



Utilisation de la surveillance SNMP

StorageGRID

NetApp

October 03, 2025

Sommaire

Utilisation de la surveillance SNMP	1
Capacités	1
Prise en charge de la version SNMP	1
Limites	2
Accès à la MIB	2
Configuration de l'agent SNMP	2
Mise à jour de l'agent SNMP	13

Utilisation de la surveillance SNMP

Si vous souhaitez surveiller StorageGRID à l'aide du protocole SNMP (simple Network Management Protocol), vous devez configurer l'agent SNMP inclus avec StorageGRID.

- ["Configuration de l'agent SNMP"](#)
- ["Mise à jour de l'agent SNMP"](#)

Capacités

Chaque nœud StorageGRID exécute un agent SNMP, ou un démon, qui fournit une base d'informations de gestion (MIB). La MIB StorageGRID contient des définitions de tableau et de notification pour les alertes et les alarmes. La base MIB contient également des informations de description du système, telles que la plateforme et le numéro de modèle pour chaque nœud. Chaque nœud StorageGRID supporte également un sous-ensemble d'objets MIB-II.

Au départ, le protocole SNMP est désactivé sur tous les nœuds. Lorsque vous configurez l'agent SNMP, tous les nœuds StorageGRID reçoivent la même configuration.

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Il fournit un accès MIB en lecture seule pour les requêtes et il peut envoyer deux types de notifications événementielle à un système de gestion :

- **Les traps** sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'accusé de réception par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple.

Les traps sont pris en charge dans les trois versions de SNMP.

- **Inform** sont similaires aux pièges, mais ils exigent une reconnaissance du système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain temps, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale ait été atteinte.

Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Les notifications d'interruption et d'information sont envoyées dans les cas suivants :

- Une alerte par défaut ou personnalisée est déclenchée à tout niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez configurer un silence pour l'alerte. Les notifications d'alerte sont envoyées par n'importe quel nœud d'administration configuré pour être l'expéditeur préféré.
- Certaines alarmes (système hérité) sont déclenchées à des niveaux de gravité spécifiés ou plus.



Les notifications SNMP ne sont pas envoyées pour chaque alarme ou chaque gravité d'alarme.

Prise en charge de la version SNMP

Le tableau fournit un résumé détaillé des éléments pris en charge pour chaque version de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Requêtes	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule
Authentification par requête	Chaîne de communauté	Chaîne de communauté	Utilisateur USM (User Security Model)
Notifications	Traps uniquement	Pièges et information	Pièges et information
Authentification des notifications	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Utilisateur USM pour chaque destination d'interruption

LIMITES

- StorageGRID supporte l'accès MIB en lecture seule. L'accès en lecture/écriture n'est pas pris en charge.
- Tous les nœuds de la grille reçoivent la même configuration.
- SNMPv3 : StorageGRID ne prend pas en charge le mode support transport (TSM).
- SNMPv3 : le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).
- SNMPv3 : le seul protocole de confidentialité pris en charge est AES.

ACCÈS À LA MIB

Vous pouvez accéder au fichier de définition MIB à l'emplacement suivant sur n'importe quel nœud StorageGRID :

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

Informations associées

["Référence des alertes"](#)

["Référence des alarmes \(système hérité\)"](#)

["Alarmes générant des notifications SNMP \(système hérité\)"](#)

["Neutralisation des notifications d'alerte"](#)

CONFIGURATION DE L'AGENT SNMP

Vous pouvez configurer l'agent SNMP StorageGRID si vous souhaitez utiliser un système de gestion SNMP tiers pour l'accès MIB en lecture seule et les notifications.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Vous pouvez configurer l'agent pour une ou plusieurs versions.

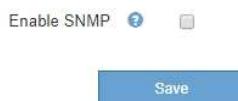
Étapes

1. Sélectionnez **Configuration > surveillance > agent SNMP**.

La page agent SNMP s'affiche.

SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.



