

Exemple de configuration des requêtes ESA, SMA et WSA avec la commande snmpwalk

Contenu

[Introduction](#)

[Conditions préalables](#)

[Configuration](#)

[Configuration ESA](#)

[Configuration SMA](#)

[Configuration du WSA](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment utiliser le `snmpwalk` afin d'interroger ou d'interroger le dispositif de sécurité de la messagerie Cisco (ESA), le dispositif de gestion de la sécurité du contenu Cisco (SMA) ou le dispositif de sécurité Web Cisco (WSA).

Conditions préalables

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ESA avec AsyncOS 5.x ou version ultérieure
- SMA avec AsyncOS 5.x ou version ultérieure
- WSA avec AsyncOS 5.x ou version ultérieure
- Une machine hôte Linux ou Unix séparée avec le paquet `net-snmp` de distribution installé est requise

Note: Ce document fait référence à des logiciels qui ne sont pas gérés ou pris en charge par Cisco. Les informations sont fournies comme courtoisie pour votre commodité. Pour obtenir de l'aide, contactez le fournisseur du logiciel.

Configuration

Cette section couvre les configurations pour les ESA, SMA et WSA.

Configuration ESA

1. Saisissez le `snmpconfig` CLI afin de s'assurer que le protocole SNMP (Simple Network Management Protocol) est activé.

2. Téléchargez tous les fichiers MIB AsyncOS associés à partir de l'[appliance de sécurité de la messagerie Cisco](#) sous Outils associés :

MIB SMI AsyncOS pour ESA (txt) MIB de messagerie AsyncOS pour ESA (txt)

3. Placez ces fichiers dans le répertoire SNMP de votre machine locale, qui ressemble généralement à `/usr/net-snmp/share/mibs/`.

4. Utilisez votre hôte SNMP pour exécuter `snmpwalk` commande :

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com iso.3.6.1.2.1.1
```

Dans la commande précédente, spécifiez :

- Tous les champs de sortie avec `'-O a'`.
- Protocole SNMP version 2c avec `'-v 2c'`.
- Une chaîne de communauté publique ou en lecture seule (doit correspondre à celle de votre appliance) `snmpconfig`) ou `'cisco'` avec `'-c cisco'`.
- Chemin absolu ou emplacement facultatif de vos fichiers MIB avec `'-M /the/path/to/snmp/mibs/'`.
- Quels fichiers MIB charger (ALL charge tout) avec `'-m « ALL »'`.
- Adresse hôte cible de votre appliance à interroger avec `'hostname'` ou `'x.x.x.x'`.
- Point de départ de l'arborescence OID de l'appliance pour commencer la marche à pied par `'iso.3.6.1.2.1.1'`.

La commande exemple ci-dessus renvoie une liste de toutes les informations de diagnostic extraites de votre appareil :

```
~$ snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL" host.example.com iso.3.6.1.2.1.1 iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702, Build Date: 2009-11-10, Serial #: 00C09F3AED0E-#####" iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

Exemple SNMPv3

```
snmpwalk -v3 -l authPriv -u v3get -a SHA -A "cisco" -x AES -X "cisco" x.x.x.x iso.3.6.1.2.1.1
```

Dans la commande précédente, spécifiez :

- Protocole SNMP version 3 avec `'-v 3'`.
- Le `-l` configure les fonctions d'authentification et de chiffrement à utiliser.
- L'option `-u` définit le nom d'utilisateur SNMP sur le sous-système User Security Module. Il s'agit d'une chaîne de 1 à 32 octets de longueur. Doit être configuré de la même manière sur les deux entités SNMP essayant de communiquer.

- L'option -a permet de définir l'authentification.
- L'option -A est la clé de chiffrement secrète.
- L'option -x permet de définir le type de chiffrement.
- L'option -X permet de définir la phrase de passe de confidentialité SNMPv3.
- Adresse hôte cible de votre appliance à interroger avec 'hostname' ou 'x.x.x.x'.
- Point de départ de l'arborescence OID de l'appliance pour commencer la marche à pied par 'iso.3.6.1.2.1.1'.

Reportez-vous également aux [didacticiels Net-SNMP](#) ou utilisez `snmpwalk --help` pour plus d'informations sur `snmpwalk` et d'autres utilitaires SNMP.

