

snmpwalk コマンドを使用した ESA、SMA、および WSA クエリの設定例

内容

[概要](#)

[前提条件](#)

[設定](#)

[ESA の設定](#)

[SMA の設定](#)

[WSA の設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、snmpwalk コマンドを発行して、Cisco Eメールセキュリティアプライアンス(ESA)、Ciscoコンテンツセキュリティ管理アプライアンス(SMA)、またはCisco Webセキュリティアプライアンス(WSA)を照会またはポーリングします。

前提条件

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AsyncOS 5.x 以降が稼働している ESA
- AsyncOS 5.x 以降が稼働している SMA
- AsyncOS 5.x 以降が稼働している WSA
- net-snmp 配布パッケージがインストールされている別個の Linux または UNIX ホスト マシンが必要です。

注：このドキュメントでは、Cisco が管理およびサポートしていないソフトウェアを参照します。この情報は、利便性のために無償で提供されています。さらにサポートが必要な場合は、ソフトウェアベンダーに連絡してください。

設定

ここでは、ESA、SMA、および WSA の設定について説明します。

ESA の設定

1. Enter the snmpconfig CLIコマンドを使用して、簡易ネットワーク管理プロトコル(SNMP)が有効になっていることを確認します。
2. [Cisco Eメールセキュリティアプライアンスの \[Related Tools\] で、関連するすべての](#)

[AsyncOS MIB ファイルをダウンロードします。](#)

ESA 用 AsyncOS SMI MIB (txt) ESA 用 AsyncOS Mail MIB (txt)

3. これらのファイルをローカルマシンのSNMPディレクトリに配置します。通常は次のようになります `/usr/net-snmp/share/mibs/`。
4. SNMPホストを使用して、 `snmpwalk` コマンドにより、WLC CLI で明確に示されます。

```
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
```

上記のコマンドで、次のように指定します。

- すべての出力フィールドに「`-O a`」が付いています。
- SNMPプロトコルバージョン2cと'`-v 2c`'です。
- 読み取り専用またはパブリックコミュニティストリング(アプライアンスの `snmpconfig settings`)または「`-c cisco`」を指定します。
- 「`-M /the/path/to/snmp/mibs/`」を使用したMIBファイルの絶対パスまたは場所 (オプション)。
- どのMIBファイルをロードするか (ALLはすべてのファイルをロードする)、'`-m "ALL"`」を使用します。
- 「hostname」または「`x.x.x.x`」でポーリングするアプライアンス上のターゲットホストアドレス。
- アプライアンスのObject Identifier (OID ; オブジェクト識別子) ツリーの開始点で、「`iso.3.6.1.2.1.1`」でウォークを開始します。

上記のコマンド例は、次のようにアプライアンスから取り出されたすべての診断情報のリストを返します。

```
~$ 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
```

SNMPv3の例

```
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
```

上記のコマンドで、次のように指定します。

- SNMPプロトコルバージョン3('v 3')。
- `-l` オプションは、使用する認証および暗号化機能を設定します。
- `-u` オプションは、SNMPユーザ名をユーザセキュリティモジュールサブシステムに設定します。長さは1 ~ 32オクテットの文字列です。通信を試みる両方のSNMPエンティティで同じ

方法で設定する必要があります。

- -aオプションは、認証を設定することです。
- -Aは秘密暗号鍵です。
- -xオプションは、暗号化のタイプを設定します。
- -Xは、SNMPv3プライバシーパスフレーズを設定することです。
- 「hostname」または「x.x.x.x」でポーリングするアプライアンス上のターゲットホストアドレス。
- アプライアンスのObject Identifier (OID ; オブジェクト識別子) ツリーの開始点で、「iso.3.6.1.2.1.1」でウォークを開始します。

Net-SNMPチュートリアルを[参照するが](#)、`snmpwalk --help` 詳細については、`snmpwalk` コマンドと他のSNMP関連ユーティリティ。

SMA の設定

1. Enter the `snmpconfig` CLIコマンドを使用して、SNMPが有効になっていることを確認します。
2. Cisco コンテンツ セキュリティ管理アプライアンスの [Related Tools] で、関連するすべての AsyncOS MIB ファイルをダウンロードします。
SMA 用 AsyncOS SMI MIB (txt) SMA 用 AsyncOS Mail MIB (txt)
3. これらのファイルをローカルマシンのSNMPディレクトリに配置します。通常は次のようになります `/usr/net-snmp/share/mibs/`。
4. SNMPホストを使用して、`snmpwalk` コマンドにより、WLC CLI で明確に示されます。

```
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
```

