Verwendung von SNMP-Überwachung

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

Verwendung von SNMP-Überwachung

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

- "Konfigurieren des SNMP-Agenten"
- "SNMP-Agent wird aktualisiert"

Sorgen

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine Management Information Base (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.

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** sind Benachrichtigungen, die vom SNMP-Agent gesendet werden, die keine Bestätigung durch das Verwaltungssystem 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** 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 wurde 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 eine Stille für die Warnung konfigurieren. Benachrichtigungen werden von jedem Admin-Node gesendet, der als bevorzugter Absender konfiguriert wurde.
- Bestimmte Alarme (Altsystem) werden mit einem bestimmten Schweregrad oder höher ausgelöst.

  SNMP-Benachrichtigungen werden nicht für jeden Alarm oder jeden Schweregrad 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.

Zugriff auf die MIB

Sie können auf die MIB-Definitionsdatei an der folgenden Stelle auf einem beliebigen StorageGRID-Knoten zugreifen:

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

Verwandte Informationen

"Alerts Referenz"

"Alarmreferenz (Altsystem)"

"Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)"

"Stummschalten von Warnmeldungen"

Konfigurieren des SNMP-Agenten

Sie können den StorageGRID SNMP-Agent konfigurieren, wenn Sie ein Drittanbieter-

SNMP-Verwaltungssystem für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwenden möchten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Der StorageGRID SNMP Agent unterstützt alle drei Versionen des SNMP-Protokolls. Sie können den Agent für eine oder mehrere Versionen konfigurieren.

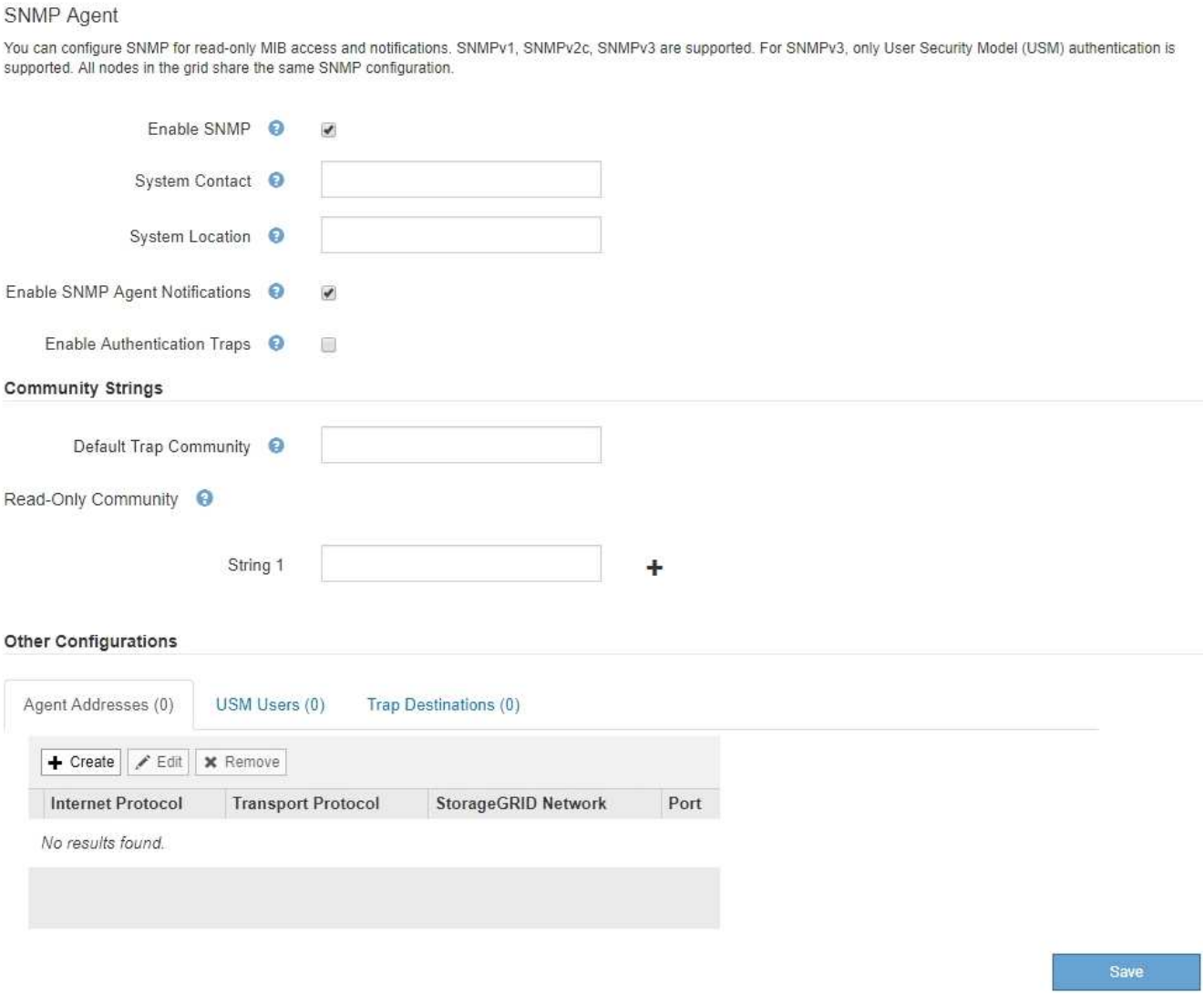
Schritte

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**.