2. Pour activer l'agent SNMP sur tous les nœuds de la grille, cochez la case **Activer SNMP**.

Les champs de configuration d'un agent SNMP s'affichent.

SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.

The screenshot shows the 'SNMP Agent' configuration page. It includes fields for 'Enable SNMP' (checked), 'System Contact' (empty), 'System Location' (empty), 'Enable SNMP Agent Notifications' (checked), and 'Enable Authentication Traps' (unchecked). Below these are sections for 'Community Strings' and 'Other Configurations'. The 'Community Strings' section has fields for 'Default Trap Community' (empty) and 'Read-Only Community' (String 1 empty, plus icon). The 'Other Configurations' section has tabs for 'Agent Addresses (0)', 'USM Users (0)', and 'Trap Destinations (0)'. Under 'Agent Addresses', there are buttons for '+ Create', 'Edit', and 'Remove', and tabs for 'Internet Protocol', 'Transport Protocol', 'StorageGRID Network', and 'Port'. A message 'No results found.' is displayed. A blue 'Save' button is located at the bottom right.

Enable SNMP

System Contact

System Location

Enable SNMP Agent Notifications

Enable Authentication Traps

Community Strings

Default Trap Community

Read-Only Community +

Other Configurations

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

+ Create Edit Remove

Internet Protocol Transport Protocol StorageGRID Network Port

No results found.

Save

3. Dans le champ **Contact système**, entrez la valeur que vous souhaitez que StorageGRID vous apporte dans les messages SNMP pour sysContact.

Le contact système est généralement une adresse e-mail. La valeur indiquée s'applique à tous les nœuds du système StorageGRID. **Contact système** peut comporter un maximum de 255 caractères.

4. Dans le champ **emplacement du système**, entrez la valeur que vous souhaitez que StorageGRID vous apporte dans les messages SNMP pour sysLocation.

L'emplacement du système peut être toute information utile pour identifier l'emplacement de votre système StorageGRID. Par exemple, vous pouvez utiliser l'adresse d'un établissement. La valeur indiquée s'applique à tous les nœuds du système StorageGRID. **Emplacement du système** peut comporter un maximum de 255 caractères.

5. Cochez la case **Activer les notifications d'agent SNMP** si vous souhaitez que l'agent SNMP StorageGRID envoie des notifications d'interruption et informe les notifications.

Si cette case n'est pas cochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais il n'envoie pas de notifications SNMP.

6. Cochez la case **Activer les interruptions d'authentification** si vous souhaitez que l'agent SNMP StorageGRID envoie une interruption d'authentification s'il reçoit un message de protocole mal authentifié.

7. Si vous utilisez SNMPv1 ou SNMPv2c, complétez la section chaînes de communauté.

Les champs de cette section sont utilisés pour l'authentification communautaire dans SNMPv1 ou SNMPv2c. Ces champs ne s'appliquent pas au protocole SNMPv3.

- a. Dans le champ **Default Trap Community**, vous pouvez également saisir la chaîne de communauté par défaut que vous souhaitez utiliser pour les destinations de déroutement.

Selon les besoins, vous pouvez fournir une autre chaîne de communauté (« personnalisée ») lorsque vous [définir une destination de recouvrement spécifique](#).

Valeur par défaut Trap Community peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces.

- b. Pour **Read-Only Community**, entrez une ou plusieurs chaînes de communauté pour autoriser l'accès MIB en lecture seule sur les adresses d'agent IPv4 et IPv6. Cliquez sur le signe plus  pour ajouter plusieurs chaînes.

Lorsque le système de gestion interroge la MIB StorageGRID, il envoie une chaîne de communauté. Si la chaîne de communauté correspond à l'une des valeurs spécifiées ici, l'agent SNMP envoie une réponse au système de gestion.

Chaque chaîne de communauté peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces. Jusqu'à cinq chaînes sont autorisées.



Pour assurer la sécurité de votre système StorageGRID, n'utilisez pas « public » comme fil de communauté. Si vous n'entrez pas de chaîne de communauté, l'agent SNMP utilise l'ID de grille de votre système StorageGRID comme chaîne de communauté.

