



# SNMP による監視を使用する StorageGRID 11.7

NetApp  
April 12, 2024

# 目次

SNMP による監視を使用する .....	1
SNMP監視の使用：概要 .....	1
SNMP エージェントを設定します .....	2
SNMP エージェントを更新します .....	12
MIBファイルにアクセスします .....	15

# SNMP による監視を使用する

## SNMP監視の使用：概要

簡易ネットワーク管理プロトコル（SNMP）を使用して StorageGRID を監視する場合は、StorageGRID に含まれる SNMP エージェントを設定する必要があります。

- ["SNMP エージェントを設定します"](#)
- ["SNMP エージェントを更新します"](#)

### 機能

各StorageGRID ノードは、MIBを提供するSNMPエージェント（デーモン）を実行します。StorageGRID の MIB には、アラートおよびアラームのテーブルおよび通知定義が含まれています。この MIB には、各ノードのプラットフォームやモデル番号など、システムの概要 情報も含まれています。各 StorageGRID ノードは MIB-II オブジェクトのサブセットもサポートしています。



を参照してください ["MIBファイルにアクセスします"](#) グリッドノードにMIBファイルをダウンロードする場合。

最初は、すべてのノードで SNMP が無効になっています。SNMP エージェントを設定すると、すべての StorageGRID ノードに同じ設定が適用されます。

StorageGRID SNMP エージェントは、3 つのバージョンの SNMP プロトコルをすべてサポートします。クエリに読み取り専用 MIB アクセスを提供し、次の 2 種類のイベントベース通知を管理システムに送信できます。

- \*トラップ\*は、管理システムによる確認応答を必要としないSNMPエージェントによって送信される通知です。トラップは、アラートがトリガーされているなど、StorageGRID 内で何らかの問題が発生したことを管理システムに通知するために使用されます。

トラップは、SNMP の 3 つのバージョンすべてでサポートされています。

- \* informs \* はトラップに似ていますが、管理システムからの確認応答が必要です。SNMP エージェントが一定時間内に確認応答を受信しなかった場合、確認応答を受信するか、最大再試行値に達するまで、通知を再送信します。

インフォームは SNMPv2c および SNMPv3 でサポートされます。

トラップ通知およびインフォーム通知は、次の場合に送信されます。

- デフォルトまたはカスタムのアラートはいずれかの重大度レベルでトリガーされます。アラートの SNMP 通知を停止するには、アラートのサイレンスを設定する必要があります。アラート通知はから送信されず ["優先送信者管理ノード"](#)。

各アラートは、アラートの重大度レベルに基づいて、activeMinorAlert、activeMajorAlert、および activeCriticalAlert の 3 つのトラップタイプのいずれかにマッピングされます。これらのトラップをトリガーできるアラートのリストについては、[を参照してください "アラート一覧"](#)。

- 特定のアラーム（従来型システム）は、指定した重大度レベル以上でトリガーされます。



SNMP通知は、すべてのアラームまたはすべての重大度について送信されるわけではありません。

## SNMP バージョンサポート

次の表に、各 SNMP バージョンでサポートされる内容の概要を示します。

	SNMPv1	SNMPv2c の場合	SNMPv3
クエリ	読み取り専用 MIB クエリ	読み取り専用 MIB クエリ	読み取り専用 MIB クエリ
クエリ認証	コミュニティストリング	コミュニティストリング	ユーザベースのセキュリティモデル（USM）ユーザ
通知	トラップのみ	トラップおよびインフォーム	トラップおよびインフォーム
通知認証	トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します	トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します	トラップの送信先ごとの USM ユーザ

## 制限

- StorageGRID は、読み取り専用 MIB アクセスをサポートしています。読み取り / 書き込みアクセスはサポートされていません。
- グリッド内のすべてのノードが同じ設定を受信します。
- SNMPv3 : StorageGRID は TSM（Transport Support Mode）をサポートしていません。
- SNMPv3 : SHA（HMAC-SHA-96）だけがサポートされています。
- SNMPv3 : AES のみがサポートされています。

## 関連情報

- ["アラート一覧"](#)
- ["アラーム一覧（従来のシステム）"](#)
- ["アラート通知をサイレント化する"](#)

