

# MIB SNMP

Ce chapitre décrit comment configurer le protocole simple de gestion de réseau (SNMP) pour superviser l'ASA.


- À propos de SNMP, à la page 1
- Lignes directrices pour SNMP, à la page 4
- Configurer SNMP, à la page 8
- Supervision SNMP, à la page 15
- Historique de SNMP, à la page 16


# À propos de SNMP

SNMP est un protocole de couche d'application qui facilite l'échange d'informations de gestion entre les appareils réseau et fait partie de la suite de protocoles TCP /IP. L'ASA prend en charge la surveillance du réseau à l'aide des versions SNMP 1, 2c et 3 de SNMP, et prend en charge l'utilisation des trois versions simultanément. L'agent SNMP qui s'exécute sur l'interface ASA vous permet de surveiller les périphériques réseau à l'aide de systèmes de gestion par réseau (Network Management Systems ou NMS), comme HP OpenView. L'ASA prend en charge l'accès SNMP en lecture seule par l'émission d'une requête GET. L'accès en écriture SNMP n'est pas autorisé, vous ne pouvez donc pas effectuer de modifications avec SNMP. En outre, la requête SNMP SET n'est pas prise en charge.

Vous pouvez configurer la ASA pour envoyer des déroutements, qui sont des messages non sollicités du périphérique géré vers le poste de gestion pour certains événements (notifications d'événement) à un système de gestion de réseau, ou vous pouvez utiliser le système de gestion de réseau pour parcourir les bases d'information de gestion (MIB) sur le périphériques de sécurité. Les MIB sont un ensemble de définitions, et les ASA gèrent une base de données de valeurs pour chaque définition. Parcourir une MIB signifie émettre une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du système NMS pour déterminer les valeurs.

**Remarque** Avec des charges de travail intensives, le déploiement de plus de 10 NMS peut avoir une incidence sur les performances de l'appareil. Pour assurer la stabilité et la réactivité de l'appareil, nous vous conseillons d'utiliser avec prudence NMS pour effectuer des interrogations SNMP et gérer le trafic d'interruption.

Les ASA possèdent un agent SNMP qui informe les stations de gestion désignées si des événements prédéfinis nécessitent une notification, par exemple, lorsqu'une liaison du réseau monte ou tombe en panne. La notification

qu'il envoie comprend un OID SNMP, qui s'identifie aux stations de gestion. L'agent ASA répond également lorsqu'une station de gestion demande des renseignements.

# Terminologie SNMP

Le tableau suivant répertorie les termes couramment utilisés avec SNMP.

***Tableau 1 : Terminologie SNMP***

| Terme | Description |
|---|---|
| Agent | Le serveur SNMP exécuté sur ASA. L'agent SNMP présente les caractéristiques suivantes :<br>• Répond aux demandes d'informations et d'actions du poste de gestion de réseau.<br>• Contrôle l'accès à sa base d'information de gestion, l'ensemble d'objets que le gestionnaire SNMP peut afficher ou modifier.<br>• N'autorise pas les opérations SET. |
| Navigation | Surveille l'intégrité d'un périphérique à partir du poste de gestion de réseau en interrogeant les informations requises de l'agent SNMP sur le périphérique. Cette activité peut comprendre l'émission d'une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du poste de gestion de réseau afin de déterminer les valeurs. |
| Bases d'informations de gestion (MIB) | Structures de données normalisées pour la collecte d'informations sur les paquets, les connexions, les tampons, les basculements, etc. Les MIB sont définies par le produit, les protocoles et les normes matérielles utilisés par la plupart des périphériques réseau. Les stations de gestion de réseau SNMP peuvent parcourir les MIB et demander l'envoi de données ou d'événements précis au fur et à mesure qu'ils se produisent. |
| Postes de gestion de réseau (NSM, Network Management Station) | Les ordinateurs ou postes de travail configurés pour superviser les événements SNMP et gérer les périphériques, tels que l'ASA |
| Identifiant d'objet (OID) | Le système qui identifie un appareil auprès de son système de gestion système et indique aux utilisateurs la source des renseignements surveillés et affichés. |
| Trap | Événements prédéfinis qui génèrent un message de l'agent SNMP au système NMS. Les événements comprennent des conditions d'alarme telles qu'un démarrage, un retrait, un démarrage à froid, un démarrage à chaud, une authentification ou des messages syslog. |

# Présentation du SNMP version 3

SNMP version 3 offre des améliorations de sécurité qui ne sont pas disponibles dans les versions SNMP 1 et 2c. Les versions SNMP 1 et 2c transmettent des données entre le serveur SNMP et l'agent SNMP en texte clair. SNMP version 3 ajoute des options d'authentification et de confidentialité pour sécuriser les opérations du protocole. En outre, cette version contrôle l'accès à l'agent SNMP et aux objets MIB par le biais du modèle de sécurité basé sur l'utilisateur (USM) et du modèle de contrôle d'accès basé sur l'affichage (VACM). L'ASA prend également en charge la création de groupes SNMP et d'utilisateurs, ainsi que d'hôtes, ce qui est nécessaire pour activer l'authentification et le chiffrement du transport pour des communications SNMP sécurisées.

## Modèles de sécurité

À des fins de configuration, les options d'authentification et de confidentialité sont regroupées dans des modèles de sécurité. Les modèles de sécurité s'appliquent aux utilisateurs et aux groupes, qui sont répartis dans les trois types suivants :

- NoAuthPriv : pas d'authentification ni de confidentialité, ce qui signifie qu'aucune sécurité n'est appliquée aux messages.
- AuthNoPriv : authentification mais pas de confidentialité, ce qui signifie que les messages sont authentifiés.
- AuthPriv : authentification et confidentialité, ce qui signifie que les messages sont authentifiés et chiffrés.

## SNMP Groups (groupes SNMP)

Un groupe SNMP est une stratégie de contrôle d'accès à laquelle des utilisateurs peuvent être ajoutés. Chaque groupe SNMP est configuré avec un modèle de sécurité et est associé à une vue SNMP. Un utilisateur appartenant à un groupe SNMP doit correspondre au modèle de sécurité du groupe SNMP. Ces paramètres spécifient le type d'authentification et de confidentialité utilisé par un utilisateur appartenant à un groupe SNMP. Chaque paire de noms de groupes SNMP et de modèles de sécurité doit être unique.

