Überwachen der Cisco ESA mit SNMP

Einleitung

In diesem Dokument wird beschrieben, wie Cisco Secure Email Gateway mithilfe von SNMP überwacht wird. Dies umfasst die MIB-Struktur, die OID-Nutzung und praktische Abfragen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse des SNMP-Protokolls
- Zugriff auf die Cisco ESA-Appliance
- Vertrautheit mit der Linux-Kommandozeile
- Cisco ESA mit aktiviertem SNMP-Dienst
- Installierter SNMP-Client (z. B. Net-SNMP-Tools)
- IronPort MIB-Dateien verfügbar und geladen
- Community-String oder SNMP v3-Anmeldedaten

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Email Gateway (ESA)
- Linux-Client mit Net-SNMP-Tools
- MIB-Dateien: IRONPORT-SMI.txt, ASYNCOS-MAIL-MIB.txt

SNMP konfigurieren

Die SNMP-Konfiguration auf der ESA erfolgt über CLI. Um SNMP auf der Cisco ESA zu aktivieren, rufen Sie die CLI auf, und führen Sie snmpconfig aus.

Das Standard-Setup umfasst Folgendes:

- Aktivieren des SNMP-Dienstes
- Auswahl von Management-Schnittstelle und Port (normalerweise 161)
- Aktivieren von SNMPv3 (Standardsicherheit: authPriv mit SHA und AES)
- Festlegen von Authentifizierungs- und Datenschutzpassphrasen
- SNMPv1/v2c aktivieren und den Community-String angeben (z. B. ironport)
- Definieren zulässiger IPv4-Netzwerke für SNMP-Anforderungen
- Konfigurieren der SNMP-Trap-Version und der Trap-Ziel-IP-Adresse
- Systemstandort und Kontaktinformationen festlegen

Nach der Aktivierung von SNMP wird eine Zusammenfassung angezeigt, die ähnlich wie diese aussieht:

```
esa1.ironport.com> snmpconfig

Current SNMP settings:
Listening on interface "Management"



      port 161.
SNMP v3: Enabled. Security level: authPriv
Authentication Protocol: SHA
Encryption Protocol: AES
SNMP v1/v2: Enabled, accepting requests from subnet



      , .
SNMP v1/v2 Community String: ironport
Trap version: V3
Trap target:



Location: esxi data center
System Contact: ciscoros soc
```

Sobald SNMP aktiviert und konfiguriert ist, kann die Appliance SNMP-Abfragen von zulässigen Quell-IPs akzeptieren.

SNMP-Client-Einrichtung und -Abfrage unter Linux

Für dieses Beispiel wurde ein Debian-Server verwendet. Beachten Sie, dass die Installationsschritte je nach Distribution Package Manager variieren können.

SNMP-Tools installieren

```
sudo apt-get install snmp snmp-mibs-downloader
```

Überprüfen Sie, ob die snmpwalk-Binärdatei installiert ist.

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk --version
NET-SNMP version: 5.9
```

MIB-Dateien laden

Speichern Sie die IronPort MIB-Dateien im Ordner /usr/share/snmp/mibs.

```
root@debian-server:/usr/share/snmp/mibs# pwd
/usr/share/snmp/mibs
root@debian-server:/usr/share/snmp/mibs# ls
ASYNCOS-MAIL-MIB.txt  IRONPORT-SMI.txt        NET-SNMP-EXAMPLES-MIB.txt  NET-SNMP-PASS-MIB.txt  UCD-DEMO-MIB.txt    UCD-IPFWACC-MIB.txt
iana                  LM-SENSORS-MIB.txt      NET-SNMP-EXTEND-MIB.txt    NET-SNMP-TC.txt        UCD-DISKIO-MIB.txt  UCD-SNMP-MIB.txt
ietf                  NET-SNMP-AGENT-MIB.txt  NET-SNMP-MIB.txt           NET-SNMP-VACM-MIB.txt  UCD-DLMOD-MIB.txt
```

debian-server oids

Anmerkung: MIB-Dateien finden Sie im SNMP-Artikel, der am Ende dieses Dokuments freigegeben wurde.

Verwenden einer OID zum Überwachen der CPU-Auslastung

Dieser Befehl fragt die ESA nach ihrer aktuellen CPU-Auslastung ab. Die OID verweist direkt auf die in der MIB definierte CPU-Metrik. Die Ausgabe zeigt einen Wert an, z. B. INTEGER: 37, was auf eine CPU-Auslastung von 37 % hinweist. So können Administratoren die Geräteleistung in Echtzeit überwachen und eingreifen, wenn die Auslastung die zulässigen Grenzwerte überschreitet.

