SNMPによる監視を使用する
StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid-115/monitor/configuring-snmp-agent.html on October 03, 2025. Always check docs.netapp.com for the latest.

目次

SNMPによる監視を使用する 1
機能 1
SNMP バージョンサポート 1
制限 2
MIBへのアクセス 2
SNMPエージェントの設定 2
SNMPエージェントを更新しています 13

SNMPによる監視を使用する

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エージェントの設定"
- "SNMPエージェントを更新しています"

機能

各 StorageGRID ノードは、管理情報ベース（ MIB ）を提供する SNMP エージェントまたは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。

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、優先送信者として設定された管理ノードから送信されます。
- 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アラーム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。

MIBへのアクセス

MIB 定義ファイルには、任意の StorageGRID ノードの次の場所からアクセスできます。

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

関連情報

"アラート一覧"

"アラーム一覧（従来のシステム）"

"SNMP 通知を生成するアラーム（従来のシステム）"

"アラート通知のサイレント化"

SNMPエージェントの設定

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。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

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。

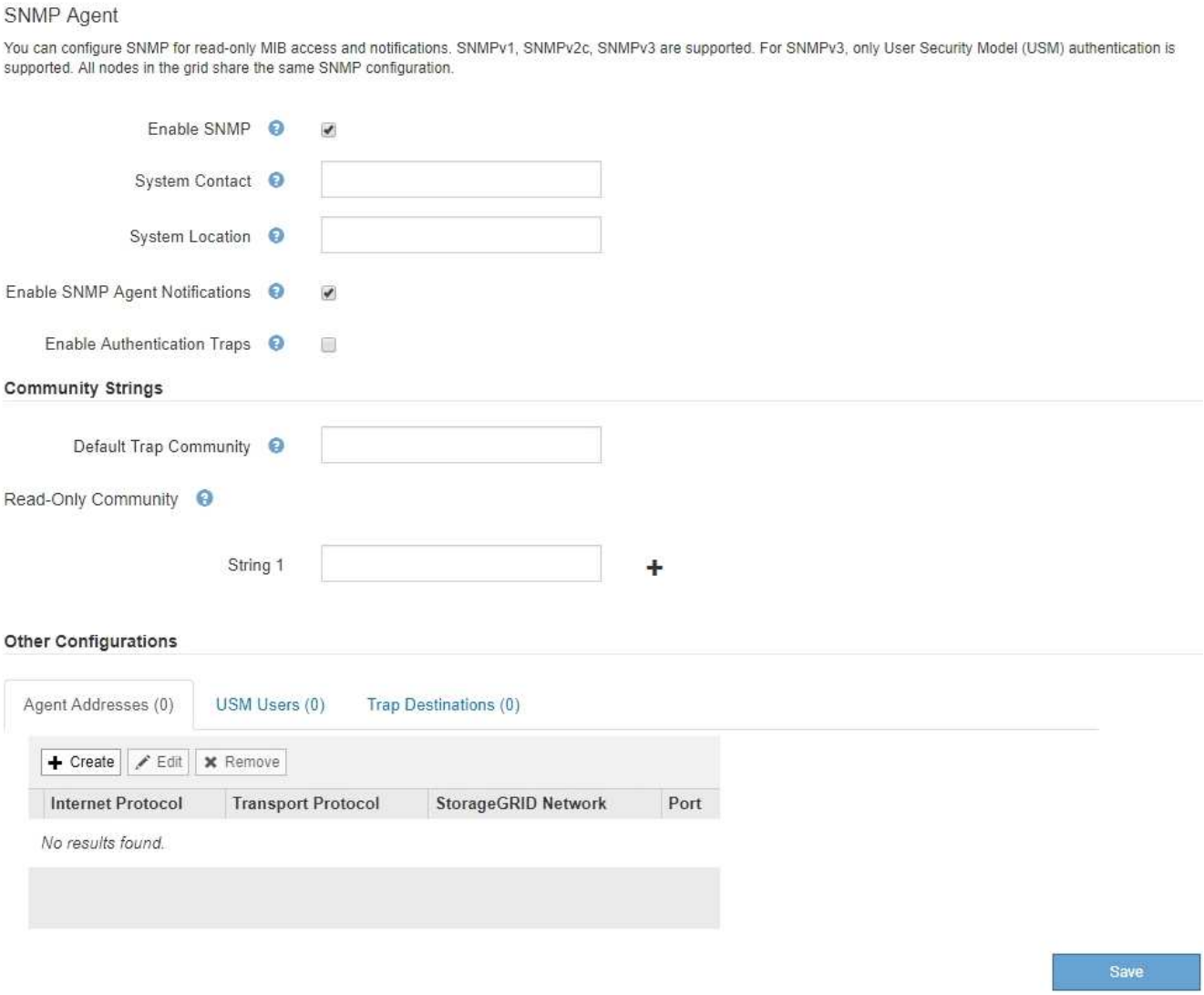
手順

1. * Configuration > Monitoring > SNMP Agent *を選択します。

   SNMP Agent ページが表示されます。

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オンにします。

   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。



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。

5. StorageGRID SNMP エージェントが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がオフの場合、 SNMP エージェントは読み取り専用 MIB アクセスをサポートしますが、 SNMP 通知は送信しません。

6. StorageGRID SNMP エージェントが不適切に認証されたプロトコルメッセージを受信した場合に認証トラップを送信するには、 [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。

7. 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。

   a. [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。

      - デフォルトのトラップコミュニティ * は 32 文字以内で、空白文字を含めることはできません。

   b. * 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。プラス記号をクリックします ➕ 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。

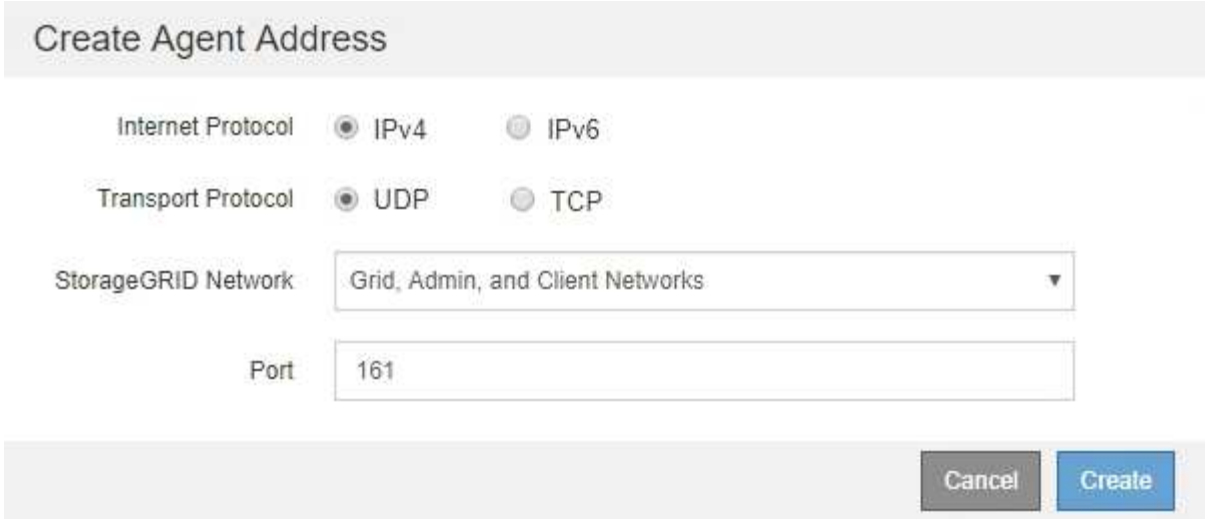
8. 必要に応じて、 Other Configurations セクションの Agent Addresses タブを選択します。