上記のコマンドで、次のように指定します。

- すべての出力フィールドに「-O a」が付いています。
- SNMPプロトコルバージョン2cと'-v 2c'です。
- 読み取り専用またはパブリックコミュニティストリング(アプライアンスの `snmpconfig settings`)または「-c cisco」を指定します。
- 「-M /the/path/to/snmp/mibs/」を使用したMIBファイルの絶対パスまたは場所 (オプション) 。
- どのMIBファイルをロードするか (ALLはすべてのファイルをロードする)、'-m "ALL"'を使用します。
- 「hostname」または「x.x.x.x」でポーリングするアプライアンス上のターゲットホストアドレス。

- アプライアンスのObject Identifier (OID ; オブジェクト識別子) ツリーの開始点で、「 iso.3.6.1.2.1.1」でウォークを開始します。

上記のコマンド例は、次のようにアプライアンスから取り出されたすべての診断情報のリストを返します。

```

:~$ 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

```

SNMPv3の例

```
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
```

上記のコマンドで、次のように指定します。

- SNMPプロトコルバージョン3('v 3')。
- -l オプションは、使用する認証および暗号化機能を設定します。
- -u オプションは、SNMPユーザ名をユーザセキュリティモジュールサブシステムに設定します。長さは1 ~ 32オクテットの文字列です。通信を試みる両方のSNMPエンティティで同じ方法で設定する必要があります。
- -a オプションは、認証を設定することです。
- -A は秘密暗号鍵です。
- -x オプションは、暗号化のタイプを設定します。
- -X は、SNMPv3プライバシーパスフレーズを設定することです。
- 「hostname」または「x.x.x.x」でポーリングするアプライアンス上のターゲットホストアドレス。
- アプライアンスのObject Identifier (OID ; オブジェクト識別子) ツリーの開始点で、「 iso.3.6.1.2.1.1」でウォークを開始します。

Net-SNMPチュートリアルを[参照するが](#)、`snmpwalk --help` 詳細については、`snmpwalk` コマンドと他のSNMP関連ユーティリティ。

WSA の設定

1. Enter the `snmpconfig` CLIコマンドを使用して、SNMPが有効になっていることを確認します。
2. Cisco Web セキュリティ アプライアンスの [Related Tools] で、関連するすべての AsyncOS MIB ファイルをダウンロードします。
WSA 用 AsyncOS SMI MIB (txt) WSA 用 AsyncOS Mail MIB (txt) AsyncOS Web MIB (txt)

3. これらのファイルをローカルマシンのSNMPディレクトリに配置します。通常は次のようになります `/usr/net-snmp/share/mibs/`。

4. SNMPホストを使用して、 `snmpwalk` コマンドにより、WLC CLI で明確に示されます。

```
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
```

上記のコマンドで、次のように指定します。

- すべての出力フィールドに「`-O a`」が付いています。
- SNMPプロトコルバージョン`2c`と`'-v 2c'`です。
- 読み取り専用またはパブリックコミュニティストリング(アプライアンスの `snmpconfig settings`)または「`-c cisco`」を指定します。
- 「`-M /the/path/to/snmp/mibs/`」を使用したMIBファイルの絶対パスまたは場所 (オプション)。
- どのMIBファイルをロードするか (ALLはすべてのファイルをロードする)、`'-m "ALL"'`を使用します。
- 「hostname」または「`x.x.x.x`」でポーリングするアプライアンス上のターゲットホストアドレス。
- アプライアンスのObject Identifier (OID ; オブジェクト識別子) ツリーの開始点で、「`iso.3.6.1.2.1.1`」でウォークを開始します。

上記のコマンド例は、次のようにアプライアンスから取り出されたすべての診断情報のリストを返します。

```
~$ 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
```

Net-SNMPチュートリアルを[参照するか](#)、`snmpwalk --help` 詳細については、`snmpwalk` コマンドと他のSNMP関連ユーティリティ。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報ははありません。