Utiliser la surveillance SNMP

StorageGRID 11.8

NetApp
March 19, 2024

Sommaire

Utiliser la surveillance SNMP

Utiliser la surveillance SNMP : présentation

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

- "Configurez l'agent SNMP"
- "Mettez à jour l'agent SNMP"

Capacités

Chaque nœud StorageGRID exécute un agent SNMP, ou démon, qui fournit une 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.

Voir "Accéder aux fichiers MIB" Si vous souhaitez télécharger les fichiers MIB sur vos nœuds grid.

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 :

Recouvrements

Les interruptions 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.

Informe

Les informations sont similaires aux pièges, mais elles nécessitent une reconnaissance par le système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain délai, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de relance 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 "Nœud d'administration de l'expéditeur préféré".

  Chaque alerte est associée à l'un des trois types de déroutement en fonction du niveau de gravité de l'alerte : activeMinorAlert, activeMajorAlert et activeCriticalAlert. Pour obtenir la liste des alertes pouvant déclencher ces interruptions, reportez-vous au "Référence des alertes".

- Certains "alarmes (système hérité)" sont déclenchées à un niveau de sévérité spécifié ou supérieur.

> 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.

Configurez l'agent SNMP

Vous pouvez configurer l'agent SNMP StorageGRID pour qu'il utilise un système de gestion SNMP tiers pour l'accès MIB en lecture seule et les notifications.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Description de la tâche

L'agent SNMP StorageGRID prend en charge SNMPv1, SNMPv2c et SNMPv3. Vous pouvez configurer l'agent pour une ou plusieurs versions. Pour SNMPv3, seule l'authentification USM (User Security Model) est prise en charge.

Tous les nœuds de la grille utilisent la même configuration SNMP.

Spécifiez la configuration de base

Dans un premier temps, activez l'agent SMNP StorageGRID et fournissez des informations de base.

Étapes

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

   La page agent SNMP s'affiche.

2. Pour activer l'agent SNMP sur tous les nœuds de la grille, cochez la case **Activer SNMP**.
3. Entrez les informations suivantes dans la section Configuration de base.

Champ	Description
Contact système	Facultatif. Le contact principal du système StorageGRID, qui est renvoyé dans les messages SNMP en tant que sysContact. Le contact système est généralement une adresse e-mail. Cette valeur s'applique à tous les nœuds du système StorageGRID. **Le contact système** peut comporter un maximum de 255 caractères.
Emplacement du système	Facultatif. Emplacement du système StorageGRID, qui est renvoyé dans les messages SNMP sous le nom 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. Cette valeur s'applique à tous les nœuds du système StorageGRID. **L'emplacement du système** peut comporter un maximum de 255 caractères.
Activer les notifications d'agent SNMP	• Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information. • Si cette option n'est pas sélectionnée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie pas de notifications SNMP.
Activer les interruptions d'authentification	Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des interruptions d'authentification s'il reçoit des messages de protocole authentifiés de manière incorrecte.

Entrez des chaînes de communauté

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

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.

Étapes

1. Pour **communauté en lecture seule**, vous pouvez éventuellement entrer une chaîne de communauté pour autoriser l'accès MIB en lecture seule sur les adresses d'agent IPv4 et IPv6.

   Pour garantir la sécurité de votre système StorageGRID, n'utilisez pas la chaîne de communauté « public ». Si vous laissez ce champ vide, l'agent SNMP utilise l'ID de grille de votre système StorageGRID comme chaîne de communauté.

   Chaque chaîne de communauté peut comporter un maximum de 32 caractères et ne peut pas contenir de caractères d'espace.

2. Sélectionnez **Ajouter une autre chaîne de communauté** pour ajouter des chaînes supplémentaires.

   Jusqu'à cinq chaînes sont autorisées.

Créer des destinations de déroutement

Utilisez l'onglet destinations d'interruption de la section autres configurations pour définir une ou plusieurs destinations pour les notifications d'interruption ou d'information StorageGRID. Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**, StorageGRID envoie des notifications à chaque destination définie lorsque des alertes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

Étapes

1. Pour le champ **Default trap community**, vous pouvez éventuellement saisir la chaîne de communauté par défaut que vous souhaitez utiliser pour les destinations d'interruption SNMPv1 ou SNMPv2.