## Utilisateurs SNMP

Les utilisateurs SNMP disposent d'un nom d'utilisateur spécifié, d'un groupe auquel ils appartiennent, d'un mot de passe d'authentification, d'un mot de passe de chiffrement et d'algorithmes d'authentification et de chiffrement à utiliser. Les options d'algorithme d'authentification sont SHA-1, SHA-224, SHA-256 HMAC et SHA-384. Les options d'algorithme de chiffrement sont 3DES et AES (qui sont disponibles en versions 128, 192 et 256). Lorsque vous créez un utilisateur, vous devez l'associer à un groupe SNMP. L'utilisateur hérite ensuite du modèle de sécurité du groupe.



**Remarque** Lors de la configuration d'un compte d'utilisateur SNMPv3, assurez-vous que la longueur de l'algorithme d'authentification est égale ou supérieure à la longueur de l'algorithme de chiffrement.

## Hôtes SNMP

Un hôte SNMP est une adresse IP à laquelle les notifications et les alertes SNMP sont envoyées. Pour configurer les hôtes SNMP version 3, ainsi que l'adresse IP cible, vous devez configurer un nom d'utilisateur, car les alertes ne sont envoyées qu'à un utilisateur configuré. Les adresses IP cibles SNMP et les noms de paramètre cibles doivent être uniques sur l'ASA. Chaque hôte SNMP ne peut être associé qu'à un seul nom d'utilisateur. Pour recevoir des alertes SNMP, configurez le NMS SNMP et assurez-vous de configurer les renseignements d'authentification de l'utilisateur sur le NMS pour qu'ils correspondent aux renseignements d'authentification de l'ASA.



**Remarque** Vous pouvez ajouter jusqu'à 8 192 hôtes. Cependant, seulement 128 de ceux-ci peuvent être utilisés pour les déroutements.

## Différences d'implémentation entre les logiciels ASA et Cisco IOS

La mise en œuvre de SNMP version 3 dans l'ASA diffère de la mise en œuvre de SNMP version 3 dans le logiciel Cisco IOS de la manière suivante :

- Les ID du moteur local et du moteur distant ne sont pas configurables. L'ID du moteur local est généré au démarrage de l'ASA ou lors de la création d'un contexte.
- Aucune prise en charge n'existe pour le contrôle d'accès basé sur l'affichage, ce qui entraîne une navigation MIB non limitée.
- La prise en charge est limitée aux MIB suivantes : USM, VACM, FRAMEWORK et TARGET.
- Vous devez créer des utilisateurs et des groupes avec le modèle de sécurité approprié.
- Vous devez supprimer les utilisateurs, les groupes et les hôtes dans le bon ordre.
- L'utilisation de la commande snmp-server host crée une règle ASA pour autoriser le trafic SNMP entrant.

# Messagerie du journal système SNMP

SNMP génère des messages de journal système détaillés, numérotés 212*nnn*. Les messages du journal système indiquent l'état des requêtes SNMP, des interruptions SNMP, des canaux SNMP et des réponses SNMP de l'ASA ou de l'ASASM à un hôte spécifié sur une interface spécifiée.

Pour obtenir des renseignements détaillés sur les messages du journal système, consultez le guide des messages de journal système.

**Remarque** L'interrogation SNMP échoue si les messages de journal système du protocole SNMP dépassent un débit élevé (environ 4 000 par seconde).

# Services d'application et outils tiers

Pour en savoir plus sur la prise en charge de SNMP, consultez l'URL suivante :

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

Pour en savoir plus, consultez le chapitre SNMP du Guide de configuration d'ASDM pour les opérations générales Cisco ASA à l'URL suivante :

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

# Lignes directrices pour SNMP

Cette section comprend les lignes directrices et les limites que vous devez consulter avant de configurer SNMP.

### Lignes directrices en matière de basculement et de mise en grappe

- Lorsque vous utilisez SNMPv3 avec mise en grappe ou basculement, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité de contrôle ou active pour forcer les utilisateurs à être dupliqués sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité (les utilisateurs et les groupes SNMPv3 sont une exception à la règle selon laquelle vous ne pouvez pas saisir de commandes de configuration sur une unité de données en grappe). Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité de contrôle/active ou directement sur l'unité de données/secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

### Lignes directrices relatives à IPv6 (tous les modèles ASA)

SNMP peut être configuré sur le transport IPv6 de sorte qu'un hôte IPv6 puisse exécuter des requêtes SNMP et recevoir des notifications SNMP d'un périphérique exécutant le logiciel IPv6. L'agent SNMP et les MIB associées ont été améliorés pour prendre en charge l'adressage IPv6.

### Lignes directrices relatives à IPv6 pour Firepower 2100

Firepower 2100 exécute un système d'exploitation sous-jacent appelé FXOS et prend en charge le mode appareil (par défaut) et le mode plateforme; voir Régler le Firepower 2100 en mode appareil ou plateforme.

En mode plateforme, vous devez configurer une adresse IP de gestion IPv6 dans FXOS. Dans l'exemple suivant, une passerelle et une interface de gestion IPv6 sont configurées :

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
IPv6 Address Prefix IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

### Directives supplémentaires

- Les interruptions d'alimentation ne sont pas émises pour les systèmes fonctionnant en mode appareil.
- Pour Firepower 2100, en mode plateforme, vous ne pouvez pas interroger les interfaces membres d'un EtherChannel, et les interruptions pour les interfaces membres ne sont pas générées. Cette fonctionnalité est prise en charge si vous activez SNMP directement dans FXOS. Le mode appareil n'est pas affecté.
- Ne prend pas en charge les interruptions ASA pour les membres de ports individuels pour le Firepower 2100 en mode plateforme; consultez le Guide de référence de Cisco Firepower 2100 FXOS MIB.
- Pour Firepower 2100, en mode appareil, vous ne pouvez pas interroger le modèle matériel ni le numéro de série. De plus, dans l'ASA, les interruptions ne sont pas générées pour ces détails. Par conséquent, configurez SNMP sur FXOS ou Chassis Manager pour interroger l'adresse IP de gestion de châssis au lieu des interfaces sur l'instance ASA.

