

Wie kann ich den Zustand der ESA überwachen?

Inhalt

[Einführung](#)

[Wie kann ich den Zustand der ESA überwachen?](#)

Einführung

Dieses Dokument beschreibt, wie Sie Services auf der E-Mail Security Appliance (ESA) überwachen können.

Wie kann ich den Zustand der ESA überwachen?

Die ESA verfügt über mehrere extern zugängliche Netzwerkdienste, die zur Überwachung von Zustand und Status des Systems verwendet werden können.

1. Die ESA wird auf ICMP ECHO REQUEST-Datagramme (gemeinhin als "Ping"-Nachrichten bezeichnet) reagieren. Ein einfacher **Ping**-Test kann die grundlegende IP-Erreichbarkeit der Appliance sowie die Frage bestimmen, ob sie mit Strom versorgt wird und normal auf der niedrigsten Ebene des Betriebssystems arbeitet. Alle konfigurierten IP-Schnittstellen reagieren auf ICMP-Pakete.
2. Die ESA kann mithilfe von SNMP-Verwaltungsstationen und SNMP-Überwachungstools überwacht werden. Die unterstützte SNMP MIB ist die IETF-standardisierte MIB-II. Auf diese Weise können IP-Schicht- und Transportschichtstatistiken auf niedriger Ebene angezeigt werden, z. B. Datagramme und Oktette innerhalb und außerhalb des Systems. Die SNMP-Verwaltung muss mit dem CLI-Befehl "**snmpconfig**" aktiviert werden. Es kann jeweils nur eine Schnittstelle aktiviert werden, um SNMP-Abfragen zu empfangen (obwohl die MIB-II-Datenbank das gesamte System abdeckt). Wenn Sie SNMP v1/v2c verwenden, müssen Sie außerdem das Netzwerk angeben, von dem die SNMP-Abfragen stammen. Die ESA kann, sofern sie mit dem Befehl "**snmpconfig**" CLI konfiguriert wurde, ein ColdStart-SNMP-Trap an eine einzige Managementstation senden. Diese Funktion kann zum Erkennen von Systemneustarts sowie zum Neustarten von SNMP-Agenten verwendet werden. Cisco stellt eine "Enterprise" MIB sowie eine "Structure of Management Information" (SMI)-Datei für die ESA bereit.
3. Wenn konfiguriert, bietet die ESA auf jeder Schnittstelle SMTP-, FTP-, SSH-, HTTP- und HTTPS-Dienste an. Diese Services können einzeln aktiviert oder deaktiviert werden. Die ESA unterstützt auch den unverschlüsselten TELNET-Zugriff, jedoch wird dies nachdrücklich abgeraten. Überwachungstools können eine Verbindung zu einem oder mehreren dieser Dienste über eine oder mehrere Schnittstellen herstellen, um zu überprüfen, ob die Dienste

ausgeführt werden, und um das richtige Banner zurückzugeben. Die Konfiguration anderer Services als SMTP wird mit dem CLI-Befehl "**interfaceConfig**" durchgeführt. Die Konfiguration von SMTP-Diensten wird mit dem CLI-Befehl "**listenerconfig**" behandelt.

4. In AsyncOS stehen XML-basierte Statistiken und Statusinformationen über die HTTP- oder HTTPS-Zugriffsmethoden zur Verfügung. Diese XML-Statistiken können von einer Überwachungsanwendung oder einem Befehlszeilentool wie "**curl**" erfasst werden. Bei einer ESA mit dem Administratorkennwort "cisco123" rufen die folgenden "**curl**"-Befehle eine Reihe von Informationen ab:

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

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

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

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

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

Weitere Informationen zum SNMP-Systemstatus finden Sie unter ESA-GUI. Wählen Sie **Hilfe und Support > Online Help (Hilfe und Support)** aus.