## SNMP エージェントを設定します

読み取り専用 MIB アクセスおよび通知にサードパーティ製 SNMP 管理システムを使用する場合は、StorageGRID SNMP エージェントを設定できます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- Root アクセス権限が割り当てられている。

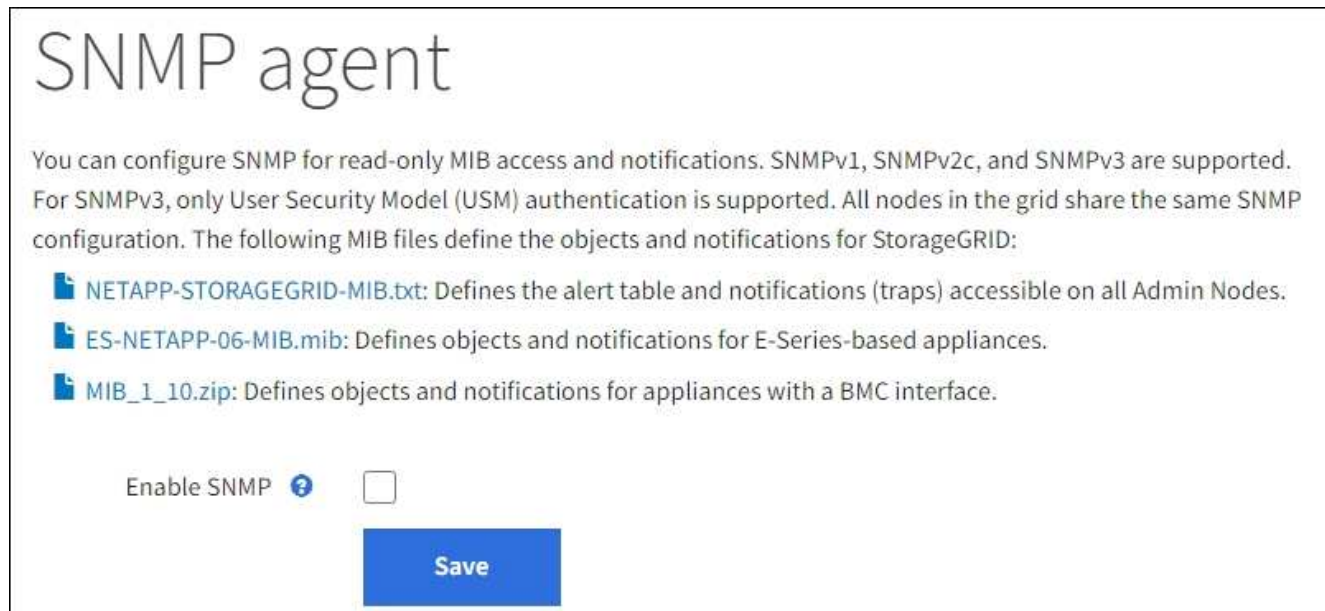
このタスクについて

StorageGRID SNMP エージェントは、3つのバージョンの SNMP プロトコルをすべてサポートします。エージェントは1つ以上のバージョンに設定できます。

手順

1. \* configuration \* > \* Monitoring \* > \* SNMP agent \* を選択します。

SNMP Agent ページが表示されます。



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 list items, each with a blue folder icon: '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 blue question mark icon and an unchecked checkbox. Below the checkbox is a blue 'Save' button.

2. すべてのグリッドノードでSNMPエージェントを有効にするには、\*[SNMPを有効にする]\*チェックボックスを選択します。

SNMP エージェントを設定するためのフィールドが表示されます。

The screenshot shows the configuration page for SNMP. It includes several sections:

- Enable SNMP**: A checkbox that is checked.
- System Contact**: An empty text input field.
- System Location**: An empty text input field.
- Enable SNMP Agent Notifications**: A checkbox that is checked.
- Enable Authentication Traps**: An unchecked checkbox.
- Community Strings**: A section containing:
  - Default Trap Community**: An empty text input field.
  - Read-Only Community**: A label with a help icon.
  - String 1**: An empty text input field with a plus sign (+) to its right, indicating it can be added to a list.
- Other Configurations**: A section with three tabs: **Agent Addresses (0)**, **USM Users (0)**, and **Trap Destinations (0)**. Below the tabs are three buttons: **+ Create**, **Edit**, and **Remove**. A table is shown below the buttons with the following headers: **Internet Protocol**, **Transport Protocol**, **StorageGRID Network**, and **Port**. The table is currently empty, with the text **No results found** centered at the bottom.