- Vous devez disposer de Cisco Works pour Windows ou d'un autre navigateur conforme à SNMP MIB-II pour recevoir des alertes SNMP ou parcourir une MIB.
- L'accès de gestion sur un tunnel VPN n'est pas pris en charge avec SNMP (la commande **management-access**). Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.
- Ne prend pas en charge le contrôle d'accès basé sur l'affichage, mais il est possible de parcourir la MIB VACM pour déterminer les paramètres d'affichage par défaut.
- ENTITY-MIB n'est pas disponible dans le contexte de non-administration. Utilisez plutôt IF-MIB pour effectuer des requêtes dans le contexte de non-administration.
- ENTITY-MIB n'est pas disponible pour le Firepower 9300. Utilisez plutôt CISCO-FIREPOWER-EQUIPMENT-MIB et CISCO-FIREPOWER-SM-MIB.
- Sur certains périphériques, il a été observé que l'ordre des interfaces (ifDescr) dans la sortie de **snmpwalk** change après un redémarrage. L'ASA utilise un algorithme pour déterminer le tableau ifIndex que SNMP interroge. Lorsque l'ASA est démarré, les interfaces sont ajoutées au tableau ifIndex dans l'ordre chargé au fur et à mesure que l'ASA lit la configuration. Les nouvelles interfaces ajoutées à l'ASA sont ajoutées à la liste des interfaces dans le tableau ifIndex. Lorsque des interfaces sont ajoutées, supprimées ou renommées, cela peut affecter l'ordre des interfaces lors du redémarrage.
- Lorsque vous fournissez un OID dans la commande **snmpwalk**, l'outil snmpwalk interroge toutes les variables de la sous-arborescence qui se trouve sous l'OID spécifié et affiche leurs valeurs. Ainsi, pour afficher une sortie complète des objets sur le périphérique, assurez-vous de fournir l'OID dans la commande **snmpwalk**.
- Ne prend pas en charge la version 3 du SNMP pour AIP SSM ou AIP SSC.
- Ne prend pas en charge le débogage SNMP.
- Ne prend pas en charge la récupération des renseignements ARP.
- Ne prend pas en charge les commandes SNMP NET.
- Lorsque vous utilisez NET-SNMP version 5.4.2.1, prend uniquement en charge la version de l'algorithme de chiffrement AES128. Ne prend pas en charge les versions des algorithmes de chiffrement AES256 ou AES192.
- Les modifications apportées à la configuration existante sont refusées si le résultat place la fonctionnalité SNMP dans un état incohérent.
- Pour la version 3 de SNMP, la configuration doit avoir lieu dans l'ordre suivant : groupe, utilisateur, hôte.
- Pour Firepower 2100, lorsque SNMPv3 est configuré sur l'interface de gestion des périphériques, tous les utilisateurs de SNMPv3 peuvent interroger le périphérique même lorsqu'ils ne sont pas mappés dans la configuration de l'hôte.
- Pour les modèles Secure Firewall, la commande **snmpwalk** interroge les membres FXOS uniquement à partir du contexte d'administration.
- Avant de supprimer un groupe, vous devez vous assurer que tous les utilisateurs associés à ce groupe sont supprimés.

- Avant de supprimer un utilisateur, vous devez vous assurer qu'aucun hôte associé à ce nom d'utilisateur n'est configuré.
- Si les utilisateurs ont été configurés pour appartenir à un groupe particulier avec un certain modèle de sécurité, et si le niveau de sécurité de ce groupe est modifié, vous devez effectuer les opérations suivantes dans cet ordre :
  - Supprimer les utilisateurs de ce groupe.
  - Modifier le niveau de sécurité du groupe.
  - Ajouter des utilisateurs qui appartiennent au nouveau groupe.
- La création de vues personnalisées pour restreindre l'accès des utilisateurs à un sous-ensemble d'objets MIB n'est pas prise en charge.
- Toutes les requêtes et toutes les interruptions sont disponibles uniquement dans la vue Lecture/Notification par défaut.
- L'interruption de la limite de connexion atteinte est générée dans le contexte d'administration. Pour générer cette interruption, vous devez avoir au moins un hôte de serveur SNMP configuré dans le contexte d'utilisateur dans lequel la limite de connexion a été atteinte.
- Si le NMS ne parvient pas à demander des objets avec succès ou ne gère pas correctement les interruptions entrantes de l'ASA, la capture de paquets est la méthode la plus utile pour déterminer le problème. Choisissez **Wizards (Assistants) > Packet Capture Wizard (Assistant de capture de paquets)** et suivez les instructions à l'écran.
- Vous pouvez ajouter jusqu'à 4 000 hôtes. Cependant, seulement 128 de ceux-ci peuvent être utilisés pour les déroutements.
- Le nombre total de destinations d'interrogation actives prises en charge est de 128.
- Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes.
- Vous pouvez associer plusieurs utilisateurs à un hôte.
- Vous pouvez spécifier des objets réseau qui se chevauchent dans différentes commandes **host-group**. Les valeurs que vous spécifiez pour le dernier groupe d'hôtes s'appliquent à l'ensemble commun d'hôtes dans les différents objets réseau.
- Si vous supprimez un groupe d'hôtes ou des hôtes qui se chevauchent avec d'autres groupes d'hôtes, les hôtes sont reconfigurés en utilisant les valeurs qui ont été spécifiées dans les groupes d'hôtes configurés.
- Les valeurs acquises par les hôtes dépendent de la séquence spécifiée que vous utilisez pour exécuter les commandes.
- La limite de taille des messages que SNMP envoie est de 1 472 octets.
- L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique.

# Configurer SNMP

Cette section décrit comment configurer SNMP.

**Procédure**

**Étape 1** Configurez une station de gestion SNMP pour recevoir les demandes de l'ASA.

**Étape 2** Configurez les alertes SNMP.

**Étape 3** Configurez les paramètres SNMP de version 1 et 2c ou les paramètres SNMP de version 3.

## Configurer une station de gestion SNMP

Pour configurer une station de gestion SNMP, procédez comme suit :

**Procédure**

**Étape 1** Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**. Par défaut, le serveur SNMP est activé.

**Étape 2** Cliquez sur **Add** (Ajouter) dans le volet **SNMP Management Stations** (Stations de gestion SNMP).

La boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP) s'affiche.