Configuration SMA

1. Saisissez le `snmpconfig` CLI afin de s'assurer que SNMP est activé.
2. Téléchargez tous les fichiers MIB AsyncOS associés depuis l'[appliance de gestion de la sécurité du contenu Cisco](#) sous Outils associés :
MIB SMI AsyncOS pour SMA (txt)MIB de messagerie AsyncOS pour SMA (txt)
3. Placez ces fichiers dans le répertoire SNMP de votre machine locale, qui ressemble généralement à `/usr/net-snmp/share/mibs/`.
4. Utilisez votre hôte SNMP pour exécuter `snmpwalk` commande :

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com
iso.3.6.1.2.1.1
```

Dans la commande précédente, spécifiez :

- Tous les champs de sortie avec '-O a'.
- Protocole SNMP version 2c avec '-v 2c'.
- Une chaîne de communauté publique ou en lecture seule (doit correspondre à celle de votre appliance) `snmpconfig`) ou 'cisco' avec '-c cisco'.
- Chemin absolu ou emplacement facultatif de vos fichiers MIB avec '-M /the/path/to/snmp/mibs/'.
- Quels fichiers MIB charger (ALL charge tout) avec '-m « ALL »'.
- Adresse hôte cible de votre appliance à interroger avec 'hostname' ou 'x.x.x.x'.
- Point de départ de l'arborescence OID de l'appliance pour commencer la marche à pied par 'iso.3.6.1.2.1.1'.

La commande exemple ci-dessus renvoie une liste de toutes les informations de diagnostic

extraites de votre appareil :

```
~$ snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL"  
host.example.com iso.3.6.1.2.1.1  
iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702,  
Build Date: 2009-11-10, Serial #: 00C09F3AED0E-#####"  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

Exemple SNMPv3

```
snmpwalk -v3 -l authPriv -u v3get -a SHA -A "cisco" -x AES -X "cisco" x.x.x.x iso.3.6.1.2.1.1
```

Dans la commande précédente, spécifiez :

- Protocole SNMP version 3 avec '-v 3'.
- L'option -l configure les fonctions d'authentification et de chiffrement à utiliser.
- L'option -u définit le nom d'utilisateur SNMP sur le sous-système User Security Module. Il s'agit d'une chaîne de 1 à 32 octets de longueur. Doit être configuré de la même manière sur les deux entités SNMP essayant de communiquer.
- L'option -a permet de définir l'authentification.
- L'option -A est la clé de chiffrement secrète.
- L'option -x permet de définir le type de chiffrement.
- L'option -X permet de définir la phrase de passe de confidentialité SNMPv3.
- Adresse hôte cible de votre appliance à interroger avec 'hostname' ou 'x.x.x.x'.
- Point de départ de l'arborescence OID de l'appliance pour commencer la marche à pied par 'iso.3.6.1.2.1.1'.

Reportez-vous également aux [didacticiels Net-SNMP](#) ou utilisez `snmpwalk --help` pour plus d'informations sur `snmpwalk` et d'autres utilitaires SNMP.

Configuration du WSA

1. Saisissez le `snmpconfig` CLI afin de s'assurer que SNMP est activé.
2. Téléchargez tous les fichiers MIB AsyncOS associés depuis l'[appliance de sécurité Web Cisco](#) sous Outils associés :
MIB SMI AsyncOS pour WSA (txt)MIB de messagerie AsyncOS pour WSA (txt)MIB Web AsyncOS (txt)
3. Placez ces fichiers dans le répertoire SNMP de votre machine locale, qui ressemble généralement à `/usr/net-snmp/share/mibs/`.
4. Utilisez votre hôte SNMP pour exécuter `snmpwalk` commande :

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com
iso.3.6.1.2.1.1
```

Dans la commande précédente, spécifiez :

- Tous les champs de sortie avec '-O a'.
- Protocole SNMP version 2c avec '-v 2c'.
- Une chaîne de communauté publique ou en lecture seule (doit correspondre à celle de votre appliance) `snmpconfig`) ou 'cisco' avec '-c cisco'.
- Chemin absolu ou emplacement facultatif de vos fichiers MIB avec '-M /the/path/to/snmp/mibs/'.
- Quels fichiers MIB charger (ALL charge tout) avec '-m « ALL »'.
- Adresse hôte cible de votre appliance à interroger avec 'hostname' ou 'x.x.x.x'.
- Point de départ de l'arborescence OID de l'apppliance pour commencer la marche à pied par 'iso.3.6.1.2.1.1'.

La commande exemple ci-dessus renvoie une liste de toutes les informations de diagnostic extraites de votre appareil :

```
:~$ snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL"
host.example.com iso.3.6.1.2.1.1
iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702,
Build Date: 2009-11-10, Serial #: 00C09F3AED0E-#####"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

Reportez-vous également aux [didacticiels Net-SNMP](#) ou utilisez `snmpwalk --help` pour plus d'informations sur `snmpwalk` et d'autres utilitaires SNMP.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.