   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す。

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

   a. [作成（ Create ）] をクリックします。

      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 エージェントがリッ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. [作成（ Create ）] をクリックします。

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。

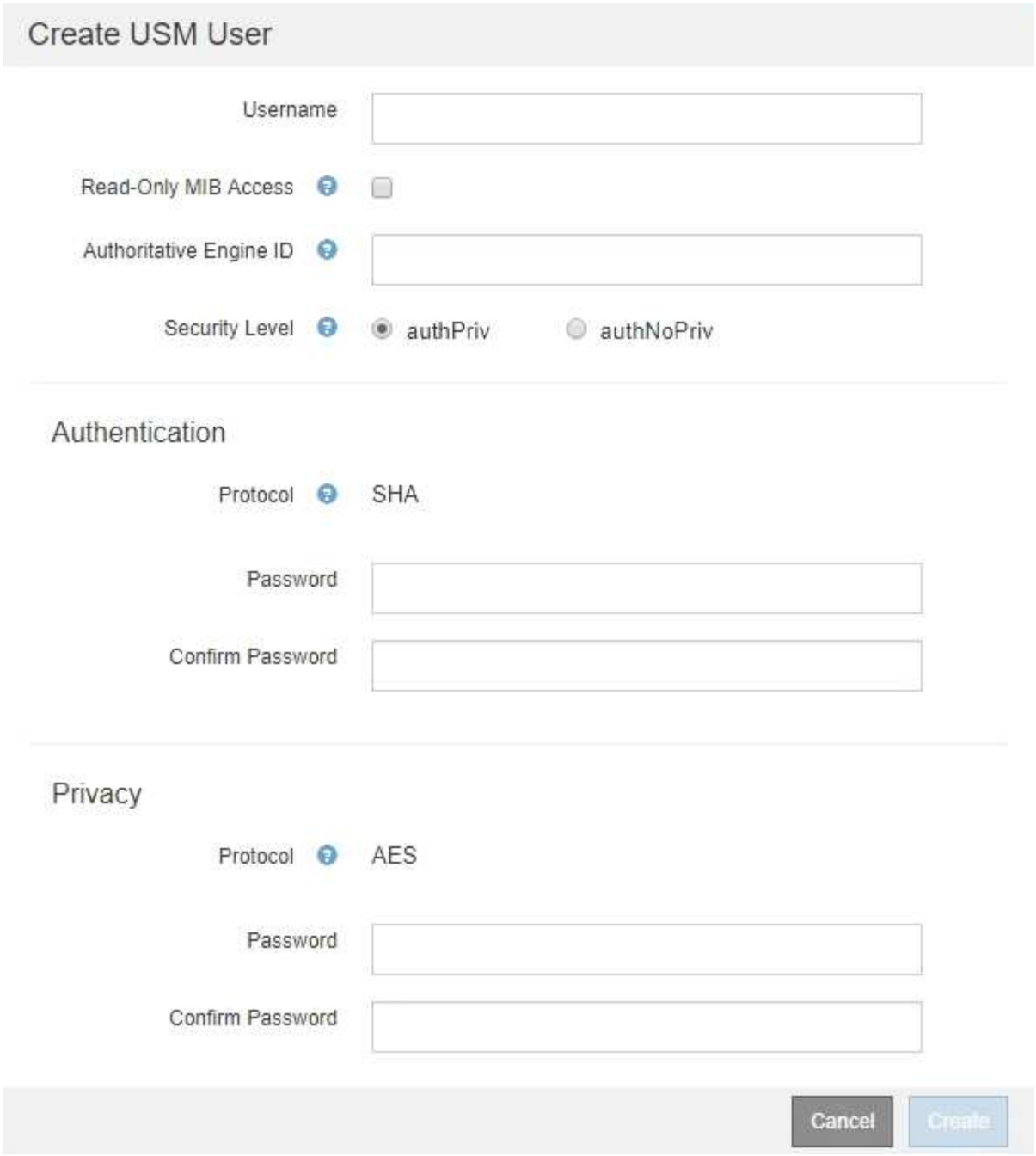
9. SNMPv3 を使用している場合は、 Other Configurations セクションの USM Users タブを選択します。