**Étape 3** Choisissez l'interface sur laquelle se trouve l'hôte SNMP.

**Étape 4** Entrez l'adresse IP de l'hôte SNMP.

**Étape 5** Saisissez le port UDP de l'hôte SNMP ou conservez la valeur par défaut, le port 162.

**Étape 6** Ajoutez l'identifiant de communauté de l'hôte SNMP. Si aucun identifiant de communauté n'est précisé pour une station de gestion, la valeur définie dans le champ **Community String** (Identifiant de communauté) (par défaut) du volet **SNMP Management Stations** (Stations de gestion SNMP) est utilisée.

**Étape 7** Choisissez la version SNMP utilisée par l'hôte SNMP.

**Étape 8** Si vous avez sélectionné la version 3 du SNMP à l'étape précédente, choisissez le nom d'un utilisateur configuré.

**Étape 9** Pour spécifier la méthode de communication avec ce NMS, cochez la case **Poll** (Interrogation) ou **Trap** (Interruption).

**Étape 10** Cliquez sur **OK**.

La boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP) se ferme.

**Étape 11** Cliquez sur **Apply** (Appliquer).

Le NMS est configuré et les modifications sont enregistrées dans la configuration en cours d'exécution. Pour en savoir plus, consultez le chapitre SNMP du Guide de configuration d'ASDM pour les opérations générales Cisco ASA à l'URL suivante :

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

# Configurer les déroutements SNMP

Pour désigner les interruptions que l'agent SNMP génère et la manière dont elles sont collectées et envoyées aux NMS, procédez comme suit :

**Remarque** Lorsque vous activez toutes les alertes de SNMP ou de syslog, il est possible que le processus SNMP consomme les ressources excédentaires de l'agent et du réseau, ce qui entraîne le blocage du système. Si vous remarquez des retards du système, des demandes non terminées ou des échéances de délais d'expiration, vous pouvez activer de manière sélective les déroutements SNMP et syslog. Par exemple, vous pouvez ignorer le niveau de gravité *Informational* (Informationnel) de l'interruption de journal système.

### Procédure

**Étape 1** Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**.

**Étape 2** Cliquez sur **Configure Traps** (Configurer les interruptions).

La boîte de dialogue **SNMP Trap Configuration** (Configuration de l'interruption SNMP) s'affiche.

**Étape 3** Cochez la case **SNMP Server traps configuration** (Configuration des interruptions de serveur SNMP).

Toutes les interruptions standard SNMP sont activées dans la configuration par défaut. Si vous ne spécifiez pas de type d'interruption, la valeur par défaut est l'interruption **syslog** (journal système). Les alertes SNMP par défaut continuent d'être activées avec l'interruption **syslog** (journal système). Toutes les autres interruptions sont désactivées par défaut. Pour désactiver une interruption, décochez la case applicable.

Les interruptions sont classées dans les catégories suivantes :

a) **Standard SNMP Traps** (Alertes SNMP standard), cochez tout ce qui s'applique.

Choisissez parmi **Critical CPU temperature** (Température du CPU critique), **Chassis temperature** (Température du châssis), et **Chassis Fan Failure** (Défaillance du ventilateur du châssis).

**Remarque** Toutes les interruptions standard SNMP sont activées dans la configuration par défaut.

b) **Environment Traps** (Interruptions d'environnement), cochez tout ce qui s'applique.

Choisissez parmi **Authentication** (Authentification), **Link up** (Reconnexion), **Link down** (Déconnexion), **Cold start** (Démarrage à froid) et **Warm start** (Démarrage à chaud).

c) **Ikev2 Traps** (Interruptions Ikev2), cochez tout ce qui s'applique.

Choisissez parmi **Start** (Démarrer) et **Stop** (Arrêter).

d) **Entity MIB Notifications** (Notifications MIB de l'entité).

Cochez cet élément pour recevoir des notifications sur les unités remplaçables sur site.

e) **IPsec Traps** (Interruptions IPsec), cochez tout ce qui s'applique.

Choisissez parmi **Start** (Démarrer) et **Stop** (Arrêter).

f) **Remote Access Traps** (Interruptions d'accès à distance).

Cochez cet élément pour recevoir des notifications lorsque le nombre de sessions établies dépasse le seuil défini.

g) **Resource Traps** (Interruptions de ressources), cochez tout ce qui s'applique.

Choisissez parmi **Connection limit reached** (Limite de connexion atteinte), **Memory threshold reached** (Seuil de mémoire atteint) et **Interface threshold reached** (Seuil d'interface atteint).

h) **NAT Traps** (Interruptions NAT).

Cochez cet élément pour recevoir des notifications lorsque des paquets IP sont rejetés par la NAT en raison de l'espace de mappage non disponible.

i) **Syslog** (Journal système).

Cochez **Enable syslog traps** (Activer les interruptions du journal système) pour recevoir des notifications lorsque le nombre de sessions établies dépasse le seuil défini.

Pour configurer le niveau de gravité de l'interruption **syslog** (journal système), sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

j) **CPU Utilization Traps** (Interruptions d'utilisation du CPU).

Cochez **CPU rising threshold reached** (Seuil d'augmentation du CPU atteint) pour recevoir des notifications lorsque l'utilisation du CPU est supérieure à la valeur **CPU Utilization threshold** (Seuil d'utilisation du CPU) configurée pour la valeur **Monitoring interval** (Intervalle de supervision) configurée.

k) **SNMP interface threshold** (Seuil d'interface SNMP).

Cochez **Configure threshold and interval** (Configurer le seuil et l'intervalle) pour recevoir des notifications lorsque l'utilisation de la bande passante de l'interface est supérieure à la valeur **SNMP interface threshold** (Seuil d'interface SNMP) configurée.

Les valeurs de seuil valides sont comprises entre 30 et 99 %. La valeur par défaut est 70 %.

l) **SNMP Memory threshold** (Seuil de mémoire SNMP).

Cochez **Configure memory threshold** (Configurer le seuil de mémoire) pour recevoir des notifications lorsque l'utilisation du CPU est supérieure à la valeur de seuil configurée pour la valeur **SNMP memory threshold** (Seuil de mémoire SNMP).

Lorsque la mémoire du contexte système utilisée atteint 80 % de la mémoire totale du système, l'interruption de seuil de mémoire est générée à partir du contexte d'administration. Pour tous les autres contextes d'utilisateur, cette interruption est générée lorsque la mémoire utilisée atteint 80 % de la mémoire totale du système dans ce contexte en particulier.

m) **Failover Traps** (Interruptions de basculement).