3. **System Contact** フィールドに、 sysContact の SNMP メッセージで StorageGRID が提供する値を入力します。

システムの連絡先は通常、電子メールアドレスです。StorageGRID システムで環境 のすべてのノードを指定する値。\* システム連絡先 \* は最大 255 文字です。

4. [システムロケーション\*] フィールドに、 StorageGRID が sysLocation の SNMP メッセージに提供する値を入力します。

システムの場所は、 StorageGRID システムの場所を特定するのに役立つ情報で、任意に指定できます。

たとえば、施設の住所を使用できます。StorageGRID システムで環境 のすべてのノードを指定する値。\* システムの場所 \* は最大 255 文字です。

- StorageGRID SNMPエージェントでトラップおよびインフォーム通知を送信する場合は、[SNMPエージェント通知を有効にする]チェックボックスをオンのままにします。

このチェックボックスをオフにすると、SNMPエージェントは読み取り専用のMIBアクセスをサポートしますが、SNMP通知は送信しません。

- 認証が正しくないプロトコルメッセージを受信した場合にStorageGRID SNMPエージェントが認証トラップを送信するようにするには、\*認証トラップを有効にする\*チェックボックスをオンにします。
- SNMPv1 または SNMPv2c を使用する場合は、コミュニティストリングセクションに必要な事項を記入します。

このセクションのフィールドは、SNMPv1 または SNMPv2c でのコミュニティベースの認証に使用されます。これらのフィールドはSNMPv3には適用されません。

- [デフォルトトラップコミュニティ \*] フィールドに、トラップ送信先に使用するデフォルトのコミュニティストリングを任意で入力します。

必要に応じて '別の (カスタム) コミュニティ文字列を指定できます [特定のトラップ送信先を定義します](#)。

\*デフォルトトラップコミュニティ\*は最大32文字で、空白文字は使用できません。

- \*読み取り専用コミュニティ\* には、1 つ以上のコミュニティストリングを入力して、IPv4 および IPv6 エージェントアドレスでの読み取り専用 MIB アクセスを許可します。プラス記号を選択します **+** 複数の文字列を追加します。

管理システムが StorageGRID MIB を照会すると、コミュニティストリングが送信されます。コミュニティストリングがここで指定した値のいずれかと一致すると、SNMP エージェントは管理システムに応答を送信します。

各コミュニティストリングの最大文字数は32文字で、空白文字は使用できません。最大 5 つの文字列を指定できます。



StorageGRID システムのセキュリティを確保するために、コミュニティストリングとして "public" を使用しないでください。コミュニティストリングを入力しない場合、SNMP エージェントは StorageGRID システムのグリッド ID をコミュニティストリングとして使用します。

- 必要に応じて、Other Configurations セクションの Agent Addresses タブを選択します。

このタブを使用して '1 つまたは複数の "リスニング・アドレス" を指定します これらは、SNMP エージェントがクエリを受信できる StorageGRID アドレスです。各エージェントアドレスには、インターネットプロトコル、転送プロトコル、StorageGRID ネットワーク、およびオプションでポートが含まれません。

エージェントアドレスを設定しない場合、デフォルトのリスニングアドレスはすべてのStorageGRID ネットワークのUDPポート161です。

- 「\* Create \*」を選択します。

Create Agent Address ダイアログボックスが表示されます。

- b. インターネットプロトコル \* の場合は、このアドレスに IPv4 と IPv6 のどちらを使用するかを選択します。

デフォルトでは、SNMP は IPv4 を使用します。

- c. [\*Transport Protocol] には、このアドレスで UDP と TCP のどちらを使用するかを選択します。

デフォルトでは、SNMP は UDP を使用します。

- d. StorageGRID Network\*] フィールドで、クエリーを受信する StorageGRID ネットワークを選択します。

- グリッドネットワーク、管理ネットワーク、クライアントネットワーク：StorageGRID は、3つのネットワークすべてで SNMP クエリーをリスンする必要があります。
- Grid ネットワーク
- 管理ネットワーク
- クライアントネットワーク