8. Vous pouvez également sélectionner l'onglet adresses d'agent dans la section autres configurations.

Utilisez cet onglet pour spécifier une ou plusieurs « adresses d'écoute ». Ce sont les adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes. Chaque adresse de l'agent inclut un protocole Internet, un protocole de transport, un réseau StorageGRID et éventuellement un port.

Si vous ne configurez pas d'adresse d'agent, l'adresse d'écoute par défaut est le port UDP 161 sur tous les réseaux StorageGRID.

- a. Cliquez sur **Créer**.

La boîte de dialogue **Créer une adresse d'agent** s'affiche.

Create Agent Address

Internet Protocol IPv4 IPv6

Transport Protocol UDP TCP

StorageGRID Network

Port

b. Pour **Internet Protocol**, indiquez si cette adresse doit utiliser IPv4 ou IPv6.

Par défaut, SNMP utilise IPv4.

c. Pour **transport Protocol**, sélectionnez si cette adresse utilisera UDP ou TCP.

Par défaut, SNMP utilise UDP.

d. Dans le champ **réseau StorageGRID**, sélectionnez le réseau StorageGRID sur lequel la requête sera reçue.

- Réseau Grid, Admin et client : StorageGRID doit écouter les requêtes SNMP sur les trois réseaux.
- Réseau Grid
- Réseau d'administration
- Réseau client



Pour vous assurer que les communications client avec StorageGRID restent sécurisées, vous ne devez pas créer d'adresse d'agent pour le réseau client.

e. Dans le champ **Port**, saisissez éventuellement le numéro de port que l'agent SNMP doit écouter.

Le port UDP par défaut d'un agent SNMP est 161, mais vous pouvez entrer n'importe quel numéro de port inutilisé.



Lorsque vous enregistrez l'agent SNMP, StorageGRID ouvre automatiquement les ports d'adresse de l'agent sur le pare-feu interne. Vous devez vous assurer que tous les pare-feu externes autorisent l'accès à ces ports.

f. Cliquez sur **Créer**.

L'adresse de l'agent est créée et ajoutée à la table.

Other Configurations

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

Internet Protocol **Transport Protocol** **StorageGRID Network** **Port**

Internet Protocol	Transport Protocol	StorageGRID Network	Port
IPv4	UDP	Grid Network	161
IPv4	UDP	Admin Network	161

9. Si vous utilisez SNMPv3, sélectionnez l'onglet utilisateurs USM dans la section autres configurations.

Utilisez cet onglet pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.



Cette étape ne s'applique pas si vous utilisez uniquement SNMPv1 ou SNMPv2c.

a. Cliquez sur **Créer**.

La boîte de dialogue **Créer un utilisateur USM** s'affiche.

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. Saisissez un **Nom d'utilisateur** unique pour cet utilisateur USM.

Les noms d'utilisateur ont un maximum de 32 caractères et ne peuvent pas contenir d'espaces. Le nom d'utilisateur ne peut pas être modifié après la création de l'utilisateur.

- c. Cochez la case **accès MIB en lecture seule** si cet utilisateur doit avoir un accès en lecture seule à la base de données MIB.

Si vous sélectionnez **accès MIB en lecture seule**, le champ **ID moteur autorisée** est désactivé.



Les utilisateurs d'USM disposant d'un accès MIB en lecture seule ne peuvent pas avoir d'ID de moteur.

- d. Si cet utilisateur sera utilisé dans une destination INFORM, saisissez l'ID de moteur * faisant autorité

pour cet utilisateur.



Les destinations SNMPv3 INFORM doivent avoir des utilisateurs avec des ID de moteur. La destination du trap SNMPv3 ne peut pas avoir d'utilisateurs avec des ID de moteur.

L'ID de moteur faisant autorité peut être de 5 à 32 octets en hexadécimal.

e. Sélectionnez un niveau de sécurité pour l'utilisateur USM.