   Die Felder zum Konfigurieren eines SNMP-Agenten werden angezeigt.



3. Geben Sie im Feld **Systemkontakt** den Wert ein, den StorageGRID in SNMP-Nachrichten für sysContact bereitstellen soll.

   Der Systemkontakt ist in der Regel eine E-Mail-Adresse. Der von Ihnen ausliefern Wert gilt für alle Nodes im StorageGRID System. **Systemkontakt** kann maximal 255 Zeichen lang sein.

4. Geben Sie im Feld **Systemstandort** den Wert ein, den StorageGRID in SNMP-Nachrichten für sysLocation bereitstellen soll.

   Der Systemstandort kann alle Informationen sein, die für die Identifizierung des Standortes Ihres StorageGRID-Systems nützlich sind. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Der von Ihnen ausliefern Wert gilt für alle Nodes im StorageGRID System. **Systemposition** kann maximal 255 Zeichen enthalten.

5. Aktivieren Sie das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, wenn der StorageGRID-SNMP-Agent Trap senden und Benachrichtigungen informieren soll.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, unterstützt der SNMP-Agent den schreibgeschützten MIB-Zugriff, aber es sendet keine SNMP-Benachrichtigungen.

6. Aktivieren Sie das Kontrollkästchen **Authentifizierungsfallen aktivieren**, wenn der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap senden soll, wenn er eine nicht ordnungsgemäß authentifizierte

Protokollnachricht empfängt.

7. Wenn Sie SNMPv1 oder SNMPv2c verwenden, füllen Sie den Abschnitt „Gemeinschaftsfolgen“ aus.

   Die Felder in diesem Abschnitt werden für die Community-basierte Authentifizierung in SNMPv1 oder SNMPv2c verwendet. Diese Felder gelten nicht für SNMPv3.

   a. Geben Sie im Feld **Default Trap Community** optional die Standard-Community-Zeichenfolge ein, die Sie für Trap-Ziele verwenden möchten.

      Bei Bedarf können Sie eine andere („`Custom`")-Community-Zeichenfolge angeben Definieren Sie ein bestimmtes Trap-Ziel.

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

   b. Geben Sie für **Read-Only Community** eine oder mehrere Community-Strings ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agent-Adressen zu ermöglichen. Klicken Sie auf das Pluszeichen ➕ Um mehrere Zeichenfolgen hinzuzufügen.

      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.

      Jede Community-Zeichenfolge kann maximal 32 Zeichen enthalten und darf keine Leerzeichen enthalten. Es sind bis zu fünf Zeichenfolgen zulässig.

      ⓘ Verwenden Sie nicht „`public`“ als Community-String, um die Sicherheit Ihres StorageGRID-Systems zu gewährleisten. Wenn Sie keine Community-Zeichenfolge eingeben, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID-Systems als Community-String.

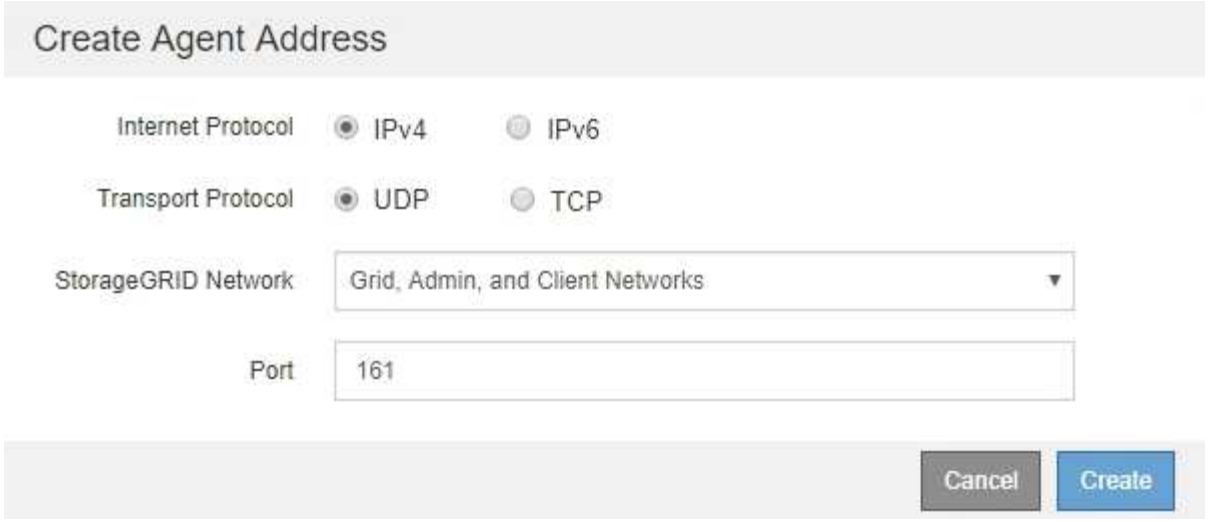
8. Wählen Sie optional im Abschnitt andere Konfigurationen die Registerkarte Agentenadressen aus.

