



# **Verwenden Sie SNMP-Überwachung**

## **StorageGRID 11.7**

NetApp  
April 12, 2024

# Inhalt

- Verwenden Sie SNMP-Überwachung ..... 1
  - Verwenden Sie SNMP-Überwachung: Übersicht ..... 1
  - Konfigurieren Sie den SNMP-Agent ..... 2
  - Aktualisieren Sie den SNMP-Agent ..... 12
  - Zugriff auf MIB-Dateien ..... 15

# 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 Alarmer 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** 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** 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. 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"](#).

- Bestimmte Alarme (Altsystem) werden mit einem bestimmten Schweregrad oder höher 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.

### Verwandte Informationen

- ["Alerts Referenz"](#)
- ["Alarmreferenz \(Altsystem\)"](#)
- ["Benachrichtigung über Stille"](#)

## Konfigurieren Sie den SNMP-Agent

Sie können den StorageGRID SNMP-Agent konfigurieren, wenn Sie ein Drittanbieter-SNMP-Verwaltungssystem für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwenden möchten.

### Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

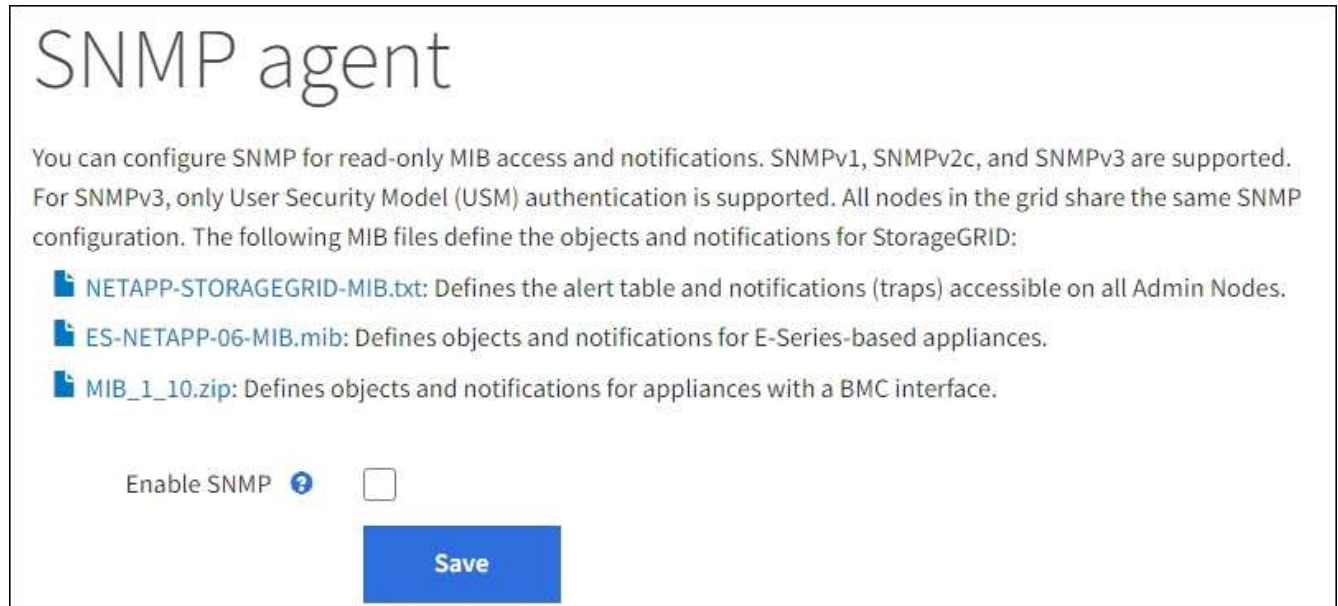
### Über diese Aufgabe

Der StorageGRID SNMP Agent unterstützt 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.



The screenshot shows the 'SNMP agent' configuration page. At the top, the title 'SNMP agent' is displayed in a large font. Below the title, there is a paragraph of text: 'You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, and SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration. The following MIB files define the objects and notifications for StorageGRID:'. Below this text, there are three entries, each with a small blue icon of a document and a file name: 'NETAPP-STORAGEGRID-MIB.txt: Defines the alert table and notifications (traps) accessible on all Admin Nodes.', 'ES-NETAPP-06-MIB.mib: Defines objects and notifications for E-Series-based appliances.', and 'MIB\_1\_10.zip: Defines objects and notifications for appliances with a BMC interface.'. At the bottom of the page, there is a label 'Enable SNMP' followed by a question mark icon and an unchecked checkbox. Below the checkbox is a blue 'Save' button.

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.

Enable SNMP ?

System Contact ?

System Location ?

Enable SNMP Agent Notifications ?

Enable Authentication Traps ?

### Community Strings

Default Trap Community ?