   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. [作成（ Create ）] をクリックします。

      [Create USM User] ダイアログボックスが表示されます。



b. この USM ユーザの一意の * 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。ユーザ名は作成後に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権が必要な場合は、 [* 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 アクセスが設定された USM ユーザは、エンジン ID を取得できません。

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 トラップの送信先にエンジン 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。

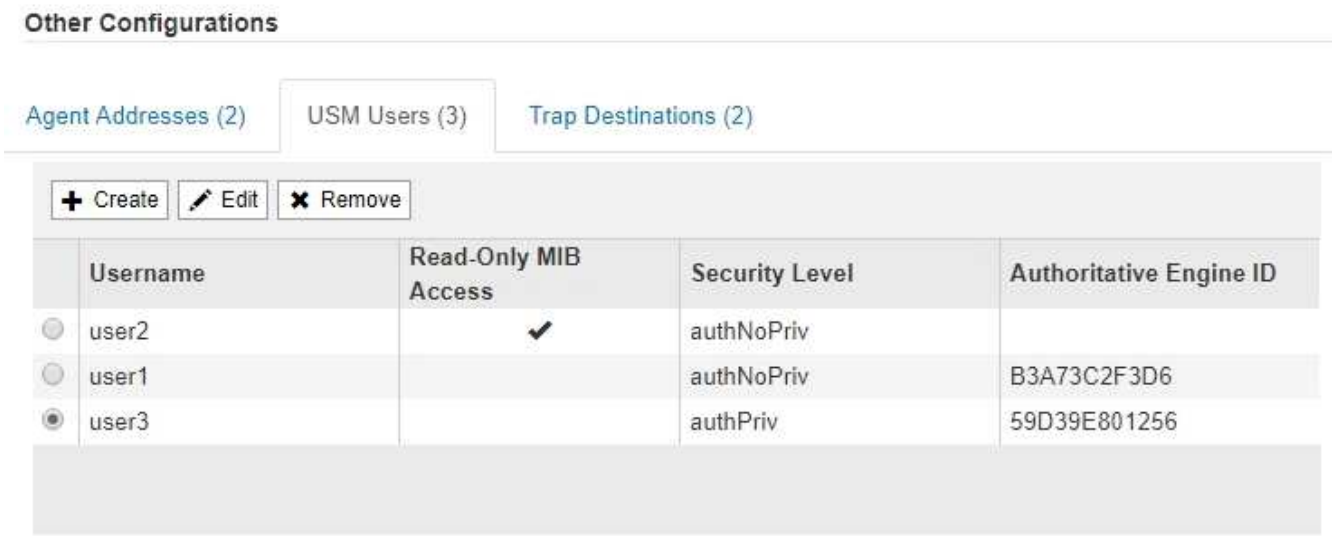
サポートされている認証プロトコルは SHA （ HMAC-SHA-96 ）だけです。