   Verwenden Sie diese Registerkarte, um eine oder mehrere „`Listening-Adressen`“ anzugeben. Dies sind die StorageGRID-Adressen, auf denen der SNMP-Agent Anfragen erhalten kann. Jede Agentenadresse umfasst ein Internetprotokoll, ein Transportprotokoll, ein StorageGRID-Netzwerk und optional einen Port.

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

   a. Klicken Sie Auf **Erstellen**.

      Das Dialogfeld Agentenadresse erstellen wird angezeigt.



b. Wählen Sie für **Internet Protocol** aus, ob diese Adresse IPv4 oder IPv6 verwendet.

   Standardmäßig verwendet SNMP IPv4.

c. Wählen Sie für **Transport Protocol** aus, ob diese Adresse UDP oder TCP verwenden soll.

   Standardmäßig verwendet SNMP UDP.

d. Wählen Sie im Feld **StorageGRID-Netzwerk** das StorageGRID-Netzwerk aus, auf dem die Abfrage empfangen wird.

   - Grid-, Admin- und Client-Netzwerke: StorageGRID sollte SNMP-Abfragen in allen drei Netzwerken abhören.
   - Grid-Netzwerk
   - Admin-Netzwerk
   - Client-Netzwerk

   > Um sicherzustellen, dass die Clientkommunikation mit StorageGRID sicher bleibt, sollten Sie keine Agentenadresse für das Clientnetzwerk erstellen.

e. Geben Sie im Feld **Port** optional die Portnummer ein, die der SNMP-Agent anhören soll.

   Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch alle nicht verwendeten Portnummern eingeben.

   > Wenn Sie den SNMP-Agent speichern, öffnet StorageGRID automatisch die Agent-Adressen-Ports in der internen Firewall. Sie müssen sicherstellen, dass alle externen Firewalls den Zugriff auf diese Ports zulassen.

f. Klicken Sie Auf **Erstellen**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