- **AuthPriv** : cet utilisateur communique avec l'authentification et la confidentialité (cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe ainsi qu'un protocole de confidentialité et un mot de passe.
- **AuthNoPriv**: Cet utilisateur communique avec l'authentification et sans confidentialité (pas de cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe.

f. Entrez et confirmez le mot de passe que cet utilisateur utilisera pour l'authentification.



Le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).

g. Si vous avez sélectionné **authPriv**, entrez et confirmez le mot de passe que cet utilisateur utilisera pour la confidentialité.



Le seul protocole de confidentialité pris en charge est AES.

h. Cliquez sur **Créer**.

L'utilisateur USM est créé et ajouté à la table.

Other Configurations

Other Configurations				
Agent Addresses (2)		USM Users (3)		Trap Destinations (2)
+ Create Edit Remove				
	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. dans la section autres configurations, sélectionnez l'onglet destinations de recouvrement.

L'onglet destinations de recouvrement permet de définir une ou plusieurs destinations pour les notifications d'interruption StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et cliquez sur **Enregistrer**, StorageGRID commence à envoyer des notifications à chaque destination définie. Des notifications sont envoyées lorsque des alertes et des alarmes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

a. Cliquez sur **Créer**.

La boîte de dialogue **Créer une destination de recouvrement** s'affiche.

Create Trap Destination

Version SNMPv1 SNMPv2C SNMPv3

Type Trap

Host

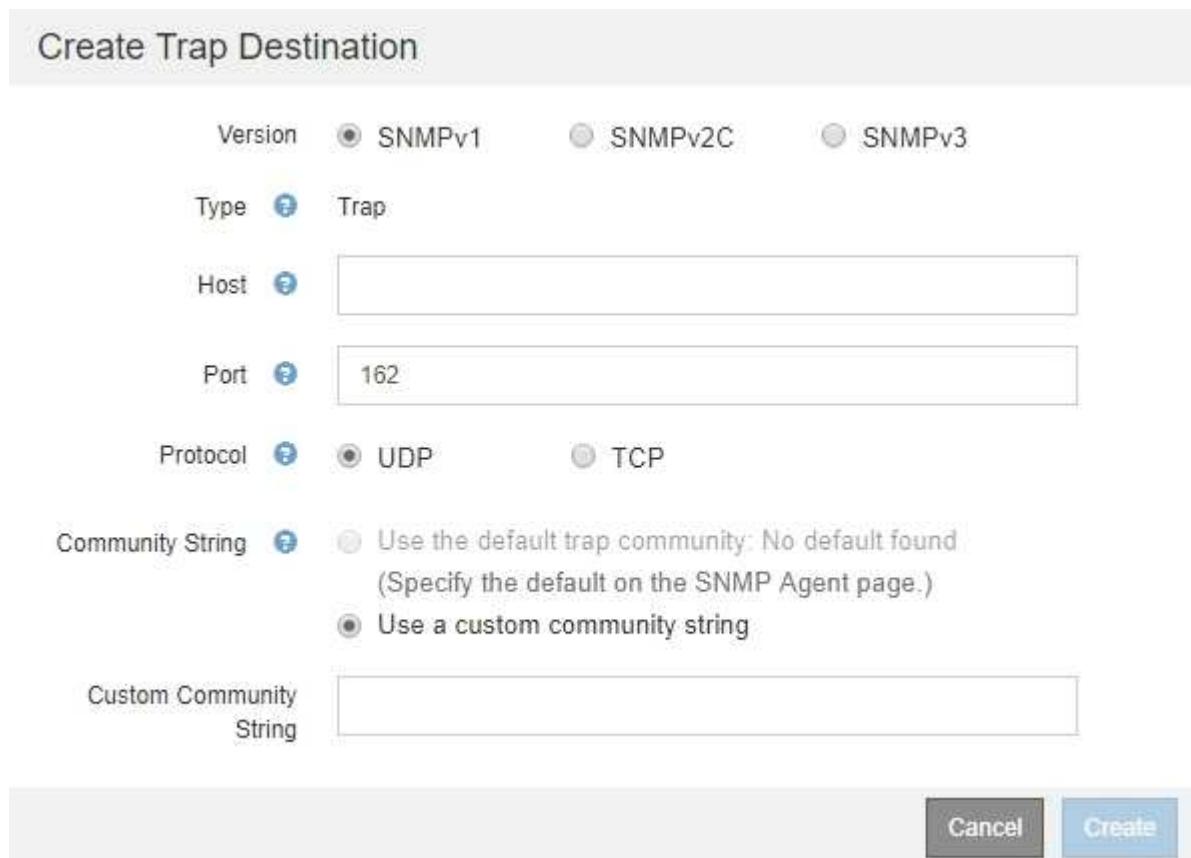
Port 162

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

Cancel **Create**



b. Dans le champ **version**, sélectionnez la version SNMP à utiliser pour cette notification.

c. Remplissez le formulaire en fonction de la version que vous avez sélectionnée

Version	Spécifiez ces informations
SNMPv1	<p>Remarque : pour SNMPv1, l'agent SNMP ne peut envoyer que des interruptions. Les informations ne sont pas prises en charge.</p> <ul style="list-style-type: none"> i. Dans le champ Host, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. ii. Pour Port, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iii. Pour Protocol, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) iv. Utilisez la communauté d'interruptions par défaut, si l'une d'entre elles a été spécifiée sur la page agent SNMP, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. <p>La chaîne de communauté personnalisée peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces.</p>
SNMPv2c	<ul style="list-style-type: none"> i. Indiquez si la destination sera utilisée pour les interruptions ou pour les informations. ii. Dans le champ Host, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. iii. Pour Port, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iv. Pour Protocol, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) v. Utilisez la communauté d'interruptions par défaut, si l'une d'entre elles a été spécifiée sur la page agent SNMP, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. <p>La chaîne de communauté personnalisée peut comporter un maximum de 32 caractères et ne peut pas contenir d'espaces.</p>

Version	Spécifiez ces informations
SNMPv3	<ul style="list-style-type: none"> i. Indiquez si la destination sera utilisée pour les interruptions ou pour les informations. ii. Dans le champ Host, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. iii. Pour Port, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iv. Pour Protocol, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) v. Sélectionnez l'utilisateur USM qui sera utilisé pour l'authentification. <ul style="list-style-type: none"> ◦ Si vous avez sélectionné Trap, seuls les utilisateurs d'USM sans ID de moteur faisant autorité sont affichés. ◦ Si vous avez sélectionné INFORM, seuls les utilisateurs d'USM avec des ID de moteur faisant autorité sont affichés.

d. Cliquez sur **Créer**.

La destination de la trappe est créée et ajoutée à la table.

Other Configurations

Agent Addresses (1)	USM Users (2)	Trap Destinations (2)																			
	<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="X Remove"/> <table border="1" data-bbox="600 1347 1490 1495"> <thead> <tr> <th data-bbox="225 1358 323 1389">Version</th><th data-bbox="430 1358 486 1389">Type</th><th data-bbox="567 1358 616 1389">Host</th><th data-bbox="771 1358 820 1389">Port</th><th data-bbox="902 1358 975 1389">Protocol</th><th data-bbox="1073 1358 1310 1389">Community/USM User</th></tr> </thead> <tbody> <tr> <td data-bbox="225 1400 323 1431"><input checked="" type="radio"/> SNMPv3</td><td data-bbox="430 1400 486 1431">Trap</td><td data-bbox="567 1400 616 1431">local</td><td data-bbox="771 1400 820 1431"></td><td data-bbox="902 1400 975 1431">UDP</td><td data-bbox="1073 1400 1294 1431">User: Read only user</td></tr> <tr> <td data-bbox="225 1442 323 1474"><input checked="" type="radio"/> SNMPv3</td><td data-bbox="430 1442 486 1474">Inform</td><td data-bbox="567 1442 674 1474">10.10.10.10</td><td data-bbox="771 1442 820 1474">162</td><td data-bbox="902 1442 975 1474">UDP</td><td data-bbox="1073 1442 1253 1474">User: Inform user</td></tr> </tbody> </table>	Version	Type	Host	Port	Protocol	Community/USM User	<input checked="" type="radio"/> SNMPv3	Trap	local		UDP	User: Read only user	<input checked="" type="radio"/> SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user		
Version	Type	Host	Port	Protocol	Community/USM User																
<input checked="" type="radio"/> SNMPv3	Trap	local		UDP	User: Read only user																
<input checked="" type="radio"/> SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user																

11. Une fois la configuration de l'agent SNMP terminée, cliquez sur **Enregistrer**

La nouvelle configuration de l'agent SNMP devient active.

Informations associées

["Neutralisation des notifications d'alerte"](#)

Mise à jour de l'agent SNMP

Vous pouvez désactiver les notifications SNMP, mettre à jour les chaînes de communauté ou ajouter ou supprimer des adresses d'agent, des utilisateurs USM et des destinations d'interruption.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

Chaque fois que vous mettez à jour la configuration de l'agent SNMP, sachez que vous devez cliquer sur **Enregistrer** en bas de la page agent SNMP pour valider les modifications que vous avez effectuées sur chaque onglet.

Étapes

1. Sélectionnez **Configuration > surveillance > agent SNMP**.

La page agent SNMP s'affiche.

2. Pour désactiver l'agent SNMP sur tous les nœuds de la grille, décochez la case **Activer SNMP** et cliquez sur **Enregistrer**.

L'agent SNMP est désactivé pour tous les nœuds de la grille. Si vous réactivez ultérieurement l'agent, tous les paramètres de configuration SNMP précédents sont conservés.

3. Vous pouvez également mettre à jour les valeurs saisies pour **Contact système** et **emplacement système**.
4. Si vous ne souhaitez plus que l'agent SNMP StorageGRID envoie des interruptions et informe les notifications, désélectionnez la case à cocher **Activer les notifications d'agent SNMP**.

Lorsque cette case à cocher n'est pas sélectionnée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie aucune notification SNMP.

5. Si vous ne souhaitez plus que l'agent SNMP StorageGRID envoie un trap d'authentification lorsqu'il reçoit un message de protocole mal authentifié, désélectionnez la case à cocher **Activer les traps d'authentification**.
6. Si vous utilisez SNMPv1 ou SNMPv2c, vous pouvez mettre à jour la section chaînes de communauté.

Les champs de cette section sont utilisés pour l'authentification communautaire dans SNMPv1 ou SNMPv2c. Ces champs ne s'appliquent pas au protocole SNMPv3.



Si vous souhaitez supprimer la chaîne de communauté par défaut, vous devez d'abord vous assurer que toutes les destinations de déroutement utilisent une chaîne de communauté personnalisée.

7. Pour mettre à jour les adresses des agents, sélectionnez l'onglet adresses des agents dans la section autres configurations.

Other Configurations

Agent Addresses (2)			
USM Users (2)			
Trap Destinations (2)			
Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/> IPv4	UDP	Grid Network	161
<input checked="" type="radio"/> IPv4	UDP	Admin Network	161

Utilisez cet onglet pour spécifier une ou plusieurs « adresses d'écoute ». Ce sont les adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes. Chaque adresse de l'agent inclut un protocole Internet, un protocole de transport, un réseau StorageGRID et un port.