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. [作成（ Create ）] をクリックします。

USM ユーザが作成され、テーブルに追加されます。

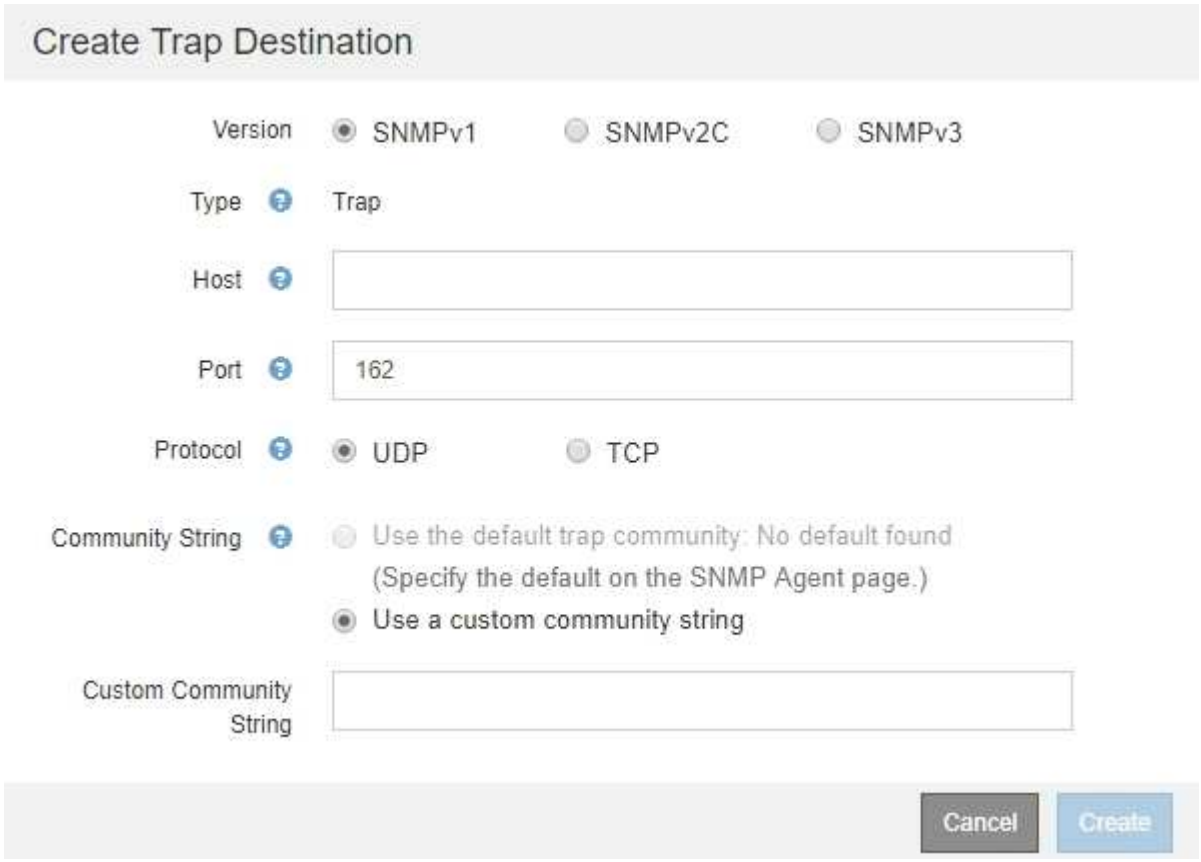


10. [その他の設定]セクションで、[トラップ送信先]タブを選択します。

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 * Save * をクリックすると、 StorageGRID は定義された各宛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. [作成（ Create ）] をクリックします。