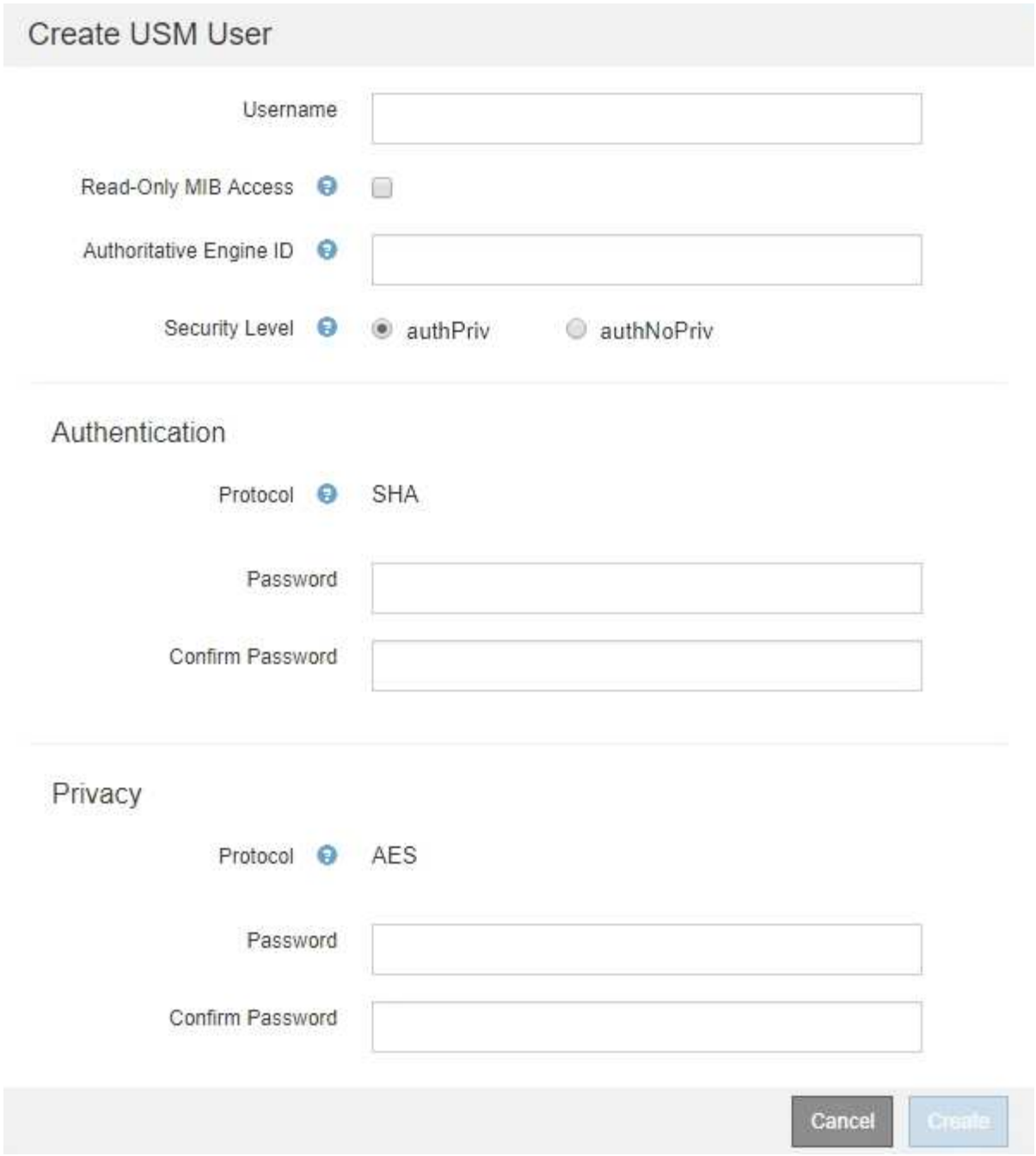
9. Wenn Sie SNMPv3 verwenden, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

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

   Dieser Schritt gilt nicht, wenn Sie nur SNMPv1 oder SNMPv2c verwenden.

   a. Klicken Sie Auf **Erstellen**.

      Das Dialogfeld USM-Benutzer erstellen wird angezeigt.



b. Geben Sie einen eindeutigen **Benutzername** für diesen USM-Benutzer ein.

   Benutzernamen haben maximal 32 Zeichen und können keine Leerzeichen enthalten. Der Benutzername kann nach dem Erstellen des Benutzers nicht geändert werden.

c. Aktivieren Sie das Kontrollkästchen **schreibgeschütztes MIB Access**, wenn dieser Benutzer nur Lesezugriff auf die MIB haben soll.

   Wenn Sie **schreibgeschütztes MIB Access** auswählen, ist das Feld **autoritative Engine ID** deaktiviert.

   USM-Benutzer mit schreibgeschütztem MIB-Zugriff können keine Engine-IDs haben.

d. Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, geben Sie die **autoritative Engine-ID** für

diesen Benutzer ein.

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

Die autoritative Engine-ID kann zwischen 5 und 32 Byte hexadezimal sein.

e. Wählen Sie eine Sicherheitsstufe für den USM-Benutzer aus.
   - **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.

f. Geben Sie das Passwort ein, das dieser Benutzer zur Authentifizierung verwenden soll, und bestätigen Sie es.

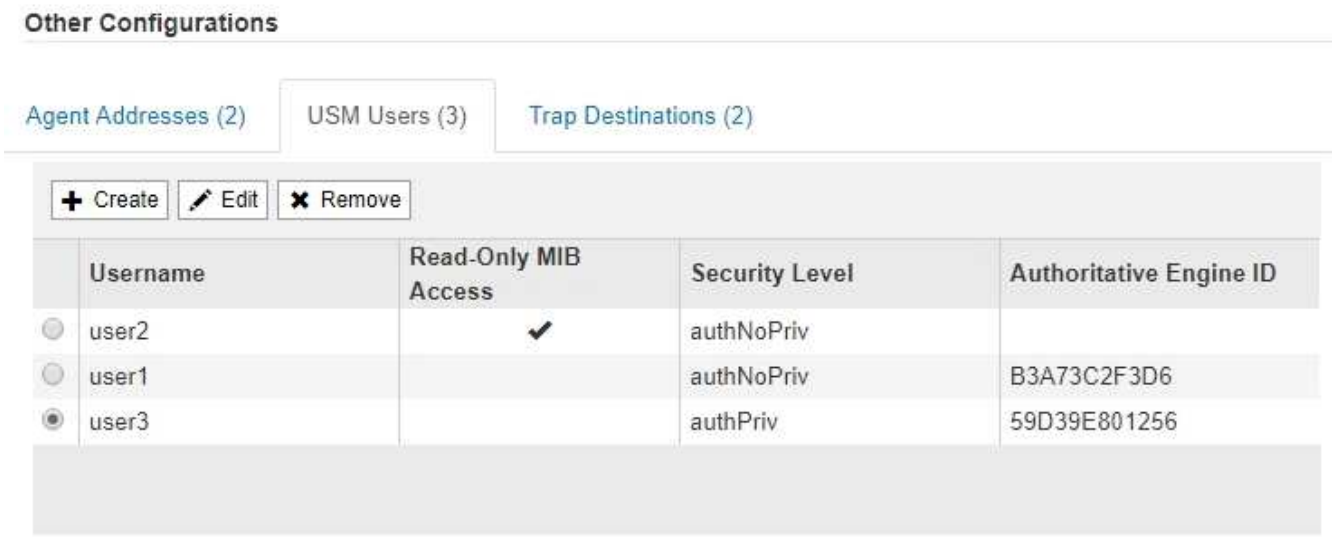
> Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).