Cochez **Enable Failover related traps** (Activer les interruptions liées au basculement) pour recevoir les alertes SNMP du journal système pour le basculement.

n) **Cluster Traps** (Interruptions de grappe).

Cochez **Enable cluster related traps** (Activer les interruptions liées à la grappe) pour recevoir les alertes SNMP du journal système pour les membres de la grappe.

o) **Peer-Flap Traps** (Interruptions d'intermittence d'homologues).

Cochez **Enable bgp/ospf peer-flap related traps** (Activer les interruptions d'intermittence d'homologues BGP/OSPF) pour recevoir les alertes SNMP du journal système pour le basculement involontaire des adresses MAC des homologues de grappe.

**Étape 4** Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du déroutement SNMP**.

**Étape 5** Cliquez sur **Apply** (Appliquer).

Les alertes SNMP sont configurées et les modifications sont enregistrées dans la configuration en cours d'exécution.

# Configurer les paramètres pour la version 1 ou 2c du SNMP

Pour configurer les paramètres pour la version 1 ou 2c du SNMP, procédez comme suit :

**Procédure**

**Étape 1** Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** .

**Étape 2** Saisissez un identifiant de communauté par défaut dans le champ **Community String** (Identifiant de communauté) (par défaut) si vous utilisez la version 1 ou 2c du SNMP. Saisissez le mot de passe utilisé par les NMS SNMP lorsqu'ils envoient des requêtes à l'ASA. L'identifiant de communauté SNMP est un secret partagé entre les NMS SNMP et les nœuds de réseau gérés. L'ASA utilise le mot de passe pour déterminer si la requête SNMP entrante est valide. Cependant, si la supervision SNMP se fait par l'interface de gestion plutôt que par l'interface de diagnostic, l'interrogation a lieu sans que l'ASA ne valide l'identifiant de communauté. Le mot de passe est une valeur sensible à la casse pouvant comporter jusqu'à 32 caractères alphanumériques. Les espaces ne sont pas permises. La valeur par défaut est public. La version 2c du SNMP permet de définir des identifiants de communauté distincts pour chaque NMS. Si aucun identifiant de communauté n'est configuré pour un NMS, la valeur définie ici est utilisée par défaut.



**Remarque** Vous devez éviter l'utilisation de caractères spéciaux (!, @, #, $, %, ^, &, *, \) dans les identifiants de communauté. En général, l'utilisation de caractères spéciaux réservés aux fonctions utilisées par le système d'exploitation peut entraîner des résultats inattendus. Par exemple, la barre oblique inverse (\) est interprétée comme un caractère d'échappement et ne doit pas être utilisée dans l'identifiant de communauté.

**Étape 3** Saisissez le nom de l'administrateur système de l'ASA. Le texte est sensible à la casse et peut comporter jusqu'à 127 caractères alphabétiques. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

**Étape 4** Saisissez l'emplacement de l'ASA géré par SNMP. Le texte est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

**Étape 5** Saisissez le numéro de port de l'ASA qui écoute les requêtes SNMP à partir des NMS; ou conservez la valeur par défaut, le numéro de port 161.

**Étape 6** (Facultatif) Cochez la case **Enable Global-Shared pool in the walk** (Activer le groupe partagé global dans la marche) pour interroger la mémoire libre et les statistiques de mémoire utilisées au moyen des opérations de marche SNMP.



**Important** Lorsque l'ASA interroge les renseignements sur la mémoire, le CPU peut être occupé par le processus SNMP pendant trop longtemps avant d'être libéré pour d'autres processus. Cela peut entraîner des saturations du CPU liées à SNMP qui peuvent entraîner des abandons de paquet.

**Étape 7** Cliquez sur **Add** (Ajouter) dans le volet **SNMP Host Access List** (Liste d'accès de l'hôte SNMP).

La boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP) s'affiche.

**Étape 8** Choisissez le nom de l'interface à partir de laquelle les interruptions sont envoyées dans la liste déroulante.

**Étape 9** Saisissez l'adresse IP du gestionnaire NMS ou SNMP qui peut se connecter à l'ASA.

**Étape 10** Saisissez le numéro de port UDP. La valeur par défaut est 162.

**Étape 11** Choisissez la version SNMP que vous utilisez dans la liste déroulante. Si vous choisissez la version 1 ou la version 2c, vous devez saisir l'identifiant de communauté. Si vous choisissez la version 3, vous devez choisir le nom d'utilisateur dans la liste déroulante.

La version spécifie la version du SNMP à utiliser pour les interruptions et les requêtes (interrogation). La communication avec le serveur est autorisée uniquement en utilisant la version sélectionnée.

**Étape 12** Cochez la case **Poll** (Interrogation) dans la zone **Server Poll/Trap Specification** (Spécification de l'interrogation et de l'interruption du serveur) pour limiter le NMS à l'envoi de requêtes (interrogation). Cochez la case **Trap** (Interruption) pour limiter le NMS à la réception d'interruptions uniquement. Vous pouvez cocher les deux cases pour effectuer les deux fonctions de l'hôte SNMP.

**Étape 13** Cliquez sur **OK** pour fermer la boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP).

Le nouvel hôte apparaît dans le volet **SNMP Host Access List** (Liste d'accès à l'hôte SNMP).

**Étape 14** Cliquez sur **Apply**.

Les paramètres SNMP pour les versions 1, 2c ou 3 sont configurés et les modifications sont enregistrées dans la configuration en cours d'exécution.

# Configurer les paramètres pour la version 3 du SNMP

Pour configurer les paramètres pour la version 3 du SNMP, procédez comme suit :

### Procédure

**Étape 1** Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**.

**Étape 2** Cliquez sur **Add (Ajouter)** > **SNMP User (Utilisateur SNMP)** sous l'onglet **SNMPv3 User/Group** (Utilisateur/Groupe SNMPv3) dans le volet **SNMPv3 Users** (Utilisateurs SNMPv3) pour ajouter un utilisateur configuré ou un nouvel utilisateur à un groupe. Lorsque vous supprimez le dernier utilisateur d'un groupe, ASDM supprime le groupe.