```
snmpwalk -v2c -c ironport

      .1.3.6.1.4.1.15497.1.1.1.2
```

Die Verwendung von OIDs in SNMP-Befehlen bietet direkten Zugriff auf spezifische Metriken für eine effektive Überwachung und Fehlerbehebung.

Symbolische Namen aktivieren

```
export MIBS=ALL
```

Durch das Festlegen von export MIBS=ALL können SNMP-Tools von in den MIB-Dateien definierten, für Menschen lesbaren Namen anstelle von langen numerischen OIDs verwendet werden. So können Abfragen einfacher geschrieben, verstanden und bearbeitet werden, da Sie auf Objekte durch aussagekräftige Namen wie workQueueMessages anstatt durch Ziffernfolgen verweisen können.

SNMP-Abfragen ausführen

Verwenden Sie snmpwalk, um die ESA nach Schlüsselmetriken abzufragen. SNMP-Abfragen ermöglichen Ihnen, Status- und Leistungsdaten in Echtzeit von Ihrer Cisco ESA abzurufen. Mithilfe symbolischer Namen können Sie ganz einfach bestimmte Objekte wie den Warteschlangenstatus, den Lizenzablauf und die Hardwarenutzung überwachen, ohne auf komplexe numerische OIDs verweisen zu müssen.

Arbeitswarteschlangen-Nachrichten

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport

      workQueueMessages
ASYNCOS-MAIL-MIB::workQueueMessages.0 = Gauge32: 0
```

Diese Ausgabe zeigt an, dass derzeit keine Meldungen in der ESA-Arbeitswarteschlange vorhanden sind. Der Wert gibt die Anzahl der E-Mails in Echtzeit an, die auf die Verarbeitung warten.

CPU-Auslastung

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

```
Dies zeigt an, dass die CPU der ESA derzeit eine Auslastung von 37 % aufweist. Der Wert gibt Ihnen einen Einblick in die Verarbeitungslast der Appliance zum Zeitpunkt der Ausführung der Abfrage.
```

Ablauftabelle für Lizenzschlüssel

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

```
       keyExpirationTable
ASYNCOS-MAIL-MIB::keyExpirationIndex.1 = INTEGER: 1
ASYNCOS-MAIL-MIB::keyExpirationIndex.2 = INTEGER: 2
ASYNCOS-MAIL-MIB::keyExpirationIndex.3 = INTEGER: 3
ASYNCOS-MAIL-MIB::keyExpirationIndex.4 = INTEGER: 4
ASYNCOS-MAIL-MIB::keyExpirationIndex.5 = INTEGER: 5
ASYNCOS-MAIL-MIB::keyExpirationIndex.6 = INTEGER: 6
ASYNCOS-MAIL-MIB::keyExpirationIndex.7 = INTEGER: 7
ASYNCOS-MAIL-MIB::keyExpirationIndex.8 = INTEGER: 8
ASYNCOS-MAIL-MIB::keyDescription.1 = STRING: Bounce Verification
ASYNCOS-MAIL-MIB::keyDescription.2 = STRING: Data Loss Prevention
ASYNCOS-MAIL-MIB::keyDescription.3 = STRING: External Threat Feeds
ASYNCOS-MAIL-MIB::keyDescription.4 = STRING: Incoming Mail Handling
ASYNCOS-MAIL-MIB::keyDescription.5 = STRING: IronPort Anti-Spam
ASYNCOS-MAIL-MIB::keyDescription.6 = STRING: IronPort Email Encryption
ASYNCOS-MAIL-MIB::keyDescription.7 = STRING: Outbreak Filters
ASYNCOS-MAIL-MIB::keyDescription.8 = STRING: Sophos Anti-Virus
ASYNCOS-MAIL-MIB::keyIsPerpetual.1 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.2 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.3 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.4 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.5 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.6 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.7 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.8 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.1 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.2 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.3 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.4 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.5 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.6 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.7 = Gauge32: 0
```

```
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.8 = Gauge32: 0
```