StorageGRID とのクライアント通信のセキュリティを確保するために、クライアントネットワーク用のエージェントアドレスを作成しないでください。

- e. [Port] フィールドには、オプションで、SNMP エージェントがリスンするポート番号を入力します。



SNMP エージェントのデフォルトの UDP ポートは 161 ですが、未使用のポート番号は任意に入力できます。



SNMP エージェントを保存すると、StorageGRID によって内部ファイアウォールのエージェントアドレスポートが自動的に開きます。これらのポートへのアクセスが外部ファイアウォールで許可されていることを確認してください。

- f. 「\* Create \*」を選択します。

エージェントアドレスが作成され、テーブルに追加されます。

#### 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. SNMPv3 を使用している場合は、Other Configurations セクションの USM Users タブを選択します。

このタブを使用して、MIB の照会またはトラップおよびインフォームの受信を許可されている USM ユーザを定義します。





この手順は、SNMPv1 または SNMPv2c のみを使用している場合は適用されません。


- a. 「\* Create \*」を選択します。


[Create USM User] ダイアログボックスが表示されます。

# 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. この USM ユーザの一意的な \* ユーザ名 \* を入力します。


ユーザ名の最大文字数は32文字で、空白文字は使用できません。ユーザの作成後にユーザ名を変更することはできません。

- c. このユーザにMIBへの読み取り専用アクセスを許可する場合は、\*[Read-only MIB Access]\*チェックボックスをオンにします。

[Read-Only MIB Access] を選択すると、 [Authoritative Engine ID] フィールドは無効になります。

 読み取り専用MIBアクセスを持つUSMユーザには、エンジンIDを設定できません。

d. このユーザを INFORM 宛先で使用する場合は、このユーザの権限のあるエンジン ID \* を入力します。

 SNMPv3 インフォームの送信先には、エンジン ID を持つユーザが必要です。SNMPv3 トラップ送信先には、エンジンIDを持つユーザを含めることはできません。


信頼できるエンジン ID は、16 進数で 5 ～ 32 バイトです。

e. USM ユーザのセキュリティレベルを選択します。

▪ \* authPriv \* : 認証とプライバシー (暗号化) と通信します。認証プロトコルとパスワード、およびプライバシープロトコルとパスワードを指定する必要があります。

▪ \* authNoPriv \* : このユーザは認証と通信し、プライバシーはありません (暗号化なし)。認証プロトコルとパスワードを指定する必要があります。

f. このユーザが認証に使用するパスワードを入力し、確認のためにもう一度入力します。

 サポートされている認証プロトコルは SHA ( HMAC-SHA-96 ) だけです。

g. [authPriv] を選択した場合は、このユーザがプライバシーに使用するパスワードを入力し、確認します。

 サポートされているプライバシープロトコルは AES のみです。

h. 「 \* Create \* 」を選択します。

USM ユーザが作成され、テーブルに追加されます。

## 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. [[select\_trap\_destination, start=10] 他の設定セクションで、トラップ送信先タブを選択します。

トラップ送信先タブでは、StorageGRID トラップまたは通知の送信先を 1 つ以上定義できます。SNMP

エージェントを有効にして[\*保存]\*を選択すると、StorageGRID は定義された各送信先への通知の送信を開始します。通知はアラートがトリガーされたときに送信されます。標準通知は、サポートされている MIB-II エンティティ（ifdown や coldStart など）についても送信されます。

- a. 「\* Create \*」を選択します。

トラップ送信先の作成ダイアログボックスが表示されます。

**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. [\* Version] フィールドで、この通知に使用する SNMP バージョンを選択します。
- b. 選択したバージョンに応じて、フォームに入力します