- a. Pour ajouter une adresse d'agent, cliquez sur **Créer**. Ensuite, reportez-vous à l'étape pour connaître les adresses des agents dans les instructions de configuration de l'agent SNMP.
 - b. Pour modifier une adresse d'agent, sélectionnez le bouton radio correspondant à l'adresse, puis cliquez sur **Modifier**. Ensuite, reportez-vous à l'étape pour connaître les adresses des agents dans les instructions de configuration de l'agent SNMP.
 - c. Pour supprimer une adresse d'agent, sélectionnez le bouton radio correspondant à l'adresse et cliquez sur **Supprimer**. Cliquez ensuite sur **OK** pour confirmer que vous souhaitez supprimer cette adresse.
 - d. Pour valider vos modifications, cliquez sur **Enregistrer** en bas de la page Agent SNMP.
8. Pour mettre à jour les utilisateurs USM, sélectionnez l'onglet utilisateurs USM dans la section autres configurations.

Other Configurations

Agent Addresses (2)			
USM Users (3)			
Trap Destinations (2)			
+	Create	Edit	Remove
Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/> user2	<input checked="" type="checkbox"/>	authNoPriv	
<input type="radio"/> user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/> user3		authPriv	59D39E801256

Utilisez cet onglet pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.

- a. Pour ajouter un utilisateur USM, cliquez sur **Créer**. Reportez-vous ensuite à l'étape pour les utilisateurs d'USM dans les instructions de configuration de l'agent SNMP.
- b. Pour modifier un utilisateur USM, sélectionnez le bouton radio de l'utilisateur, puis cliquez sur **Modifier**.

Reportez-vous ensuite à l'étape pour les utilisateurs d'USM dans les instructions de configuration de l'agent SNMP.

Le nom d'utilisateur d'un utilisateur USM existant ne peut pas être modifié. Si vous devez modifier un nom d'utilisateur, vous devez le supprimer et en créer un nouveau.



Si vous ajoutez ou supprimez l'ID moteur faisant autorité d'un utilisateur et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination, comme indiqué à l'étape [Destination du trap SNMP](#). Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

- c. Pour supprimer un utilisateur USM, sélectionnez le bouton radio de l'utilisateur et cliquez sur **Supprimer**. Cliquez ensuite sur **OK** pour confirmer que vous souhaitez supprimer cet utilisateur.



Si l'utilisateur que vous avez supprimé est actuellement sélectionné pour une destination de recouvrement, vous devez modifier ou supprimer la destination, comme indiqué à l'étape [Destination du trap SNMP](#). Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Undefined trap destination usmUser 'user1'

OK

- a. Pour valider vos modifications, cliquez sur **Enregistrer** en bas de la page Agent SNMP.

1. Pour mettre à jour les destinations de recouvrement, sélectionnez l'onglet destinations de recouvrement dans la section autres configurations.

Other Configurations

Agent Addresses (1) USM Users (2) Trap Destinations (2)

+ Create Edit Remove

Version	Type	Host	Port	Protocol	Community/USM User
SNMPv3	Trap	local		UDP	User: Read only user
SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user

L'onglet destinations de recouvrement permet de définir une ou plusieurs destinations pour les notifications d'interruption StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et cliquez sur **Enregistrer**, StorageGRID commence à envoyer des notifications à chaque destination définie. Des

notifications sont envoyées lorsque des alertes et des alarmes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

- a. Pour ajouter une destination d'interruption, cliquez sur **Créer**. Reportez-vous ensuite à l'étape pour connaître les destinations de déroutement dans les instructions de configuration de l'agent SNMP.
 - b. Pour modifier une destination de recouvrement, sélectionnez le bouton radio de l'utilisateur et cliquez sur **Modifier**. Reportez-vous ensuite à l'étape pour connaître les destinations de déroutement dans les instructions de configuration de l'agent SNMP.
 - c. Pour supprimer une destination d'interruption, sélectionnez le bouton radio de la destination, puis cliquez sur **Supprimer**. Cliquez ensuite sur **OK** pour confirmer que vous souhaitez supprimer cette destination.
 - d. Pour valider vos modifications, cliquez sur **Enregistrer** en bas de la page Agent SNMP.
2. Lorsque vous avez mis à jour la configuration de l'agent SNMP, cliquez sur **Enregistrer**.

Informations associées

["Configuration de l'agent SNMP"](#)

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.