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。



b. [* 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。

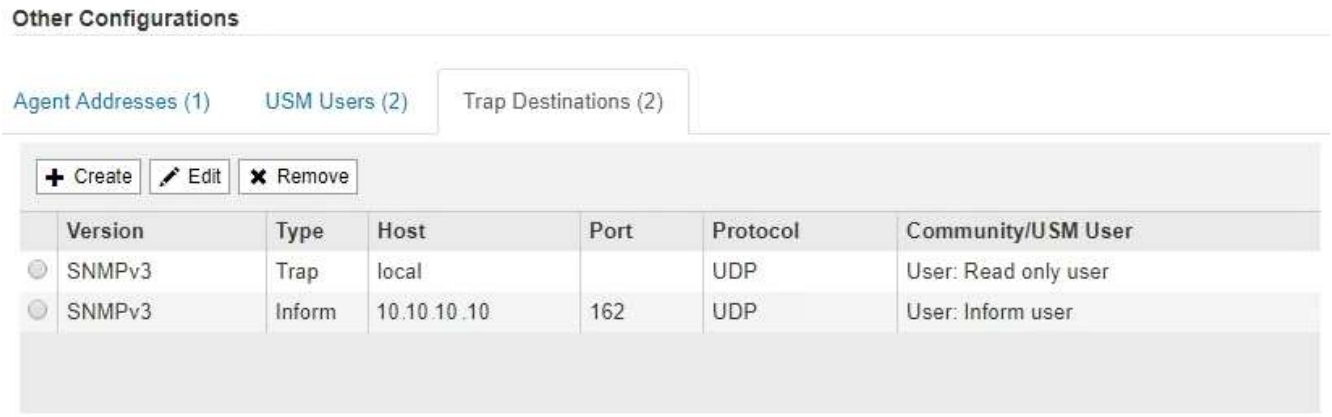
c. 選択したバージョンに応じて、フォームに入力します

バージョン	この情報を指定します
SNMPv1	• 注： 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ません。 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。 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）。 iii. **Protocol** 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）。 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。 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、空白を含めることはできません。

バージョン	この情報を指定します
SNMPv2c の場合	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。 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。 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）。 iv. **Protocol** 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）。 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。 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、空白を含めることはできません。
SNMPv3	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。 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。 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）。 iv. **Protocol** 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）。 v. 認証に使用する USM ユーザを選択します。 ◦ [*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。 ◦ *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。

d. [作成（ Create ）] をクリックします。

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、 * Save * をクリックします

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

"アラート通知のサイレント化"

SNMPエージェントを更新しています

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。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

SNMPエージェント設定を更新する場合は、[SNMP Agent]ページの下部にある[*Save]をクリックして、各タブで行った変更をコミットする必要があります。

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。

2. 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、 * SNMP を有効にする * チェックボックスをオフにして、 * 保存 * をクリックします。

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。

3. 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。

4. StorageGRID SNMP エージェントが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には、必要に応じて、 [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 MIB アクセスをサポートしますが、 SNMP 通知は送信しません。

5. 認証されていないプロトコルメッセージを StorageGRID SNMP エージェントが受信したときに認証トラップを送信しないようにするには、必要に応じて、 [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。

6. 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。

7. 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。

   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。

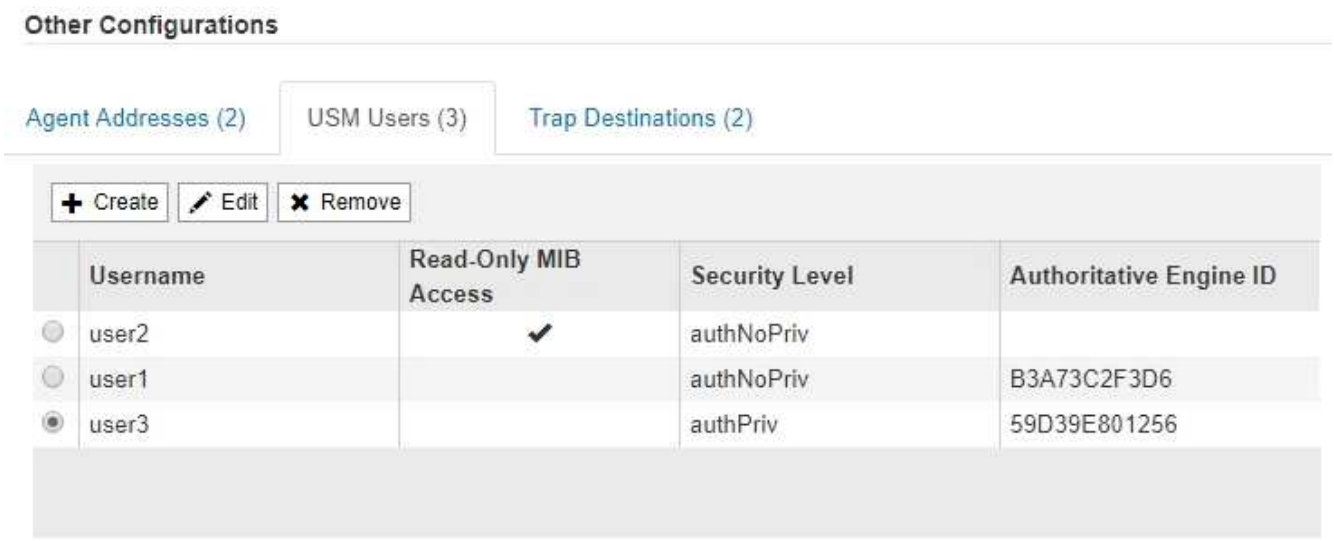
   a. エージェントアドレスを追加するには、 * 作成 * をクリックします。次に、 SNMP エージェントの設定手順に記載されているエージェントアドレスの手順を参照してください。

