ESA, SMA, and WSA Queries with the snmpwalk Command Configuration Example

Contents

Introduction

This document describes how to use the `snmpwalk` command in order to query or poll the Cisco Email Security Appliance (ESA), Cisco Content Security Management Appliance (SMA), or Cisco Web Security Appliance (WSA).

Prerequisites

The information in this document is based on these software and hardware versions:

- ESA with AsyncOS 5.x or later
- SMA with AsyncOS 5.x or later
- WSA with AsyncOS 5.x or later
- A separate Linux or Unix host machine with the distribution net-snmp package installed is required

> **Note**: This document references software that is not maintained or supported by Cisco. The information is provided as a courtesy for your convenience. For further assistance, contact the software vendor.

Configure

This section covers the configurations for the ESA, SMA, and WSA.

ESA Configuration

1. Enter the `snmpconfig` CLI command in order to ensure that Simple Network Management Protocol (SNMP) is enabled.

2. Download all related AsyncOS MIB files from the Cisco Email Security Appliance under

Related Tools:
AsyncOS SMI MIB for ESA (txt)AsyncOS Mail MIB for ESA (txt)

3. Place these files in your local machine SNMP directory, which usually resembles **/usr/net-snmp/share/mibs/.**

4. Use your SNMP host to run the snmpwalk command:

```
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
```

In the previous command, specify:

- All output fields with '-O a'.
- SNMP protocol version 2c with '-v 2c'.
- A read-only or public community string (must match your appliance's snmpconfig settings) or 'cisco' with '-c cisco'.
- The optional absolute path or location of your MIB files with '-M /the/path/to/snmp/mibs/'.
- Which MIB files to load (ALL loads everything) with '-m "ALL"'.
- The target host address on your appliance to poll with 'hostname' or 'x.x.x.x'.
- The starting point of the appliance's Object Identifier (OID) tree to begin the walk with 'iso.3.6.1.2.1.1'.

The sample command listed previously returns a list of all diagnostic information pulled from your appliance:

```
:~$ 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 Example

```
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
```

In the previous command, specify:

- SNMP protocol version 3 with '-v 3'.
- The -l option configures authentication and encryption features to be used.
- The -u option sets SNMP user name to the User Security Module subsystem. This is a string from 1 to 32 octets of length. Should be configured in the same way at both SNMP entities trying to communicate.
- The -a option is to set Authentication.

- The -A is the secret encryption key.

- The -x option is to set the type of Encryption.
- The -X is to set the SNMPv3 privacy passphrase.

- The target host address on your appliance to poll with 'hostname' or 'x.x.x.x'.

- The starting point of the appliance's Object Identifier (OID) tree to begin the walk with 'iso.3.6.1.2.1.1'.

Refer also to the Net-SNMP Tutorials or use **snmpwalk --help** for more details on the snmpwalk command and other SNMP-related utilities.

SMA Configuration

1. Enter the snmpconfig CLI command in order to ensure that SNMP is enabled.

2. Download all related AsyncOS MIB files from the Cisco Content Security Management Appliance under Related Tools:
   AsyncOS SMI MIB for SMA (txt)AsyncOS Mail MIB for SMA (txt)
3. Place these files in your local machine SNMP directory, which usually resembles /usr/net-snmp/share/mibs/.

4. Use your SNMP host to run the snmpwalk command:

   ```
   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
   ```

In the previous command, specify:

- All output fields with '-O a'.

- SNMP protocol version 2c with '-v 2c'.

- A read-only or public community string (must match your appliance's snmpconfig settings) or 'cisco' with '-c cisco'.

- The optional absolute path or location of your MIB files with '-M /the/path/to/snmp/mibs/'.

- Which MIB files to load (ALL loads everything) with '-m "ALL"'.

- The target host address on your appliance to poll with 'hostname' or 'x.x.x.x'.

- The starting point of the appliance's Object Identifier (OID) tree to begin the walk with 'iso.3.6.1.2.1.1'.

The sample command listed previously returns a list of all diagnostic information pulled from your appliance:

```
:~$ 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 Example

```
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
```

In the previous command, specify:

- SNMP protocol version 3 with '-v 3'.
- The - option configures authentication and encryption features to be used.
- The -u option sets SNMP user name to the User Security Module subsystem. This is a string from 1 to 32 octets of length. Should be configured in the same way at both SNMP entities trying to communicate.
- The -a option is to set Authentication.
- The -A is the secret encryption key.
- The -x option is to set the type of Encryption.
- The -X is to set the SNMPv3 privacy passphrase.
- The target host address on your appliance to poll with 'hostname' or 'x.x.x.x'.
- The starting point of the appliance's Object Identifier (OID) tree to begin the walk with 'iso.3.6.1.2.1.1'.

Refer also to the Net-SNMP Tutorials or use **snmpwalk --help** for more details on the snmpwalk command and other SNMP-related utilities.

WSA Configuration

1. Enter the snmpconfig CLI command in order to ensure that SNMP is enabled.
2. Download all related AsyncOS MIB files from the Cisco Web Security Appliance under Related Tools:
   AsyncOS SMI MIB for WSA (txt)AsyncOS Mail MIB for WSA (txt)AsyncOS Web MIB (txt)
3. Place these files in your local machine SNMP directory, which usually resembles **/usr/net-snmp/share/mibs/**.
4. Use your SNMP host to run the snmpwalk command:

   ```
   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
   ```

In the previous command, specify:

- All output fields with '-O a'.

- SNMP protocol version 2c with '-v 2c'.
- A read-only or public community string (must match your appliance's snmpconfig settings) or 'cisco' with '-c cisco'.
- The optional absolute path or location of your MIB files with '-M /the/path/to/snmp/mibs/'.
- Which MIB files to load (ALL loads everything) with '-m "ALL"'.
- The target host address on your appliance to poll with 'hostname' or 'x.x.x.x'.
- The starting point of the appliance's Object Identifier (OID) tree to begin the walk with 'iso.3.6.1.2.1.1'.

The sample command listed previously returns a list of all diagnostic information pulled from your appliance:

```
:~$ 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
```

Refer also to the Net-SNMP Tutorials or use **snmpwalk --help** for more details on the snmpwalk command and other SNMP-related utilities.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.