- keyExpirationIndex.X: Jeder Index steht für einen eindeutigen Feature-Schlüssel, der auf der Cisco ESA installiert ist.
- keyDescription.X: Enthält den Namen oder die Beschreibung der einzelnen Feature-Schlüssel, z. B. 'Bounce-Verifizierung', 'Schutz vor Datenverlust', 'IronPort Anti-Spam' und 'Sophos Anti-Virus'.
- keyIsPerpetual.x: Gibt an, ob die Lizenz für jede Funktion unbefristet ist. Der Wert true (1) bedeutet, dass die Lizenz nicht abläuft.
- keySecondsUntilExpire.x: Zeigt an, wie viele Sekunden bis zum Ablauf der Lizenz verbleiben. Mit dem Wert 0 wird bestätigt, dass die Lizenz unbefristet ist oder bereits abgelaufen ist.

```
[]> summary

Feature Name                                                    License Authorization Status
--------------------------------------------------------------------------------------------
Email Security Appliance Anti-Spam License                      In Compliance
Email Security Appliance Outbreak Filters                       In Compliance
Email Security Appliance Graymail Safe-unsubscribe              Not requested
Email Security Appliance External Threat Feeds                  In Compliance
Email Security Appliance Advanced Malware Protection Reputation Not requested
Mail Handling                                                   In Compliance
Email Security Appliance Sophos Anti-Malware                    In Compliance
Email Security Appliance PXE Encryption                         In Compliance
Email Security Appliance Advanced Malware Protection            Not requested
Email Security Appliance McAfee Anti-Malware                    Not requested
Email Security Appliance Intelligent Multi-Scan                 Not requested
Email Security Appliance Image Analyzer                         Not requested
Email Security Appliance Bounce Verification                    In Compliance
Email Security Appliance Data Loss Prevention                   In Compliance
```

Lizenzbeispiel

Diese Ausgabe bestätigt die aktuellen Feature-Schlüssel der Appliance, ihre Beschreibungen und den Lizenzstatus. Alle aufgeführten Lizenzen sind unbefristet, wie durch keyIsPerpetual und keySecondsUntilExpire angegeben. Diese Informationen tragen dazu bei, dass wichtige Sicherheitsfunktionen auf Ihrer Cisco ESA aktiv und gültig bleiben.

Unterschied zwischen numerischen OIDs und symbolischen Namen

Numerische OIDs:

- Sie sind universell und funktionieren immer, auch wenn die MIB-Dateien nicht auf das System geladen werden.
- Beispiel: .1.3.6.1.4.1.15497.1.1.1.2.
- Sie sind weniger lesbar und können schwer zu merken sein.

Symbolnamen:

- Dies sind benutzerfreundliche Namen, die in den MIB-Dateien definiert sind, z. B. perCentCPUtilization.
- Sie erleichtern das Schreiben und Verstehen von Befehlen.
- Sie erfordern, dass die MIB-Dateien korrekt geladen und die MIBS-Umgebungsvariable

konfiguriert werden.
- Beispiel: snmpwalk -v2c -c ironport 10.31.124.165 perCentCPUtilization.

Ist es das Gleiche?

Beide Methoden fragen dieselbe Metrik ab und liefern identische Ergebnisse, aber symbolische Namen sind praktischer und für Menschen lesbarer, während numerische OIDs in Umgebungen, in denen MIB-Dateien nicht vorhanden oder geladen sein können, zuverlässiger sind.

Zugehörige Informationen

- Überwachung von Systemzustand und -status mit SNMP
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.