   Si nécessaire, vous pouvez fournir une chaîne de communauté différente (« personnalisée ») lorsque vous définissez une destination d'interruption spécifique.

   La communauté de recouvrement par défaut peut comporter 32 caractères maximum et ne peut pas contenir de caractères d'espace.

2. Pour ajouter une destination d'interruption, sélectionnez **Créer**.
3. Sélectionnez la version SNMP qui sera utilisée pour cette destination d'interruption.
4. Remplissez le formulaire Créer une destination d'interruption pour la version que vous avez sélectionnée.

SNMPv1

Si vous avez sélectionné SNMPv1 comme version, renseignez ces champs.

Champ	Description
Type	Doit être Trap pour SNMPv1.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet (FQDN) pour recevoir l'interruption.
Port	Utilisez 162, le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de déroutement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Chaîne de communauté	Utilisez la communauté d'interruptions par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruptions. La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.

SNMPv2c

Si vous avez sélectionné SNMPv2c comme version, renseignez ces champs.

Champ	Description
Type	Indique si la destination sera utilisée pour les interruptions ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet pour recevoir l'interruption.
Port	Utilisez 162, qui est le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de déroutement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Chaîne de communauté	Utilisez la communauté d'interruptions par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruptions. La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.

SNMPv3

Si vous avez sélectionné SNMPv3 comme version, renseignez ces champs.

Champ	Description
Type	Indique si la destination sera utilisée pour les interruptions ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet pour recevoir l'interruption.
Port	Utilisez 162, qui est le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de déroutement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Utilisateur USM	Utilisateur USM qui sera utilisé pour l'authentification. • 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. • Si aucun utilisateur n'est affiché : i. Créez et enregistrez la destination de l'interruption. ii. Accédez à Créez des utilisateurs USM et créez l'utilisateur. iii. Revenez à l'onglet destinations des interruptions, sélectionnez la destination enregistrée dans le tableau et sélectionnez **Modifier**. iv. Sélectionnez l'utilisateur.

5. Sélectionnez **Créer**.

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

Créez des adresses d'agent

Vous pouvez également utiliser l'onglet adresses des agents de la section autres configurations pour spécifier une ou plusieurs « adresses d'écoute ». Il s'agit des adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes.

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.

Étapes

1. Sélectionnez **Créer**.
2. Entrez les informations suivantes.

Champ	Description
Protocole Internet	Indique si cette adresse utilisera IPv4 ou IPv6. Par défaut, SNMP utilise IPv4.
Protocole de transport	Indique si cette adresse utilise UDP ou TCP. Par défaut, SNMP utilise UDP.
Réseau StorageGRID	Quel réseau StorageGRID l'agent écoutera ? • Réseaux Grid, Admin et client : l'agent SNMP écoute les requêtes sur les trois réseaux. • Réseau Grid • Réseau d'administration • Réseau client **Remarque** : si vous utilisez le réseau client pour des données non sécurisées et que vous créez une adresse d'agent pour le réseau client, sachez que le trafic SNMP sera également non sécurisé.
Port	Éventuellement, le numéro de port sur lequel 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. **Remarque** : 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.

3. Sélectionnez **Créer**.

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

Créez des utilisateurs USM

Si vous utilisez SNMPv3, utilisez l'onglet utilisateurs USM de la section autres configurations pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.

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

Ces étapes ne s'appliquent pas si vous utilisez uniquement SNMPv1 ou SNMPv2c.

Étapes

1. Sélectionnez **Créer**.
2. Entrez les informations suivantes.

Champ	Description
Nom d'utilisateur	Un nom unique pour cet utilisateur USM. Les noms d'utilisateur peuvent comporter jusqu'à 32 caractères et ne peuvent pas contenir de caractères d'espace. Le nom d'utilisateur ne peut pas être modifié après la création de l'utilisateur.
Accès MIB en lecture seule	Si cette option est sélectionnée, cet utilisateur doit disposer d'un accès en lecture seule à la MIB.
ID de moteur autoritaire	Si cet utilisateur sera utilisé dans une destination INFORM, l'ID de moteur faisant autorité pour cet utilisateur. Entrez 10 à 64 caractères hexadécimaux (5 à 32 octets) sans espace. Cette valeur est requise pour les utilisateurs USM qui seront sélectionnés dans les destinations d'interruption pour les informations. Cette valeur n'est pas autorisée pour les utilisateurs USM qui seront sélectionnés dans les destinations d'interruption pour les interruptions. **Remarque** : ce champ n'est pas affiché si vous avez sélectionné **accès MIB en lecture seule** car les utilisateurs USM qui ont un accès MIB en lecture seule ne peuvent pas avoir d'ID moteur.
Niveau de sécurité	Le niveau de sécurité de 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.
Protocole d'authentification	Toujours défini sur SHA, qui est le seul protocole pris en charge (HMAC-SHA-96).
Mot de passe	Le mot de passe que cet utilisateur utilisera pour l'authentification.
Protocole de confidentialité	Affiché uniquement si vous avez sélectionné **authPriv** et toujours réglé sur AES, qui est le seul protocole de confidentialité pris en charge.
Mot de passe	Affiché uniquement si vous avez sélectionné **authPriv**. Le mot de passe que cet utilisateur utilisera pour la confidentialité.

3. Sélectionnez **Créer**.

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

4. Une fois la configuration de l'agent SNMP terminée, sélectionnez **Enregistrer**.

   La nouvelle configuration de l'agent SNMP devient active.

Mettez à jour 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.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Description de la tâche

Voir "Configurez l'agent SNMP" Pour plus de détails sur chaque champ de la page agent SNMP. Vous devez sélectionner **Enregistrer** au bas de la page pour valider les modifications que vous apportez à 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 sélectionnez **Enregistrer**.

   Si vous réactivez l'agent SNMP, tous les paramètres de configuration SNMP précédents sont conservés.

3. Si vous le souhaitez, mettez à jour les informations de la section Configuration de base :
   a. Si nécessaire, mettez à jour le **contact système** et **emplacement système**.
   b. Vous pouvez également cocher ou décocher la case **Activer les notifications d'agent SNMP** pour contrôler si l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.

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

   c. Si vous le souhaitez, cochez ou décochez la case **Activer les interruptions d'authentification** pour contrôler si l'agent SNMP StorageGRID envoie des interruptions d'authentification lorsqu'il reçoit des messages de protocole incorrectement authentifiés.
4. Si vous utilisez SNMPv1 ou SNMPv2c, vous pouvez éventuellement mettre à jour ou ajouter une communauté **en lecture seule** dans la section chaînes de communauté.
5. Pour mettre à jour les destinations des interruptions, sélectionnez l'onglet destinations des interruptions dans la section autres configurations.

   Utilisez cet onglet pour définir une ou plusieurs destinations pour les notifications d'interruption StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**,

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

Pour plus d'informations sur ce que vous devez saisir, reportez-vous à la section "Créer des destinations de recouvrement".

- Vous pouvez également mettre à jour ou supprimer la communauté de déroutements par défaut.

  Si vous supprimez la communauté d'interruptions par défaut, vous devez d'abord vous assurer que toutes les destinations d'interruptions existantes utilisent une chaîne de communauté personnalisée.

- Pour ajouter une destination d'interruption, sélectionnez **Créer**.
- Pour modifier une destination d'interruption, sélectionnez le bouton radio et sélectionnez **Modifier**.
- Pour supprimer une destination d'interruption, sélectionnez le bouton radio et sélectionnez **Supprimer**.
- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

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

   Utilisez cet onglet pour spécifier une ou plusieurs « adresses d'écoute ». Il s'agit des adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes.

   Pour plus d'informations sur ce que vous devez saisir, reportez-vous à la section "Créez des adresses d'agent".

   - Pour ajouter une adresse d'agent, sélectionnez **Créer**.
   - Pour modifier une adresse d'agent, sélectionnez le bouton radio et sélectionnez **Modifier**.
   - Pour supprimer une adresse d'agent, sélectionnez le bouton radio et sélectionnez **Supprimer**.
   - Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

7. Pour mettre à jour les utilisateurs USM, 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.

   Pour plus d'informations sur ce que vous devez saisir, reportez-vous à la section "Créez des utilisateurs USM".

   - Pour ajouter un utilisateur USM, sélectionnez **Create**.
   - Pour modifier un utilisateur USM, sélectionnez le bouton radio et sélectionnez **Modifier**.