g. Wenn Sie **authPriv** ausgewählt haben, geben Sie das Passwort ein und bestätigen Sie es.

> Das einzige unterstützte Datenschutzprotokoll ist AES.

h. Klicken Sie Auf **Erstellen**.

Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

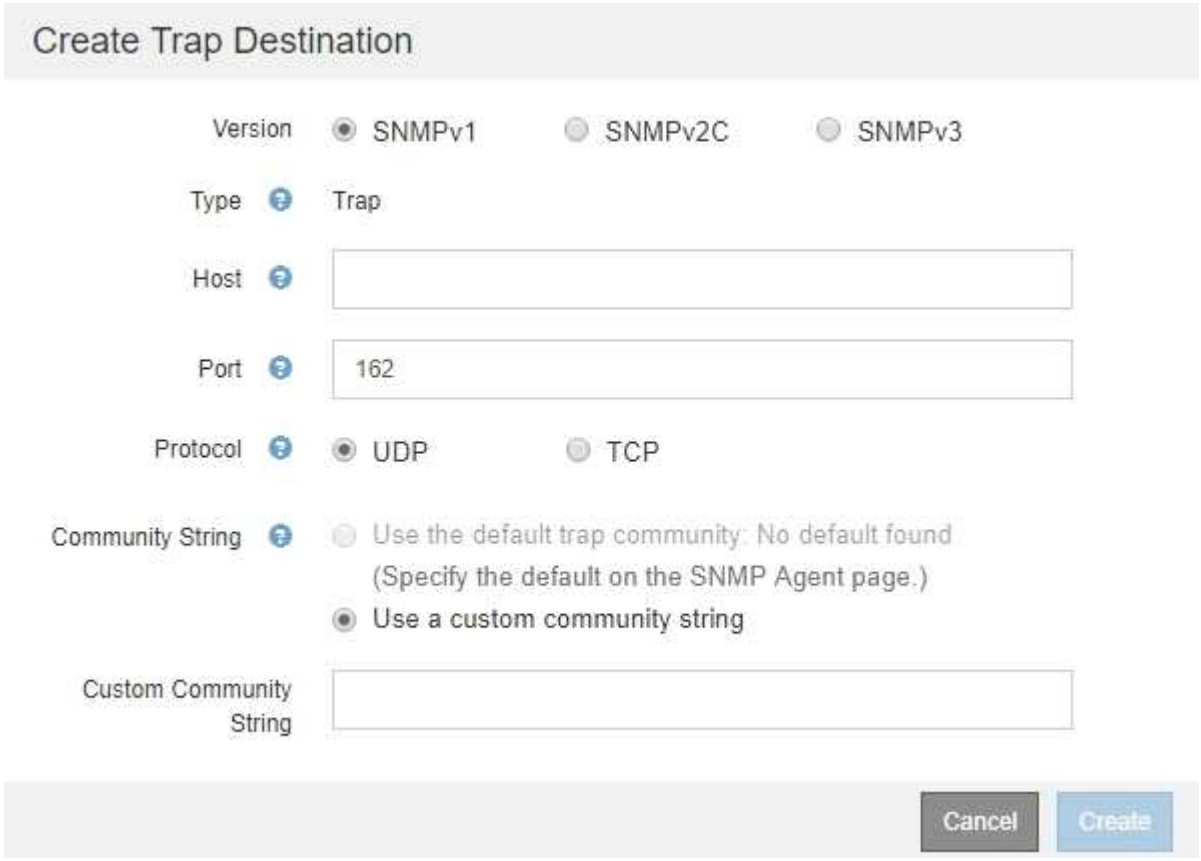


10. Wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Trap-Ziele aus.

Auf der Registerkarte Trap-Ziele können Sie ein oder mehrere Ziele für StorageGRID-Trap definieren oder Benachrichtigungen informieren. Wenn Sie den SNMP-Agent aktivieren und auf **Speichern** klicken, beginnt StorageGRID mit dem Senden von Benachrichtigungen an jedes definierte Ziel. Benachrichtigungen werden gesendet, wenn Warnungen und Alarme ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

a. Klicken Sie Auf **Erstellen**.