Read-Only Community ?

String 1  +

### Other Configurations

Agent Addresses (0)    USM Users (0)    Trap Destinations (0)

+ Create   Edit   Remove

Internet Protocol	Transport Protocol	StorageGRID Network	Port
No results found			

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 ausliefernde 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 auslieferte Wert gilt für alle Nodes im StorageGRID System. **Systemposition** kann maximal 255 Zeichen enthalten.

5. Lassen Sie das Kontrollkästchen **SNMP-Agentenbenachrichtigungen aktivieren** aktiviert, wenn der StorageGRID SNMP-Agent Trap- und Benachrichtigungen senden soll.

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

6. Aktivieren Sie das Kontrollkästchen **Authentifizierungs-Traps aktivieren**, wenn der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap senden soll, wenn er eine nicht ordnungsgemäß authentifizierte Protokollnachricht erhält.
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](#).

**Default Trap Community** darf 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. Wählen Sie das Pluszeichen aus **+** 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 darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten. Es sind bis zu fünf Zeichenfolgen zulässig.



Um die Sicherheit Ihres StorageGRID-Systems zu gewährleisten, verwenden Sie „public“ nicht als Community-String. 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 Abhöradresse in allen StorageGRID-Netzwerken UDP-Port 161.

- a. Wählen Sie **Erstellen**.

Das Dialogfeld Agentenadresse erstellen wird angezeigt.

# Create Agent Address

Internet Protocol  IPv4  IPv6

Transport Protocol  UDP  TCP

StorageGRID Network

Port

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. Wählen Sie **Erstellen**.

Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

#### Other Configurations

Agent Addresses (2)    USM Users (2)    Trap Destinations (2)

**+ Create**   **Edit**   **Remove**

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

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. Wählen Sie **Erstellen**.


Das Dialogfeld USM-Benutzer erstellen wird angezeigt.

# Create USM User

Username 


Read-Only MIB Access 

Authoritative Engine ID 

Security Level   authPriv  authNoPriv

---

Authentication


Protocol  SHA

Password

Confirm Password

---

Privacy

Protocol  AES

Password

Confirm Password

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

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

c. Aktivieren Sie das Kontrollkästchen **schreibgeschützter MIB-Zugriff**, wenn dieser Benutzer schreibgeschützten Zugriff 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. Das 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. Wählen Sie **Erstellen**.

Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

### Other Configurations

Agent Addresses (2)

USM Users (3)

Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	✓	authNoPriv	
<input type="radio"/>	user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3		authPriv	59D39E801256

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-Agenten aktivieren und **Speichern** auswählen,

sendet StorageGRID Benachrichtigungen an jedes definierte Ziel. Benachrichtigungen werden gesendet, wenn Warnungen ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

a. Wählen Sie **Erstellen**.

Das Dialogfeld Trap-Ziel erstellen wird angezeigt.

**Create Trap Destination**

Version  SNMPv1  SNMPv2C  SNMPv3

Type  Trap

Host

Port

Protocol   UDP  TCP

Community String   Use the default trap community: No default found (Specify the default on the SNMP Agent page.)

Use a custom community string

Custom Community String

a. Wählen Sie im Feld **Version** die SNMP-Version für diese Benachrichtigung aus.

b. Füllen Sie das Formular aus, basierend auf der ausgewählten Version

Version	Geben Sie diese Informationen an
<p>SNMPv1</p> <p>(Bei SNMPv1 kann der SNMP-Agent nur Traps senden. Informationen werden nicht unterstützt.)</p>	<ul style="list-style-type: none"> <li>i. Geben Sie im Feld <b>Host</b> eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen.</li> <li>ii. Verwenden Sie für <b>Port</b> den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.)</li> <li>iii. Verwenden Sie für <b>Protokoll</b> den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.)</li> <li>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.</li> </ul> <p>Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.</p>
<p>SNMPv2c</p>	<ul style="list-style-type: none"> <li>i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird.</li> <li>ii. Geben Sie im Feld <b>Host</b> eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen.</li> <li>iii. Verwenden Sie für <b>Port</b> den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.)</li> <li>iv. Verwenden Sie für <b>Protokoll</b> den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.)</li> <li>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.</li> </ul> <p>Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.</p>

Version	Geben Sie diese Informationen an
SNMPv3	<ul style="list-style-type: none"> <li>i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird.</li> <li>ii. Geben Sie im Feld <b>Host</b> eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen.</li> <li>iii. Verwenden Sie für <b>Port</b> den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.)</li> <li>iv. Verwenden Sie für <b>Protokoll</b> den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.)</li> <li>v. Wählen Sie den USM-Benutzer aus, der zur Authentifizierung verwendet werden soll. <ul style="list-style-type: none"> <li>◦ Wenn Sie <b>Trap</b> ausgewählt haben, werden nur USM-Benutzer ohne maßgebliche Engine-IDs angezeigt.</li> <li>◦ Wenn Sie <b>Inform</b> ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt.</li> </ul> </li> </ul>

c. Wählen Sie **Erstellen**.

Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

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

Die neue SNMP-Agent-Konfiguration wird aktiv.

#### Verwandte Informationen

["Benachrichtigung über Stille"](#)

## 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 müssen mit einem beim Grid Manager angemeldet sein ["Unterstützter Webbrowser"](#).
- Sie müssen über die Root-Zugriffsberechtigung verfügen.

#### Über diese Aufgabe

Jedes Mal, wenn Sie den aktualisieren ["SNMP-Agent-Konfiguration"](#) Beachten Sie, dass Sie unten auf der SNMP Agent-Seite **Speichern** auswählen müssen, um alle Änderungen zu übernehmen, 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 wählen Sie **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-Agentenbenachrichtigungen aktivieren**, wenn Sie nicht mehr möchten, dass der StorageGRID SNMP-Agent Trap- und Benachrichtigungen sendet.

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

5. Deaktivieren Sie optional das Kontrollkästchen **Enable Authentication Traps**, wenn Sie nicht mehr möchten, dass der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap sendet, wenn er eine falsch 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.

### Other Configurations

Agent Addresses (2)
USM Users (2)
Trap Destinations (2)

+ Create
✎ Edit
✕ Remove

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

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, wählen Sie **Create**. 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 wählen **Bearbeiten**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des

SNMP-Agenten.

- c. Um eine Agentenadresse zu entfernen, aktivieren Sie das Optionsfeld für die Adresse und wählen **Entfernen** aus. Wählen Sie dann **OK**, um zu bestätigen, dass Sie diese Adresse entfernen möchten.
  - d. Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der SNMP Agent-Seite aus.
8. Wenn Sie USM-Benutzer aktualisieren möchten, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

### Other Configurations

Agent Addresses (2)    USM Users (3)    Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	✓	authNoPriv	
<input type="radio"/>	user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3		authPriv	59D39E801256

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

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 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.

- a. Um einen USM-Benutzer zu entfernen, aktivieren Sie das Optionsfeld für den Benutzer und wählen Sie **Entfernen** aus. Wählen Sie dann **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.

- b. Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der SNMP Agent-Seite aus.
9. Wenn Sie Trap-Ziele aktualisieren möchten, 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-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID 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, wählen Sie **Create**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
  - b. Um ein Trap-Ziel zu bearbeiten, aktivieren Sie das Optionsfeld für den Benutzer und wählen **Bearbeiten**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
  - c. Um ein Trap-Ziel zu entfernen, aktivieren Sie das Optionsfeld für das Ziel und wählen Sie **Entfernen** aus. Wählen Sie dann **OK**, um zu bestätigen, dass Sie dieses Ziel entfernen möchten.
  - d. Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der SNMP Agent-Seite aus.
10. 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

### 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.
3. Optional können Sie auf MIB-Dateien am folgenden Speicherort auf einem beliebigen StorageGRID-Knoten zugreifen: `/usr/share/snmp/mibs`
4. Um den zu extrahieren `storagegrid` OIDs aus der MIB-Datei:
  - a. Erhalten Sie die OID des Stamms der StorageGRID MIB:

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

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

- a. Grüße dann für die StorageGRID-OID in der gesamten Struktur (mit Einfügen, um Linien zu verbinden):

```
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
		Das MIB-Modul für NetApp StorageGRID Entities.

## MIB-Objekte

Objektname	Objekt-ID (OID)	Beschreibung
ActiveAlertCount		Die Anzahl der aktiven Warnungen in der activeAlertTable.
ActiveAlertTable		Eine Tabelle mit aktiven Warnmeldungen in StorageGRID.
ActiveAlertId		Die ID der Warnmeldung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
ActiveAlertName		Der Name der Warnmeldung.
ActiveAlertInstance		Der Name der Entität, die die Warnmeldung generiert hat, normalerweise der Knotenname.
ActiveAlertSchweregrad		Der Schweregrad der Meldung.
ActiveAlertStartTime		Datum und Uhrzeit der Auslösung der Warnmeldung.

## Benachrichtigungstypen (Traps)

Alle Benachrichtigungen enthalten die folgenden Variablen als verbindendes:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSchweregrad
- ActiveAlertStartTime

<b>Benachrichtigungstyp</b>	<b>Objekt-ID (OID)</b>	<b>Beschreibung</b>
ActiveMinorAlert		Ein Alarm mit geringem Schweregrad
ActiveMajorAlert		Ein Alarm mit dem Hauptschweregrad
ActiveCriticalAlert		Eine Meldung mit dem Schweregrad „kritisch“

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.