バージョン	この情報を指定します
<p>SNMPv1</p> <p>(SNMPv1の場合、SNMPエージェントはトラップのみを送信できます。インフォームはサポートされていません)。</p>	<ul style="list-style-type: none"> <li>i. [* Host*] フィールドに、トラップを受信する IPv4 または IPv6 アドレス (または FQDN) を入力します。</li> <li>ii. * Port * には、別の値を使用する必要がある場合を除き、デフォルト (162) を使用してください。(162 は SNMP トラップの標準ポートです)。</li> <li>iii. <b>Protocol</b> には、デフォルト (UDP) を使用します。TCP もサポートされています。(UDP は標準の SNMP トラッププロトコルです)。</li> <li>iv. SNMP Agent ページでトラップコミュニティが指定されている場合は、デフォルトのトラップコミュニティを使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。</li> </ul> <p>カスタムコミュニティストリングの最大文字数は32文字で、空白は使用できません。</p>
<p>SNMPv2c の場合</p>	<ul style="list-style-type: none"> <li>i. トラップまたはインフォームに宛先を使用するかどうかを選択します。</li> <li>ii. [* Host*] フィールドに、トラップを受信する IPv4 または IPv6 アドレス (または FQDN) を入力します。</li> <li>iii. * Port * には、別の値を使用する必要がある場合を除き、デフォルト (162) を使用してください。(162 は SNMP トラップの標準ポートです)。</li> <li>iv. <b>Protocol</b> には、デフォルト (UDP) を使用します。TCP もサポートされています。(UDP は標準の SNMP トラッププロトコルです)。</li> <li>v. SNMP Agent ページでトラップコミュニティが指定されている場合は、デフォルトのトラップコミュニティを使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。</li> </ul> <p>カスタムコミュニティストリングの最大文字数は32文字で、空白は使用できません。</p>

バージョン	この情報を指定します
SNMPv3	<ul style="list-style-type: none"> <li>i. トラップまたはインフォームに宛先を使用するかどうかを選択します。</li> <li>ii. [* Host*] フィールドに、トラップを受信する IPv4 または IPv6 アドレス（または FQDN）を入力します。</li> <li>iii. * Port * には、別の値を使用する必要がある場合を除き、デフォルト（162）を使用してください。（162 は SNMP トラップの標準ポートです）。</li> <li>iv. <b>Protocol</b> には、デフォルト（UDP）を使用します。TCP もサポートされています。（UDP は標準の SNMP トラッププロトコルです）。</li> <li>v. 認証に使用する USM ユーザを選択します。 <ul style="list-style-type: none"> <li>◦ [*Trap] を選択した場合は、権限のあるエンジン ID を持たない USM ユーザだけが表示されます。</li> <li>◦ *INFORM を選択した場合は、権限のあるエンジン ID を持つ USM ユーザのみが表示されます。</li> </ul> </li> </ul>

c. 「\* Create \*」を選択します。

トラップの送信先が作成され、テーブルに追加されます。

11. SNMPエージェントの設定が完了したら、\*[保存]\*を選択します。

新しい SNMP エージェント設定がアクティブになります。

#### 関連情報

["アラート通知をサイレント化する"](#)

## SNMP エージェントを更新します

SNMP 通知の無効化、コミュニティストリングの更新、エージェントアドレス、USM ユーザ、トラップの送信先の追加や削除を行うことができます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- Root Access権限が必要です。

このタスクについて

を更新するたびに ["SNMP エージェントの設定"](#)各タブで行った変更をコミットするには、[SNMP Agent]ページの下部にある\*[保存]\*を選択する必要があることに注意してください。

手順

1. \* configuration \* > \* Monitoring \* > \* SNMP agent \* を選択します。

SNMP Agent ページが表示されます。

- すべてのグリッドノードでSNMPエージェントを無効にする場合は、**[Enable SNMP]**\*チェックボックスをオフにし、**[Save]**\*を選択します。

SNMP エージェントはすべてのグリッドノードで無効になっています。あとでエージェントを再度有効にした場合、以前の SNMP 設定は保持されます。

- 必要に応じて、入力した値を \* System Contact \* および \* System Location \* で更新します。
- 必要に応じて、StorageGRID SNMPエージェントからトラップおよびインフォーム通知を送信しないようにする場合は、\* SNMPエージェント通知を有効にする\*チェックボックスをオフにします。