**Remarque** Après la création d'un utilisateur, vous ne pouvez pas modifier le groupe auquel appartient l'utilisateur.

La boîte de dialogue **Add SNMP User Entry** (Ajouter une entrée d'utilisateur SNMP) s'affiche.

**Étape 3** Choisissez le groupe auquel appartient l'utilisateur SNMP. Les groupes disponibles sont les suivants :

- **Auth&Encryption**, dans lequel les utilisateurs ont l'authentification et le chiffrement configurés
- **Authentication_Only**, dans lequel les utilisateurs n'ont que l'authentification configurée
- **No_Authentication**, dans lequel les utilisateurs n'ont ni l'authentification ni le chiffrement configurés



**Remarque** Vous ne pouvez pas modifier les noms de groupe.

**Étape 4** Cliquez sur l'onglet **USM Model** (Modèle USM) pour utiliser les groupes de modèles de sécurité utilisateur (USM).

**Étape 5** Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add SNMP USM Entry** (Ajouter une entrée USM SNMP) s'affiche.

**Étape 6** Saisissez le nom du groupe.

**Étape 7** Choisissez le niveau de sécurité dans la liste déroulante. Ce paramètre vous permet d'attribuer un groupe USM configuré comme niveau de sécurité aux utilisateurs SNMPv3.

**Étape 8** Saisissez le nom d'un utilisateur configuré ou d'un nouvel utilisateur. Le nom d'utilisateur doit être unique pour le groupe de serveurs SNMP sélectionné.

**Étape 9** Indiquez le type de mot de passe que vous souhaitez utiliser en cliquant sur l'un des deux boutons radio : **Encrypted** (Chiffré) ou **Clear Text** (Texte clair).

**Étape 10** Indiquez le type d'authentification que vous souhaitez utiliser en cliquant sur l'un des quatre boutons radio : **SHA**, **SHA224**, **SHA256** ou **SHA384**.

**Étape 11** Saisissez le mot de passe à utiliser pour l'authentification.

**Étape 12** Indiquez le type de chiffrement que vous souhaitez utiliser en cliquant sur l'un de ces deux boutons radio : **3DES** ou **AES**.

**Étape 13** Si vous avez choisi le chiffrement AES, choisissez le niveau de chiffrement AES à utiliser : **128**, **192** ou **256**.

**Étape 14** Saisissez le mot de passe à utiliser pour le chiffrement. Le nombre maximal de caractères alphanumériques autorisé pour ce mot de passe est de 64.

**Étape 15** Cliquez sur **OK** pour créer un groupe (s'il s'agit du premier utilisateur de ce groupe), affichez ce groupe dans la liste déroulante **Group Name** (Nom du groupe) et créez un utilisateur pour ce groupe.

La boîte de dialogue **Add SNMP User Entry** (Ajouter une entrée d'utilisateur SNMP) se ferme.

**Étape 16** Cliquez sur **Apply** (Appliquer).

Les paramètres SNMP pour la version 3 sont configurés et les modifications sont enregistrées dans la configuration en cours d'exécution.

# Configurer un groupe d'utilisateurs

Pour configurer une liste d'utilisateurs SNMP avec un groupe d'utilisateurs spécifiés, procédez comme suit :

### Procédure

**Étape 1** Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** .

**Étape 2** Cliquez sur **Add (Ajouter)** > **SNMP User Group (Groupe d'utilisateurs SNMP)** sous l'onglet **SNMPv3 User/Group** (Utilisateur/Groupe SNMPv3) dans le volet **SNMPv3 Users** (Utilisateurs SNMPv3) pour ajouter un groupe d'utilisateurs configuré ou un nouveau groupe d'utilisateurs. Lorsque vous supprimez le dernier utilisateur d'un groupe, ASDM supprime le groupe.

La boîte de dialogue **Add SNMP User Group** (Ajouter un groupe d'utilisateurs SNMP) apparaît.

**Étape 3** Saisissez le nom du groupe d'utilisateurs.

**Étape 4** Cliquez sur le bouton radio **Existing User/User Group** (Utilisateur/Groupe d'utilisateurs existant) pour sélectionner un utilisateur ou un groupe d'utilisateurs existant.

**Étape 5** Cliquez sur le bouton radio **Create new user** (Créer un nouvel utilisateur) pour créer un nouvel utilisateur.

**Étape 6** Choisissez le groupe auquel appartient l'utilisateur SNMP. Les groupes disponibles sont les suivants :

- **Auth&Encryption**, dans lequel les utilisateurs ont l'authentification et le chiffrement configurés
- **Authentication_Only**, dans lequel les utilisateurs n'ont que l'authentification configurée
- **No_Authentication**, dans lequel les utilisateurs n'ont ni l'authentification ni le chiffrement configurés

**Étape 7** Saisissez le nom d'un utilisateur configuré ou d'un nouvel utilisateur. Le nom d'utilisateur doit être unique pour le groupe de serveurs SNMP sélectionné.

**Étape 8** Indiquez le type de mot de passe que vous souhaitez utiliser en cliquant sur l'un des deux boutons radio : **Encrypted** (Chiffré) ou **Clear Text** (Texte clair).

**Étape 9** Indiquez le type d'authentification que vous souhaitez utiliser en cliquant sur l'un des quatre boutons radio : **SHA**, **SHA224**, **SHA256** ou **SHA384**.

**Étape 10** Saisissez le mot de passe à utiliser pour l'authentification.

**Étape 11** Confirmez le mot de passe à utiliser pour l'authentification.

**Étape 12** Indiquez le type de chiffrement que vous souhaitez utiliser en cliquant sur l'un de ces deux boutons radio : **3DES** ou **AES**.

**Étape 13** Saisissez le mot de passe à utiliser pour le chiffrement. Le nombre maximal de caractères alphanumériques autorisé pour ce mot de passe est de 64.

**Étape 14** Confirmez le mot de passe à utiliser pour le chiffrement.

**Étape 15** Cliquez sur **Add** (Ajouter) pour ajouter le nouvel utilisateur au groupe d'utilisateurs spécifié dans le volet **Members in Group** (Membres du groupe). Cliquez sur **Remove** (Supprimer) pour supprimer un utilisateur existant du volet **Members in Group** (Membres du groupe).

