FAQ ESA : AsyncOS prend-il en charge la surveillance SNMP ?

Contenu

Introduction

Ce document décrit quels déroutements SNMP (Simple Network Management Protocol) sont pris en charge par AsyncOS.

AsyncOS prend-il en charge la surveillance SNMP ?

Le système d'exploitation Cisco AsyncOS prend en charge la surveillance de l'état du système via SNMP. AsyncOS prend en charge SNMPv1, v2 et v3.

Cela inclut la base MIB (Enterprise Management Information Base) de Cisco, ASYNCOS-MAIL-MIB. ASYNCOS-MAIL-MIB aide les administrateurs à mieux contrôler l'état du système. En outre, cette version implémente un sous-ensemble en lecture seule de MIB-II tel que défini dans les RFC 1213 et 1907. (Pour plus d'informations sur SNMP, consultez RFC 1065, 1066 et 1067.)

Remarque :

- SNMP est désactivé par défaut.
- Les opérations SET SNMP (configuration) ne sont pas implémentées.
- L'utilisation de SNMPv3 avec authentification par mot de passe et chiffrement DES est obligatoire afin d'activer ce service. (Pour plus d'informations sur SNMPv3, voir RFC 2571-2575.) Vous devez définir une phrase de passe SNMPv3 d'au moins huit caractères afin d'activer la surveillance de l'état du système SNMP. La première fois que vous saisissez une phrase de passe SNMPv3, vous devez la saisir à nouveau pour confirmer. La commande **snmpconfig** *se souvient* de cette phrase la prochaine fois que vous exécutez la commande.
- Le nom d'utilisateur SNMPv3 est : v3get.
  ```
  > snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
  ```
- Si vous utilisez uniquement SNMPv1 ou SNMPv2, vous devez définir une chaîne de communauté. La chaîne de communauté n'est pas publique par défaut.
- Pour SNMPv1 et SNMPv2, vous devez spécifier un réseau à partir duquel les requêtes SNMP GET sont acceptées.
- Afin d'utiliser des interruptions, un gestionnaire SNMP (non inclus dans AsyncOS) doit être en

cours d'exécution et son adresse IP doit être entrée comme cible de déroutement. (Vous pouvez utiliser un nom d'hôte, mais si vous le faites, les interruptions ne fonctionneront que si le DNS fonctionne.)

Utilisez la commande **snmpconfig** afin de configurer l'état du système SNMP pour l'appliance. Après avoir choisi et configuré des valeurs pour une interface, l'appliance répond aux requêtes GET SNMPv3. Ces demandes de version 3 doivent inclure un mot de passe correspondant. Par défaut, les demandes des versions 1 et 2 sont rejetées. Si cette option est activée, les demandes de version 1 et 2 doivent avoir une chaîne de communauté correspondante.

Cisco Systems fournit une base MIB *d'entreprise* ainsi qu'un fichier SMI (Structure of Management Information) :

- ASYNCOS-MAIL-MIB.txt : description compatible SNMPv2 de la base MIB d'entreprise pour les appliances Cisco.
- IRONPORT-SMI.txt : définit le rôle de la base de données MIB ASYNCOS-MAIL dans les produits gérés SNMP d'IronPort.

Les deux fichiers MIB se trouvent à partir de la page d'assistance du dispositif de sécurité de la messagerie Cisco.

> **Conseil** : Certains clients peuvent avoir besoin de compiler les deux fichiers dans un seul fichier « .my », par exemple pour prendre en charge HP OpenView. Un outil permettant d'y parvenir est disponible à l'adresse www.mg-soft.com.

Reportez-vous au chapitre **Gestion et surveillance via l'interface de ligne de commande** du **Guide d'utilisation des e-mails** pour plus de détails sur la surveillance SNMP.

Informations connexes

- Guides de l'utilisateur final du dispositif de sécurité de la messagerie Cisco
- Support et documentation techniques - Cisco Systems