このチェックボックスをオフにすると、SNMPエージェントは読み取り専用のMIBアクセスをサポートしますが、SNMP通知は送信しません。

- 適切に認証されていないプロトコルメッセージを受信したときにStorageGRID SNMPエージェントから認証トラップが送信されないようにするには、**[認証トラップを有効にする]**\*チェックボックスをオフにします。
- SNMPv1 または SNMPv2c を使用する場合は、必要に応じてコミュニティストリングセクションを更新します。

このセクションのフィールドは、SNMPv1 または SNMPv2c でのコミュニティベースの認証に使用されます。これらのフィールドはSNMPv3には適用されません。



デフォルトのコミュニティストリングを削除する場合は、最初にすべてのトラップ送信先でカスタムのコミュニティストリングを使用する必要があります。

- エージェントアドレスを更新する場合は、**[その他の設定]**セクションの**[エージェントアドレス]**タブを選択します。

### 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

このタブを使用して '1 つまたは複数の " リスニング・アドレス " を指定します。これらは、SNMP エージェントがクエリを受信できる StorageGRID アドレスです。各エージェントアドレスには、インターネットプロトコル、転送プロトコル、StorageGRID ネットワーク、ポートが含まれます。

- エージェントアドレスを追加するには、**[作成]**\*を選択します。次に、SNMP エージェントの設定手順に記載されているエージェントアドレスの手順を参照してください。
- エージェントアドレスを編集するには、アドレスのラジオボタンを選択し、**[編集]**\*を選択します。次

に、SNMP エージェントの設定手順に記載されているエージェントアドレスの手順を参照してください。

- c. エージェントアドレスを削除するには、アドレスのラジオボタンを選択し、**[削除]\***を選択します。次に、**OK \***を選択して、このアドレスを削除することを確認します。
  - d. 変更をコミットするには、[SNMP Agent]ページの下部にある**\*[Save]\***を選択します。
8. USM ユーザを更新するには、Other Configurations セクションで USM Users タブを選択します。

## 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

このタブを使用して、MIB の照会またはトラップおよびインフォームの受信を許可されている USM ユーザを定義します。

- a. USMユーザを追加するには、**\*[作成]\***を選択します。次に、SNMP エージェントの設定手順の USM ユーザ向けの手順を参照してください。
- b. USMユーザを編集するには、ユーザのラジオボタンを選択し、**\*[編集]\***を選択します。次に、SNMP エージェントの設定手順の USM ユーザ向けの手順を参照してください。

既存のUSMユーザのユーザ名は変更できません。ユーザ名を変更する必要がある場合は、ユーザを削除して新しいユーザを作成する必要があります。



ユーザの権限のあるエンジン ID を追加または削除した場合、そのユーザが現在デスティネーションに対して選択されているときは、手順の説明に従って、デスティネーションを編集または削除する必要があります [SNMP トラップの送信先](#)。そうしないと、SNMP エージェント設定を保存したときに検証エラーが発生します。

- a. USMユーザを削除するには、ユーザのラジオボタンを選択し、**[削除]\***を選択します。次に、**OK \***を選択して、このユーザの削除を確認します。



削除したユーザがトラップの送信先として選択されている場合は、手順の説明に従って、送信先を編集または削除する必要があります [SNMP トラップの送信先](#)。そうしないと、SNMP エージェント設定を保存したときに検証エラーが発生します。

- b. 変更をコミットするには、[SNMP Agent]ページの下部にある**\*[Save]\***を選択します。
9. `[[snmp_trap_destination, start=9]` トラップ送信先を更新するには、[その他の設定]セクションの[トラップ送信先]タブを選択します。



トラップ送信先タブでは、StorageGRID トラップまたは通知の送信先を 1 つ以上定義できます。SNMP エージェントを有効にして\*[保存]\*を選択すると、StorageGRID は定義された各送信先への通知の送信を開始します。通知は、アラートとアラームがトリガーされたときに送信されます。標準通知は、サポートされている MIB-II エンティティ（ifdown や coldStart など）についても送信されます。