   b. 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、 * Edit * をクリックします。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 * をクリックします。次に、 [OK] をクリックして、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** をクリックします。

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。



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、 * Create * をクリックします。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、ユーザのオプションボタンを選択し、 * Edit * をクリックします。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。

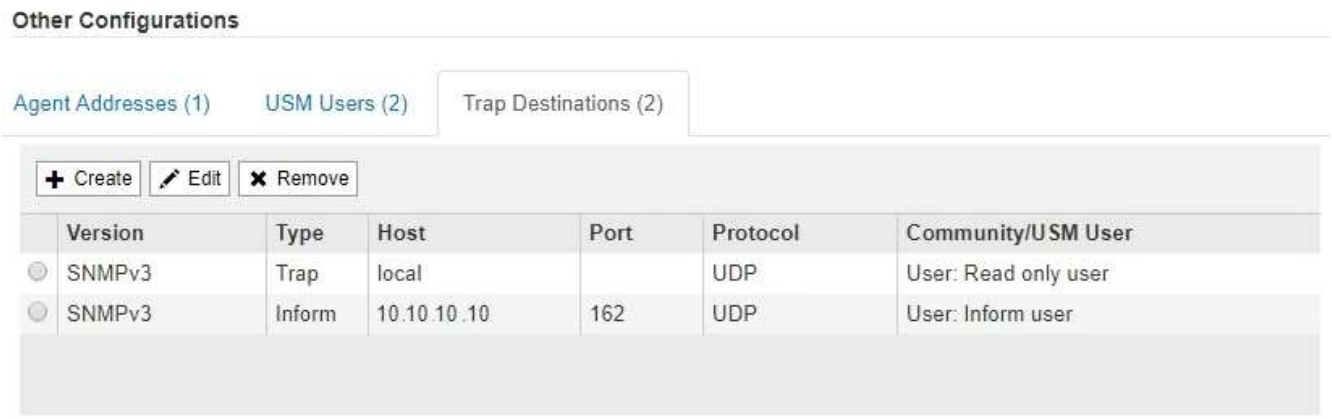
   ユーザの権限のあるエンジン ID を追加または削除した場合、そのユーザが現在デスティネーションに対して選択されているときは、手順の説明に従って、デスティネーションを編集または削除する必要があります SNMP トラップの送信先。そうしないと、 SNMP エージェント設定を保存したときに検証エラーが発生します。

c. USM ユーザを削除するには、ユーザのオプションボタンを選択し、 * Remove * をクリックします。次に、 [OK] をクリックして、このユーザーを削除することを確認します。

   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。

a. 変更をコミットするには、 SNMP Agent ページの下部にある **Save** をクリックします。

1. トラップ送信先を更新する場合は、[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 * Save * をクリックすると、 StorageGRID は定義された各宛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 * をクリックします。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、ユーザのオプションボタンを選択し、 * Edit * をクリックします。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、送信先のオプションボタンを選択し、 * Remove * （削除）をクリックします。次に、 [OK] をクリックして、この宛先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** をクリックします。

2. SNMP エージェント設定を更新したら、 * Save * をクリックします。

関連情報

"SNMPエージェントの設定"

著作権に関する情報

Copyright © 2025 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権を有し、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権については、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。