   Das Dialogfeld Trap-Ziel erstellen wird angezeigt.



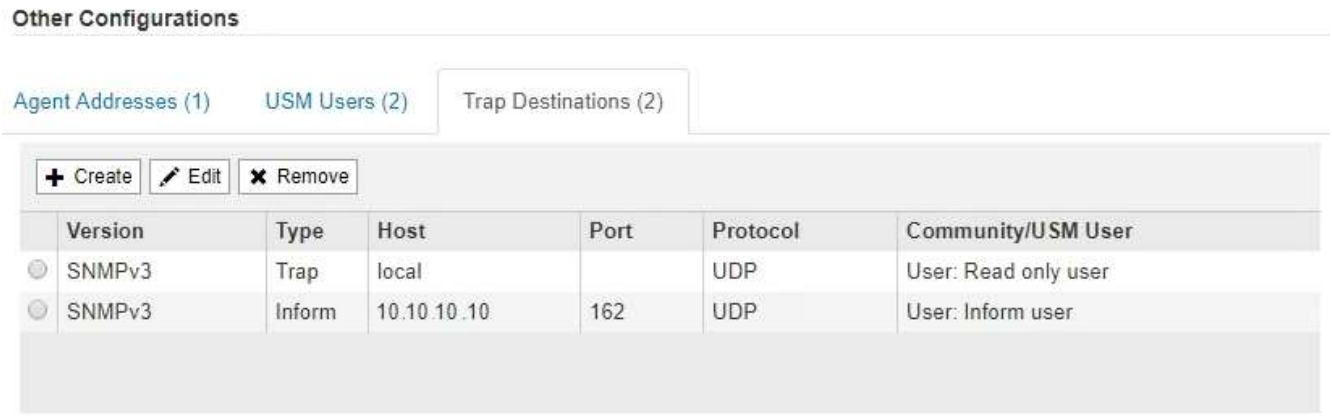
b. Wählen Sie im Feld **Version** die SNMP-Version für diese Benachrichtigung aus.
c. Füllen Sie das Formular aus, basierend auf der ausgewählten Version

Version	Geben Sie diese Informationen an
SNMPv1	**Hinweis:** für SNMPv1 kann der SNMP-Agent nur Traps senden. Informationen werden nicht unterstützt. i. Geben Sie im Feld **Host** eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. ii. Verwenden Sie für **Port** den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iii. Verwenden Sie für **Protokoll** den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) iv. Verwenden Sie die Standard-Trap-Community, wenn eine auf der Seite SNMP Agent angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.
SNMPv2c	i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird. ii. Geben Sie im Feld **Host** eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. iii. Verwenden Sie für **Port** den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iv. Verwenden Sie für **Protokoll** den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) v. Verwenden Sie die Standard-Trap-Community, wenn eine auf der Seite SNMP Agent angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.

Version	Geben Sie diese Informationen an
SNMPv3	i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird. ii. Geben Sie im Feld **Host** eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. iii. Verwenden Sie für **Port** den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iv. Verwenden Sie für **Protokoll** den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) v. Wählen Sie den USM-Benutzer aus, der zur Authentifizierung verwendet werden soll. ◦ 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.

d. Klicken Sie Auf **Erstellen**.

   Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.



11. Wenn Sie die SNMP-Agent-Konfiguration abgeschlossen haben, klicken Sie auf **Speichern**

    Die neue SNMP-Agent-Konfiguration wird aktiv.

Verwandte Informationen

"Stummschalten von Warnmeldungen"

SNMP-Agent wird aktualisiert

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Immer wenn Sie die SNMP-Agent-Konfiguration aktualisieren, müssen Sie auf der Seite SNMP-Agent auf **Speichern** klicken, um alle Änderungen zu speichern, die Sie auf jeder Registerkarte vorgenommen haben.

Schritte

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

   Die Seite SNMP-Agent wird angezeigt.

2. Wenn Sie den SNMP-Agent auf allen Grid-Knoten deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **SNMP aktivieren** und klicken Sie auf **Speichern**.

   Der SNMP-Agent ist für alle Grid-Knoten deaktiviert. Wenn Sie den Agent später wieder aktivieren, werden alle vorherigen SNMP-Konfigurationseinstellungen beibehalten.