**Étape 16** Cliquez sur **OK** pour créer un nouvel utilisateur pour le groupe d'utilisateurs spécifié.

La boîte de dialogue **Add SNMP User Group** (Ajouter un groupe d'utilisateurs SNMP) se ferme.

**Étape 17** Cliquez sur **Apply** (Appliquer).

Les paramètres SNMP pour la version 3 sont configurés et les modifications sont enregistrées dans la configuration en cours d'exécution.

# Supervision SNMP

Consultez les commandes suivantes pour superviser SNMP. Vous pouvez saisir ces commandes en sélectionnant **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

- **show running-config snmp-server** [**default**]

  Cette commande affiche tous les renseignements de configuration du serveur SNMP.

- **show running-config snmp-server group**

  Cette commande affiche les paramètres de configuration du groupe SNMP.

- **show running-config snmp-server host**

  Cette commande affiche les paramètres de configuration utilisés par SNMP pour contrôler les messages et les notifications envoyés aux hôtes distants.

- **show running-config snmp-server host-group**

  Cette commande affiche les configurations du groupe d'hôtes SNMP.

- **show running-config snmp-server user**

  Cette commande affiche les paramètres de configuration SNMP basés sur l'utilisateur.

- **show running-config snmp-server user-list**

  Cette commande affiche les configurations de la liste d'utilisateurs SNMP.

- **show snmp-server engineid**

  Cette commande affiche l'ID du moteur SNMP configuré.

- **show snmp-server group**

  Cette commande affiche les noms des groupes SNMP configurés. Si l'identifiant de communauté a déjà été configuré, deux groupes supplémentaires s'affichent par défaut dans la sortie. Ce comportement est normal.

- **show snmp-server statistics**

Cette commande affiche les caractéristiques configurées du serveur SNMP. Pour réinitialiser tous les compteurs SNMP à zéro, utilisez la commande **clear snmp-server statistics**.

- **show snmp-server user**

  Cette commande affiche les caractéristiques configurées des utilisateurs.

# Historique de SNMP

***Tableau 2 : Historique de SNMP***

| Nom de la caractéristique | Version | Description |
|---|---|---|
| SNMP versions 1 et 2c | 7.0(1) | Fournit des renseignements sur la supervision du réseau ASA et les événements en transmettant les données entre le serveur SNMP et l'agent SNMP par l'identifiant de communauté en texte clair.<br><br>Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP. |
| SNMP version 3 | 8.2(1) | Fournit un chiffrement et une prise en charge 3DES ou AES pour SNMP version 3, la forme la plus sécurisée des modèles de sécurité pris en charge. Cette version vous permet de configurer les utilisateurs, les groupes et les hôtes, ainsi que les caractéristiques d'authentification à l'aide d'USM. En outre, cette version permet le contrôle d'accès à l'agent et aux objets MIB et comprend une prise en charge MIB supplémentaire.<br><br>Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP. |
| Chiffrement de mot de passe | 8.3(1) | Prend en charge le chiffrement de mot de passe. |
| Alertes SNMP et MIB | v 8.4(1) | Prend en charge les mots clés supplémentaires suivants : **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop \| start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**.<br><br>Le tableau entPhysicalTable signale les entrées pour les capteurs, les ventilateurs, les alimentations et les composants connexes.<br><br>Prend en charge les MIB supplémentaires suivantes : CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB.<br><br>Prend en charge les interruptions supplémentaires suivantes : ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart.<br><br>Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP. |

| Nom de la caractéristique | Version | Description |
|---|---|---|
| Prise en charge de l'OID IF-MIB ifAlias | 8.2(5)/8.4(2) | L'ASA prend désormais en charge l'OID ifAlias. Lorsque vous parcourez l'IF-MIB, l'OID ifAlias sera défini à la valeur qui a été définie pour la description de l'interface. |
| Module de services ASA (ASASM) | 8.5(1) | L'ASASM prend en charge toutes les MIB et interruptions présentes dans 8.4(1), à l'exception des éléments suivants :<br>MIB non prises en charge dans 8.5(1) :<br>• CISCO-ENTITY-SENSOR-EXT-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge).<br>• ENTITY-SENSOR-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge).<br>• DISMAN-EXRPSION-MIB (seuls les objets des groupes expExpressionTable, expObjectTable et expValueTable sont pris en charge).<br>Interruptions non prises en charge dans 8.5(1) :<br>• ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB). Cette interruption est utilisée uniquement pour les défaillances d'alimentation, les défaillances de ventilateur et les événements de température élevée du processeur.<br>• InterfacesBandwidthUtilization. |
| Interruptions SNMP | 8.6(1) | Prend en charge les mots clés supplémentaires suivants pour les modèles ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X : **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**.<br>Nous avons modifié la commande suivante : **snmp-server enable traps**. |
| MIB liées au VPN | 9.0(1) | Une version mise à jour de CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB a été implementée pour prendre en charge la fonctionnalité de chiffrement de nouvelle génération.<br>Les MIB suivantes ont été activées pour l'ASASM :<br>• ALTIGA-GLOBAL-REG.my<br>• ALTIGA-LBSSF-STATS-MIB.my<br>• ALTIGA-MIB.my<br>• ALTIGA-SSL-STATS-MIB.my<br>• CISCO-IPSEC-FLOW-MONITOR-MIB.my<br>• CISCO-REMOTE-ACCESS-MONITOR-MIB.my |
| MIB TrustSec de Cisco | 9.0(1) | La prise en charge de la MIB suivante a été ajoutée : CISCO-TRUSTSEC-SXP-MIB. |

| Nom de la caractéristique | Version | Description |
|---|---|---|
| OID SNMP | 9.1(1) | Cinq nouveaux OID de type prestataire physique SNMP ont été ajoutés pour prendre en charge les appareils ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X. |
| MIB NAT | 9.1(2) | Ajout des OID cnatAddrBindNumberOfEntries et cnatAddrBindSessionCount pour prendre en charge les entrées xlate_count et max_xlate_count, qui sont équivalents à l'autorisation de l'interrogation à l'aide de la commande **show xlate count**. |
| Hôtes SNMP, groupes d'hôtes et listes d'utilisateurs | 9.1(5) | Vous pouvez maintenant ajouter jusqu'à 4 000 hôtes. Le nombre de destinations d'interrogation actives prises en charge est de 128. Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes. Vous pouvez associer plusieurs utilisateurs à un hôte.<br>Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP. |
| Taille des messages SNMP | 9.2(1) | La limite de taille des messages que SNMP envoie a été augmentée à 1 472 octets. |
| OID et MIB SNMP | 9.2(1) | L'ASA prend désormais en charge l'OID cpmCPUTotal5minRev.<br>L'ASA virtuel a été ajouté en tant que nouveau produit aux OID sysObjectID et entPhysicalVendorType de SNMP.<br>Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge la nouvelle plateforme ASA virtuel.<br>Une nouvelle MIB SNMP pour superviser l'utilisation des licences partagées des VPN a été ajoutée. |
| OID et MIB SNMP | 9.3(1) | La prise en charge de CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) a été ajoutée pour l'ASASM. |

