使用SNMP監控Cisco ESA

簡介

本文說明如何使用SNMP監控Cisco安全電子郵件閘道，包括MIB結構、OID使用情況和實際查詢。

必要條件

需求

思科建議您瞭解以下主題：

- SNMP協定基礎知識
- 訪問Cisco ESA裝置
- 熟悉Linux命令列
- 啟用SNMP服務的Cisco ESA
- 已安裝SNMP使用者端（例如Net-SNMP工具）
- IronPort MIB檔案可用並載入
- 社群字串或SNMP v3憑據

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全電子郵件閘道(ESA)
- 使用Net-SNMP工具的Linux客戶端
- MIB檔案：IRONPORT-SMI.txt、ASYNCOS-MAIL-MIB.txt

設定SNMP

ESA上的SNMP配置通過CLI完成。若要在Cisco ESA上啟用SNMP，請訪問CLI並運行snmpconfig。

預設設定包括：

- 啟用SNMP服務
- 選擇管理介面和埠（通常為161）
- 啟用SNMPv3(預設安全：authPriv（含SHA和AES）
- 設定身份驗證和隱私密碼
- 啟用SNMPv1/v2c，指定社群字串（例如ironport）
- 為SNMP請求定義允許的IPv4網路
- 配置SNMP陷阱版本和陷阱目標IP地址
- 設定系統位置和聯絡資訊

啟用SNMP後，您可以看到類似以下的摘要：

```
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
```

啟用並配置SNMP後，裝置即可接受來自允許的源IP的SNMP查詢。

Linux上的SNMP客戶端設定和查詢

在本示例中，使用了Debian伺服器。請注意，安裝步驟可能因分發包管理器的不同而不同。

安裝SNMP工具

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

驗證是否已安裝snmpwalk binary。

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

載入MIB檔案

將IronPort MIB檔案放在/usr/share/snmp/mibs檔案夾。

```
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 oid

附註：MIB檔案可以在本文檔末尾共用的SNMP文章中找到。

使用OID監控CPU利用率

此命令查詢ESA其當前CPU利用率。OID直接指向MIB中定義的CPU度量。輸出會顯示一個值，例如INTEGER:37，表示裝置CPU使用率為37%。這使管理員能夠即時監控裝置效能，並在利用率超過可接受限制時進行干預。

```
snmpwalk -v2c -c ironport

      .1.3.6.1.4.1.15497.1.1.1.2
```

在SNMP命令中使用OID可以直接訪問特定指標，以便進行有效的監控和故障排除。

啟用符號名稱

```
export MIBS=ALL
```

設定export MIB=ALL允許SNMP工具使用在MIB檔案中定義的人為可讀名稱，而不是長數字OID。這使得查詢更易於編寫、理解和故障排除，因為您可以使用有意義的名稱（如workQueueMessages）而不是數字序列來引用對象。

運行SNMP查詢

使用snmpwalk查詢ESA以獲取關鍵度量。SNMP查詢允許您從思科ESA檢索即時狀態和效能資料。通過使用符號名稱，您可以輕鬆監控特定對象，如隊列狀態、許可證到期和硬體利用率，而無需參考複雜的數字OID。

工作隊列消息

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

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

此輸出顯示ESA工作隊列中當前有零條消息。該值表示等待處理的即時電子郵件數。

CPU利用率

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

這表明ESA的CPU當前使用率為37%。通過此值，您可以深入瞭解執行查詢時裝置的處理負載。

許可證金鑰到期表

```
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:每個索引代表安裝在Cisco ESA上的唯一功能金鑰。
- keyDescription.X:提供每個功能金鑰的名稱或說明，例如「退回驗證」、「防資料丟失」、「IronPort反垃圾郵件」和「Sophos防病毒」。
- keyIsPerpetual.X:指示每個功能的許可證是否為永久許可證。值true(1)表示許可證未過期。
- keySecondsUntilExpire.X:顯示許可證到期前剩餘的秒數。值為0可確認許可證是永久許可證或已過期。

```
[]> 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
```

許可證示例

此輸出確認裝置的當前功能金鑰、其說明和許可證狀態。所有列出的許可證都是永久許可證，如keyIsPerpetual和keySecondsUntilExpire所示。此資訊有助於確保您的思科ESA上的基本安全功能保持活躍和有效。

數字OID和符號名稱之間的區別

數字OID:

- 它們是通用的，並且總是可以工作，即使MIB檔案沒有載入到系統上。
- 範例：.1.3.6.1.4.1.15497.1.1.1.2。
- 它們很難讀懂，也很難記憶。

符號名稱：

- 這些是在MIB檔案中定義的使用者友好名稱，例如perCentCPUUtization。
- 它們使命令更容易編寫和理解。
- 它們要求正確載入MIB檔案，並配置MIB環境變數。
- 範例：snmpwalk -v2c -c ironport 10.31.124.165% CPUUilization。

還是一樣？

這兩種方法查詢相同的度量並產生相同的結果，但符號名稱更實用、更易於閱讀，而數字OID在無法存在或載入MIB檔案的環境中更可靠。

相關資訊

- 使用SNMP監控系統運行狀況和狀態
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。