- a. トラップ送信先を追加するには、\*[作成]\*を選択します。次に、SNMP エージェントの設定手順のトラップ送信先の手順を参照してください。
- b. トラップ送信先を編集するには、ユーザのラジオボタンを選択し、\*[編集]\*を選択します。次に、SNMP エージェントの設定手順のトラップ送信先の手順を参照してください。
- c. トラップ送信先を削除するには、送信先のラジオボタンを選択し、[削除]\*を選択します。次に、OK \* を選択して、この送信先の削除を確定します。
- d. 変更をコミットするには、[SNMP Agent]ページの下部にある\*[Save]\*を選択します。

10. SNMP エージェントの設定を更新したら、\*[保存]\*を選択します。

## MIB ファイルにアクセスします

MIB ファイルには、グリッド内のノードの管理対象リソースとサービスのプロパティの定義と情報が含まれています。StorageGRID のオブジェクトと通知を定義する MIB ファイルにアクセスできます。これらのファイルは、グリッドの監視に役立ちます。

を参照してください ["SNMP による監視を使用する"](#) SNMP および MIB ファイルの詳細については、を参照してください。

## MIB ファイルにアクセスします

手順

1. \* configuration \* > \* Monitoring \* > \* SNMP agent \* を選択します。
2. [SNMP agent] ページで、ダウンロードするファイルを選択します。
  - \* NETAPP-STORAGEGRID-MIB.txt \* : すべての管理ノードでアクセス可能なアラートテーブルと通知 (トラップ) を定義します。
  - \* ES-NetApp-06-MIB.mib \* : E シリーズベースのアプライアンスのオブジェクトと通知を定義します。
  - \* mib\_1\_10.zip \* : BMC インターフェイスを使用するアプライアンスのオブジェクトと通知を定義します。
3. 必要に応じて、任意の StorageGRID ノードの次の場所にある MIB ファイルにアクセスできます。  
/usr/share/snmp/mibs
4. を展開します storagegrid MIB ファイルの OID :
  - a. StorageGRID MIB のルートの OID を取得します。

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

結果 .1.3.6.1.4.1.789.28669 (28669 は常に StorageGRID の OID)

- a. 次に、ツリー全体の StorageGRID OID を grep で指定します (貼り付けを使用して行を結合します)。

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



。 snmptranslate コマンドには、MIBの探索に役立つ多くのオプションがあります。このコマンドは、任意のStorageGRID ノードで使用できます。

## MIBファイルの内容

すべてのオブジェクトはStorageGRID OIDの下にあります。

オブジェクト名	オブジェクトID (OID)	説明
		ネットアップStorageGRID エンティティ用のMIBモジュール。

## MIBオブジェクト

オブジェクト名	オブジェクトID (OID)	説明
activeAlertCount	1.3.6.1.4.1.+789.28669.1.3	activeAlertTable内のアクティブなアラートの数。
activeAlertTableの略	1.3.6.1.4.1.+789.28669.1.4	StorageGRID のアクティブなアラートのテーブル。
activeAlertId	1.3.6.1.4.1.+789.28669.1.4.1.1	アラートのID。現在アクティブなアラートのセット内でのみ一意です。
activeAlertNameの略	1.3.6.1.4.1.+789.28669.1.4.1.2	アラートの名前。
activeAlertInstanceの略	1.3.6.1.4.1.+789.28669.1.4.1.3	アラートを生成したエンティティの名前（通常はノード名）。
activeAlertSeverityの略	1.3.6.1.4.1.+789.28669.1.4.1.4	アラートの重大度。
activeAlertStartTimeの略	1.3.6.1.4.1.+789.28669.1.4.1.5	アラートがトリガーされた日時。

## 通知タイプ（トラップ）

すべての通知には、変数バインドとして次の変数が含まれます。

- activeAlertId
- activeAlertNameの略
- activeAlertInstanceの略

- activeAlertSeverityの略
- activeAlertStartTimeの略

通知タイプ	オブジェクトID (OID)	説明
activeMinorAlertの略	1.3.6.1.4.1.+789.28669.0.6	重大度がMinorのアラート
activeMajorAlertの略	1.3.6.1.4.1.+789.28669.0.7	Major重大度のアラート
activeCriticalAlertの略	1.3.6.1.4.1.+789.28669.0.8	重大度がCriticalのアラート

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。