3. Aktualisieren Sie optional die Werte, die Sie für **Systemkontakt** und **Systemstandort** eingegeben haben.
4. Deaktivieren Sie optional das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, wenn der StorageGRID-SNMP-Agent nicht mehr Trap senden und Benachrichtigungen informieren soll.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, unterstützt der SNMP-Agent den schreibgeschützten MIB-Zugriff, aber es sendet keine SNMP-Benachrichtigungen.

5. Deaktivieren Sie optional das Kontrollkästchen **Authentifizierungsfallen aktivieren**, wenn Sie nicht mehr möchten, dass der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap sendet, wenn er eine nicht ordnungsgemäß authentifizierte Protokollnachricht empfängt.
6. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren Sie optional den Abschnitt Community Strings.

   Die Felder in diesem Abschnitt werden für die Community-basierte Authentifizierung in SNMPv1 oder SNMPv2c verwendet. Diese Felder gelten nicht für SNMPv3.

   > Wenn Sie den Standard-Community-String entfernen möchten, müssen Sie zunächst sicherstellen, dass alle Trap-Ziele eine benutzerdefinierte Community-Zeichenfolge verwenden.

7. Wenn Sie Agentenadressen aktualisieren möchten, wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Agentenadressen aus.

Verwenden Sie diese Registerkarte, um eine oder mehrere „`Listening-Adressen`“ anzugeben. Dies sind die StorageGRID-Adressen, auf denen der SNMP-Agent Anfragen erhalten kann. Jede Agentenadresse umfasst ein Internetprotokoll, ein Transportprotokoll, ein StorageGRID-Netzwerk und einen Port.

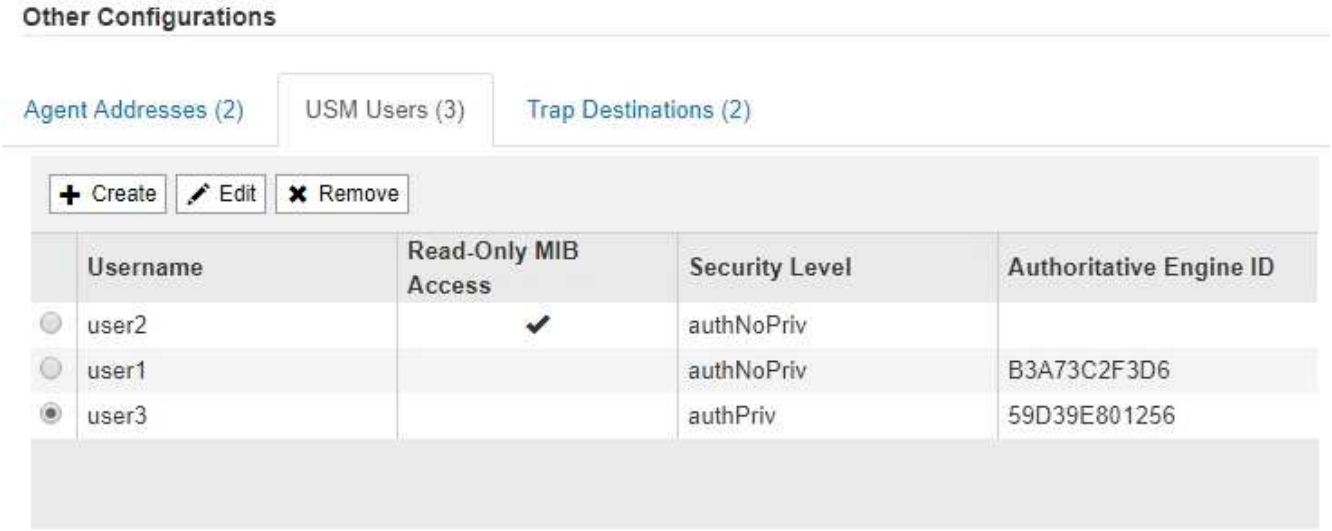
a. Um eine Agentenadresse hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.

b. Um eine Agentenadresse zu bearbeiten, aktivieren Sie das Optionsfeld für die Adresse und klicken auf **Bearbeiten**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.

c. Um eine Agentenadresse zu entfernen, wählen Sie das Optionsfeld für die Adresse aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie diese Adresse entfernen möchten.

d. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

8. Wenn Sie USM-Benutzer aktualisieren möchten, 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.

a. Um einen USM-Benutzer hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für USM-

Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.