     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 de moteur d'un utilisateur faisant autorité et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

   - Pour supprimer un utilisateur USM, sélectionnez le bouton radio et sélectionnez **Supprimer**.

Si l'utilisateur que vous avez supprimé est actuellement sélectionné pour une destination d'interruption, vous devez modifier ou supprimer la destination. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

8. Lorsque vous avez mis à jour la configuration de l'agent SNMP, sélectionnez **Enregistrer**.

Accéder aux fichiers MIB

Les fichiers MIB contiennent des définitions et des informations sur les propriétés des ressources et services gérés pour les nœuds de votre grille. Vous pouvez accéder aux fichiers MIB qui définissent les objets et les notifications pour StorageGRID. Ces fichiers peuvent être utiles pour la surveillance de votre grille.

Voir "Utiliser la surveillance SNMP" Pour plus d'informations sur les fichiers SNMP et MIB.

Accéder aux fichiers MIB

Procédez comme suit pour accéder aux fichiers MIB.

Étapes

1. Sélectionnez **CONFIGURATION** > **surveillance** > **agent SNMP**.
2. Sur la page agent SNMP, sélectionnez le fichier à télécharger :
   - **NETAPP-STORAGEGRID-MIB.txt** : définit la table d'alertes et les notifications (traps) accessibles sur tous les noeuds d'administration.
   - **ES-NETAPP-06-MIB.mib** : définit les objets et les notifications pour les appliances basées sur E-Series.
   - **MIB_1_10.zip** : définit les objets et les notifications pour les appareils dotés d'une interface BMC.

   Vous pouvez également accéder aux fichiers MIB à l'emplacement suivant sur n'importe quel nœud StorageGRID : `/usr/share/snmp/mibs`

3. Pour extraire les OID StorageGRID du fichier MIB :

   a. Obtenir l'OID de la racine de la MIB StorageGRID :

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

   Résultat : `.1.3.6.1.4.1.789.28669` (`28669` Est toujours l'OID pour StorageGRID)

   a. Grep pour l'OID StorageGRID dans toute l'arborescence (utilisation de `paste` pour joindre des lignes) :

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

Le `snmptranslate` Command a de nombreuses options qui sont utiles pour explorer la MIB. Cette commande est disponible sur n'importe quel nœud StorageGRID.

Contenu du fichier MIB

Tous les objets se trouvent sous l'OID StorageGRID.

Nom de l'objet	ID objet (OID)	Description
iso.org.dod.internet. entreprises privées. netapp.storagegrid		Le module MIB pour les entités NetApp StorageGRID.

Objets MIB

Nom de l'objet	ID objet (OID)	Description
ActiveAlertCount	**1.3.6.1.4.1.** 789.28669.1.3	Nombre d'alertes actives dans activeAlertTable.
ActiveAlertTable	**1.3.6.1.4.1.** 789.28669.1.4	Tableau des alertes actives dans StorageGRID.
ActiveAlertId	**1.3.6.1.4.1.** 789.28669.1.4.1.1	ID de l'alerte. Uniquement unique dans l'ensemble actuel d'alertes actives.
ActiveAlertName	**1.3.6.1.4.1.** 789.28669.1.4.1.2	Nom de l'alerte.
ActiveAlertInstance	**1.3.6.1.4.1.** 789.28669.1.4.1.3	Nom de l'entité qui a généré l'alerte, en général le nom du nœud.
ActiveAlertSeverity	**1.3.6.1.4.1.** 789.28669.1.4.1.4	Gravité de l'alerte.
ActiveAlertStartTime	**1.3.6.1.4.1.** 789.28669.1.4.1.5	Date et heure de déclenchement de l'alerte.

Types de notification (interruptions)

Toutes les notifications incluent les variables suivantes en tant que variables :

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance

- ActiveAlertSeverity
- ActiveAlertStartTime

Type de notification	ID objet (OID)	Description
ActiveMinorAlert	**1.3.6.1.4.1.** 789.28669.0.6	Alerte avec gravité mineure
ActiveMajorAlert	**1.3.6.1.4.1.** 789.28669.0.7	Alerte de gravité majeure
ActiveCriticalAlert	**1.3.6.1.4.1.** 789.28669.0.8	Alerte avec gravité critique

Informations sur le copyright

Informations sur les marques commerciales