Häufig gestellte Fragen zur ESA: Unterstützt AsyncOS die SNMP-Überwachung?

Inhalt

Einführung

In diesem Dokument wird beschrieben, welche SNMP-Traps (Simple Network Management Protocol) von AsyncOS unterstützt werden.

Unterstützt AsyncOS die SNMP-Überwachung?

Das Cisco AsyncOS-Betriebssystem unterstützt die Systemstatusüberwachung über SNMP. AsyncOS unterstützt SNMPv1, v2 und v3.

Dazu gehören die Cisco Enterprise Management Information Base (MIB), ASYNCOS-MAIL-MIB. Die ASYNCOS-MAIL-MIB unterstützt Administratoren bei der besseren Überwachung des Systemstatus. Darüber hinaus implementiert diese Version eine schreibgeschützte Teilmenge von MIB-II, wie in den RFCs 1213 und 1907 definiert. (Weitere Informationen zu SNMP finden Sie unter RFCs 1065, 1066 und 1067.)

Hinweis:

- SNMP ist standardmäßig deaktiviert.
- SNMP SET-Vorgänge (Konfiguration) sind nicht implementiert.
- Die Verwendung von SNMPv3 mit Kennwortauthentifizierung und DES-Verschlüsselung ist erforderlich, um diesen Dienst zu aktivieren. (Weitere Informationen zu SNMPv3 finden Sie unter RFCs 2571-2575.) Sie müssen eine SNMPv3-Passphrase von mindestens acht Zeichen festlegen, um die SNMP-Systemstatusüberwachung zu aktivieren. Bei der ersten Eingabe einer SNMPv3-Passphrase müssen Sie diese zur Bestätigung erneut eingeben. Der Befehl **snmpconfig** *speichert* diese Zeichenfolge bei der nächsten Ausführung des Befehls.
- Der SNMPv3-Benutzername lautet: v3get.
  ```
  > snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
  ```
- Wenn Sie nur SNMPv1 oder SNMPv2 verwenden, müssen Sie einen Community-String festlegen. Der Community-String ist nicht standardmäßig für public festgelegt.
- Für SNMPv1 und SNMPv2 müssen Sie ein Netzwerk angeben, von dem SNMP GET-Anforderungen akzeptiert werden.

- Um Traps verwenden zu können, muss ein SNMP-Manager (der nicht in AsyncOS enthalten ist) ausgeführt werden, und seine IP-Adresse muss als Trap-Ziel eingegeben werden. (Sie können einen Hostnamen verwenden, aber wenn Sie dies tun, funktionieren Traps nur, wenn DNS funktioniert.)

Verwenden Sie den Befehl **snmpconfig**, um den SNMP-Systemstatus für die Appliance zu konfigurieren. Nachdem Sie Werte für eine Schnittstelle ausgewählt und konfiguriert haben, reagiert die Appliance auf SNMPv3 GET-Anforderungen. Diese Anforderungen der Version 3 müssen ein passendes Kennwort enthalten. Standardmäßig werden Anfragen der Versionen 1 und 2 abgelehnt. Wenn diese Option aktiviert ist, müssen die Anforderungen der Versionen 1 und 2 einen übereinstimmenden Community String enthalten.

Cisco Systems stellt eine *Enterprise* MIB sowie eine Structure of Management Information (SMI)-Datei bereit:

- ASYNCOS-MAIL-MIB.txt - eine SNMPv2-kompatible Beschreibung der Enterprise MIB für Cisco Appliances.
- IRONPORT-SMI.txt: Definiert die Rolle der ASYNCOS-MAIL-MIB in den von IronPort verwalteten SNMP-Produkten.

Beide MIB-Dateien können auf der Seite zum Produktsupport für die Cisco E-Mail Security Appliance gefunden werden.

> **Tipp**: Einige Kunden müssen möglicherweise beide Dateien in einer einzigen My-Datei kompilieren, um beispielsweise HP OpenView zu unterstützen. Ein Tool, das dies ermöglicht, finden Sie unter www.mg-soft.com.

Weitere Einzelheiten zur SNMP-Überwachung finden Sie im Kapitel **Verwalten und Überwachen über die CLI** im **E-Mail-Benutzerhandbuch**.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems