies sind die StorageGRID -Adressen, unter denen der SNMP-Agent Abfragen empfangen kann.

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

Schritte

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

Feld	Beschreibung
Internetprotokoll	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	Auf welches StorageGRID -Netzwerk der Agent lauscht. • Grid-, Admin- und Client-Netzwerke: Der SNMP-Agent überwacht alle drei Netzwerke auf Abfragen. • Netznetzwerk • Admin-Netzwerk • Kundennetzwerk **Hinweis**: Wenn Sie das Client-Netzwerk für unsichere Daten verwenden und eine Agentenadresse für das Client-Netzwerk erstellen, beachten Sie, dass auch der SNMP-Verkehr unsicher ist.
Hafen	Optional die Portnummer, auf der der SNMP-Agent lauschen soll. Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch jede beliebige nicht verwendete Portnummer eingeben. **Hinweis**: Wenn Sie den SNMP-Agenten speichern, öffnet StorageGRID automatisch die Agenten-Adressports 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.

USM-Benutzer erstellen

Wenn Sie SNMPv3 verwenden, verwenden Sie die Registerkarte „USM-Benutzer“ im Abschnitt „Weitere Konfigurationen“, um die USM-Benutzer zu definieren, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

SNMPv3-*Inform*-Ziele müssen Benutzer mit Engine-IDs haben. Das 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 lang sein und keine Leerzeichen enthalten. Der Benutzername kann nach der Erstellung des Benutzers nicht mehr geändert werden.
Nur-Lese-MIB-Zugriff	Wenn diese Option ausgewählt ist, sollte dieser Benutzer nur Lesezugriff auf die MIB haben.
Autoritative Engine-ID	Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, die maßgebliche Engine-ID für diesen Benutzer. Geben Sie 10 bis 64 Hex-Zeichen (5 bis 32 Bytes) ohne Leerzeichen ein. Dieser Wert ist für USM-Benutzer erforderlich, die in Trap-Zielen für Informs 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 mit schreibgeschütztem MIB-Zugriff 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 Kennwort sowie ein Datenschutzprotokoll und ein Kennwort angeben. • **authNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Privatsphäre (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Kennwort angeben.
Authentifizierungsprotokoll	Immer auf SHA eingestellt, das einzige unterstützte Protokoll (HMAC-SHA-96).
Passwort	Das Kennwort, das dieser Benutzer zur Authentifizierung verwendet.
Datenschutzprotokoll	Wird nur angezeigt, wenn Sie **authPriv** ausgewählt und immer auf AES eingestellt haben, das einzige unterstützte Datenschutzprotokoll.
Passwort	Wird nur angezeigt, wenn Sie **authPriv** ausgewählt haben. Das Passwort, das dieser Benutzer aus Datenschutzgründen verwenden wird.

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-Agenten

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Sehen"Konfigurieren des SNMP-Agenten" für Details zu jedem Feld auf der SNMP-Agent-Seite. Sie müssen unten auf der Seite **Speichern** auswählen, um alle auf den einzelnen Registerkarten vorgenommenen Änderungen zu übernehmen.

Schritte

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

   Die SNMP-Agent-Seite wird angezeigt.

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

   Wenn Sie den SNMP-Agenten erneut aktivieren, bleiben alle vorherigen SNMP-Konfigurationseinstellungen erhalten.

3. Aktualisieren Sie optional die Informationen im Abschnitt „Grundkonfiguration“:
   a. Aktualisieren Sie bei Bedarf den **Systemkontakt** und den **Systemstandort**.
   b. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, 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 **Authentifizierungs-Traps aktivieren**, um zu steuern, ob der StorageGRID SNMP-Agent Authentifizierungs-Traps sendet, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.
4. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren oder fügen Sie optional eine **Nur-Lese-Community** im Abschnitt „Community-Strings“ hinzu.
5. Um Trap-Ziele zu aktualisieren, wählen Sie die Registerkarte Trap-Ziele im Abschnitt „Andere Konfigurationen“ aus.

   Verwenden Sie diese Registerkarte, 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. Für

die unterstützten MIB-II-Entitäten werden auch Standardbenachrichtigungen gesendet (z. B. ifDown und coldStart).

Einzelheiten zu den einzugebenden Informationen finden Sie unter"Erstellen von Trap-Zielen" .

- Aktualisieren oder entfernen Sie optional die Standard-Trap-Community.

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

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

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

   Einzelheiten zu den einzugebenden Informationen finden Sie unter"Agentenadressen erstellen" .

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

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

   Verwenden Sie diese Registerkarte, um die USM-Benutzer zu definieren, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

   Einzelheiten zu den einzugebenden Informationen finden Sie unter"Erstellen von USM-Benutzern" .

   - Um einen USM-Benutzer hinzuzufügen, wählen Sie **Erstellen**.
   - Um einen USM-Benutzer zu bearbeiten, aktivieren Sie das Optionsfeld und wählen Sie **Bearbeiten**.

     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 autoritative Engine-ID eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt beim Speichern der SNMP-Agent-Konfiguration ein Validierungsfehler auf.

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

     > Wenn der von Ihnen entfernte Benutzer derzeit für ein Trap-Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt beim Speichern der SNMP-Agent-Konfiguration ein Validierungsfehler auf.

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

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

Zugriff auf MIB-Dateien

MIB-Dateien enthalten Definitionen und Informationen zu den Eigenschaften verwalteter Ressourcen und Dienste für die Knoten in Ihrem Grid. Sie können auf MIB-Dateien zugreifen, die die Objekte und Benachrichtigungen für StorageGRID definieren. Diese Dateien können für die Überwachung Ihres Netzes nützlich sein.

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

Zugriff auf MIB-Dateien

Befolgen Sie diese Schritte, um auf die MIB-Dateien zuzugreifen.

Schritte

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

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

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

   a. Holen Sie sich die OID des Stammverzeichnisses 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. Suchen Sie im gesamten Baum nach der StorageGRID -OID (mithilfe `paste` zum Verbinden von Zeilen):

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

> Der `snmptranslate` Der Befehl verfügt über viele Optionen, die zum Erkunden der MIB nützlich sind. Dieser Befehl ist auf jedem StorageGRID -Knoten verfügbar.

Inhalt der MIB-Datei

Alle Objekte befinden sich unter der StorageGRID -OID.

Objektname	Objekt-ID (OID)	Beschreibung
		Das MIB-Modul für NetApp StorageGRID Einheiten.

MIB-Objekte

Objektname	Objekt-ID (OID)	Beschreibung
activeAlertCount		Die Anzahl der aktiven Warnungen in der activeAlertTable.
aktiveAlarmtabelle		Eine Tabelle mit aktiven Warnungen in StorageGRID.
aktiveAlertId		Die ID der Warnung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
activeAlertName		Der Name der Warnung.
activeAlertInstance		Der Name der Entität, die die Warnung generiert hat, normalerweise der Knotenname.
activeAlertSeverity		Der Schweregrad der Warnung.
activeAlertStartTime		Datum und Uhrzeit der Auslösung des Alarms.

Benachrichtigungstypen (Traps)

Alle Benachrichtigungen enthalten die folgenden Variablen als Varbinds:

- aktiveAlertId
- activeAlertName
- activeAlertInstance
- activeAlertSeverity
- activeAlertStartTime

Benachrichtigungstyp	Objekt-ID (OID)	Beschreibung
aktiver MinorAlarm		Eine Warnung mit geringem Schweregrad
aktiver MajorAlert		Eine Warnung mit hohem Schweregrad
aktivKritischerAlarm		Eine Warnung mit kritischem Schweregrad