How do I monitor the health of the ESA?

TAC **Document ID: 118349**

Contributed by Nasir Shakour and Enrico Werner, Cisco TAC
Engineers.

Aug 26, 2014

Contents

Introduction
How do I monitor the health of the ESA?

Introduction

This document describes how you can monitor services on the Email Security Appliance (ESA).

How do I monitor the health of the ESA?

The ESA has several externally−accessible network services that can be used to monitor the health and status of the system.

1. The ESA will respond to ICMP ECHO REQUEST datagrams (commonly called "ping" messages). A simple "***ping***" test can determine basic IP reachability of the appliance and whether it has power and is operating normally at the lowest level of the operating system. All IP interfaces configured will respond to ICMP packets.
2. The ESA can be monitored using SNMP management stations and SNMP monitoring tools. The SNMP MIB supported is the IETF−standardized MIB−II. This can be used to see low−level IP−layer and transport−layer statistics, such as datagrams and octets in and out of the system. SNMP management must be enabled with the "***snmpconfig***" CLI command. Only one interface can be enabled at a time to receive SNMP queries (although the MIB−II database covers the entire system). Also, if you are using SNMP v1/v2c, you must specify the network that your SNMP queries will come from. The ESA can send a coldStart SNMP trap to a single management station, if configured using the "***snmpconfig***" CLI command. This can be used to detect system reboots as well as SNMP agent restarts. Cisco provides an "enterprise" MIB as well as a "Structure of Management Information" (SMI) file for the ESA.
3. If configured, the ESA will offer SMTP, FTP, SSH, HTTP, and HTTPS services on any interface. These services can be individually enabled or disabled. The ESA also supports unencrypted TELNET access, although this is strongly discouraged. Monitoring tools can connect to one or more of these services on one or more interfaces to verify that the services are running and returning the correct banner. Configuration of services other than SMTP is handled using "***interfaceconfig***" CLI command; configuration of SMTP services is handled with the "***listenerconfig***" CLI command.
4. In AsyncOS XML−based statistics and status information are available via the HTTP or HTTPS access methods. These XML statistics can be gathered by a monitoring application or a command−line tool such as ***"curl"***. For example, for an ESA with administrative password "cisco123," the following "***curl***" commands will retrieve a variety of information:

```
curl −k https://esa.example.com/xml/status −u admin:cisco123
```

- Equivalent to the ESA CLI command "status" for general system status

```
curl -k https://esa.example.com/xml/dnsstatus -u admin:cisco123
```

- Equivalent to the ESA CLI command "dnsstatus" for DNS status

```
curl -k https://esa.example.com/xml/topin -u admin:cisco123
```

- Equivalent to the ESA CLI command "topin" for top incoming domains

```
curl -k https://esa.example.com/xml/tophosts -u admin:cisco123
```

- Equivalent to the ESA CLI command "tophosts" for top outgoing messages

```
curl -k https://esa.example.com/xml/hoststatus -u admin:cisco123 -F hostname=example.com
```

- Equivalent to the ESA CLI command "hoststatus" for a particular host.

For more information about SNMP System Status, go to ESA GUI and choose ***Help and Support* > *Online Help***.

Updated: Aug 26, 2014 Document ID: 118349