| Nom de la caractéristique | Version | Description |
|---|---|---|
| MIB et alertes SNMP | 9.3(2) | Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge l'ASA 5506-X.<br><br>L'ASA 5506-X a été ajouté en tant que nouveau produit aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP.<br><br>L'ASA prend désormais en charge CISCO-CONFIG-MAN-MIB, qui vous permet de faire les opérations suivantes :<br>• Savoir quelles commandes ont été saisies pour une configuration en particulier.<br>• Avertir le NMS lorsqu'une modification s'est produite dans la configuration d'exécution.<br>• Suivez les horodatages associés à la dernière fois que la configuration d'exécution a été modifiée ou enregistrée.<br>• Suivez les autres modifications apportées aux commandes, comme les détails du terminal et les sources de commandes.<br><br>Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP > Configure Traps (Configurer les interruptions) > SNMP Trap Configuration (Configuration des alertes SNMP). |
| MIB et alertes SNMP | 9.4(1) | Les ASA 5506W-X, ASA 5506H-X, ASA 5508-X et ASA 5516-X ont été ajoutés en tant que nouveaux produits aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP. |
| Hôtes d'interruption de serveur SNMP illimités par contexte | 9.4(1) | L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique.<br><br>Nous n'avons pas modifié d'écrans ASDM. |
| Ajout de la prise en charge pour ISA 3000 | 9.4(1.225) | La gamme de produits ISA 3000 est désormais prise en charge pour SNMP. Nous avons ajouté de nouveaux OID pour cette plateforme. La commande **snmp-server enable traps entity** a été modifiée pour inclure une nouvelle variable *l1-bypass-status*. Cela active le changement d'état du contournement matériel.<br><br>Nous n'avons pas modifié d'écrans ASDM. |
| Prise en charge de cempMemPoolTable dans CISCO-ENHANCED-MEMPOOL-MIB | 9.6(1) | Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB est maintenant pris en charge. Il s'agit d'un tableau des entrées de surveillance de la réserve de mémoire pour toutes les entités physiques d'un système géré.<br><br>**Remarque**<br>CISCO-ENHANCED-MEMPOOL-MIB utilise des compteurs de 64 bits et prend en charge les rapports de mémoire sur les plateformes avec plus de 4 Go de RAM. |

| Nom de la caractéristique | Version | Description |
|---|---|---|
| Prise en charge des MIB en mode d'horloge E2E transparent pour le protocole PTP (Precision Time Protocol) | 9.7(1) | Les MIB correspondant au mode d'horloge E2E transparent sont maintenant prises en charge.<br>**Remarque**<br>Seules les opérations SNMP get, bulkget, getnext et walk sont prises en charge. |
| SNMP sur IPv6 | 9.9(2) | L'ASA prend désormais en charge SNMP sur IPv6, y compris la communication avec des serveurs SNMP sur IPv6, permettant l'exécution de requêtes et d'interruptions sur IPv6 et prenant en charge les adresses IPv6 pour les MIB existantes. Nous avons ajouté les nouveaux objets MIB IPv6 SNMP suivants, comme décrit dans la RFC 8096.<br>• ipv6InterfaceTable (OID : 1.3.6.1.2.1.4.30) : contient des renseignements spécifiques à IPv6 par interface.<br>• ipAddressPrefixTable (OID :1.3.6.1.2.1.4.32) : comprend tous les préfixes appris par cette entité.<br>• ipAddressTable (OID : 1.3.6.1.2.1.4.34) : contient des renseignements d'adressage pertinents pour les interfaces de l'entité.<br>• ipNetToPhysicalTable (OID : 1.3.6.1.2.1.4.35) : contient le mappage des adresses IP aux adresses physiques.<br>Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** |
| Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP | 9.10(1) | Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP.<br>Nous n'avons pas modifié d'écrans ASDM. |
| Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP | 9.12(1) | Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP.<br>Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** |
| Authentification SNMPv3 | 9.14(1) | Vous pouvez maintenant utiliser le code HMAC SHA-256 pour l'authentification de l'utilisateur.<br>Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** |
| Pour les paires de basculements en version 9.14(1) ou toute version ultérieure, l'ASA ne partage plus les données du moteur client SNMP avec son homologue. | 9.14(1) | L'ASA ne partage plus les données du moteur client SNMP avec son homologue. |

| Nom de la caractéristique | Version | Description |
|---|---|---|
| Interrogation SNMP sur le VPN de site à site | 9.14(2) | Pour une interrogation SNMP sécurisée sur un VPN de site à site, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN. |
| La prise en charge des OID CISCO-MEMORY-POOL-MIB est rendue obsolète | 9.15(1) | Les OID CISCO-MEMORY-POOL-MIB (ciscoMemoryPoolUsed, ciscoMemoryPoolFree) sont obsolètes pour les systèmes qui utilisent des compteurs de 64 bits.<br>Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB fournit des entrées de supervision de la réserve de mémoire pour les systèmes qui utilisent des compteurs de 64 bits. |
| Authentification SNMPv3 | 9.16(1) | Vous pouvez maintenant utiliser SHA-224 et SHA-384 pour l'authentification de l'utilisateur. Vous ne pouvez plus utiliser MD5 pour l'authentification de l'utilisateur.<br>Vous ne pouvez plus utiliser DES pour le chiffrement.<br>Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** |
| Prise en charge de l'interface de boucle avec retour pour SNMP | 9.18(2) | Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour SNMP.<br>Commandes nouvelles/modifiées : **interface loopback**, **snmp-server host**<br>Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**.<br>La prise en charge d'ASDM a été ajoutée dans la version 7.19. |

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.