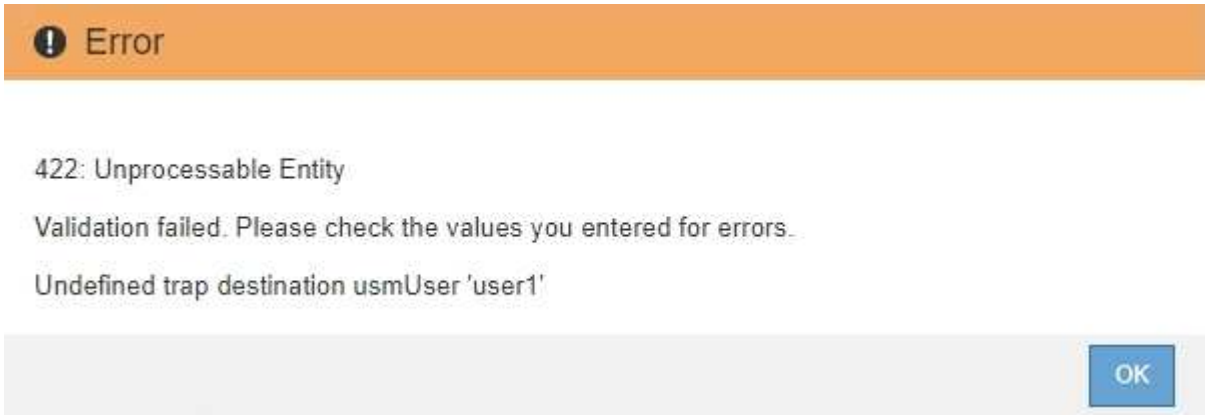
b. Um einen USM-Benutzer zu bearbeiten, wählen Sie das Optionsfeld für den Benutzer aus, und klicken Sie auf **Bearbeiten**. Lesen Sie dann den Schritt für USM-Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.

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

   Wenn Sie die autorisierende Engine-ID eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen, wie in Schritt beschrieben SNMP-Trap-Ziel. Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

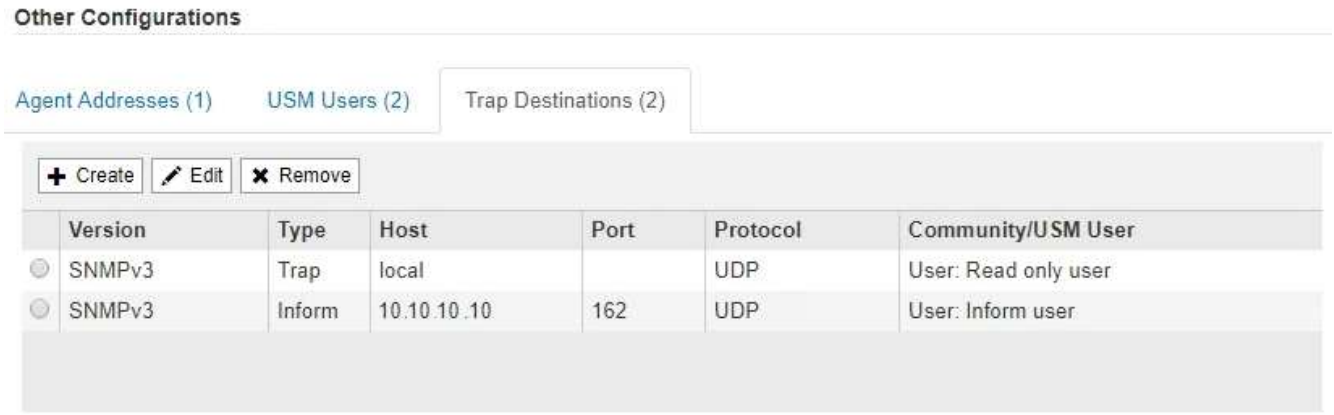
c. Um einen USM-Benutzer zu entfernen, wählen Sie das Optionsfeld für den Benutzer aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie diesen Benutzer entfernen möchten.

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



a. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

1. Wenn Sie Trap-Ziele aktualisieren möchten, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte Trap-Ziele aus.



Auf der Registerkarte Trap-Ziele können Sie ein oder mehrere Ziele für StorageGRID-Trap definieren oder Benachrichtigungen informieren. Wenn Sie den SNMP-Agent aktivieren und auf **Speichern** klicken, beginnt StorageGRID mit dem Senden von Benachrichtigungen an jedes definierte Ziel. Benachrichtigungen werden gesendet, wenn Warnungen und Alarme ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

a. Um ein Trap-Ziel hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
b. Um ein Trap-Ziel zu bearbeiten, wählen Sie das Optionsfeld für den Benutzer aus und klicken auf **Bearbeiten**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
c. Um ein Trap-Ziel zu entfernen, wählen Sie das Optionsfeld für das Ziel aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie dieses Ziel entfernen möchten.
d. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

2. Wenn Sie die SNMP-Agent-Konfiguration aktualisiert haben, klicken Sie auf **Speichern**.

Verwandte Informationen

"Konfigurieren des SNMP-Agenten"