使用SNMP监控Cisco ESA

简介

本文档介绍如何使用SNMP监控Cisco安全邮件网关，包括MIB结构、OID使用情况和实际查询。

先决条件

要求

Cisco 建议您了解以下主题：

- SNMP协议基础知识
- 访问Cisco ESA设备
- 熟悉Linux命令行
- 启用SNMP服务的思科ESA
- 已安装SNMP客户端（例如Net-SNMP工具）
- 可用并加载的IronPort MIB文件
- 社区字符串或SNMP v3凭证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全邮件网关(ESA)
- 使用Net-SNMP工具的Linux客户端
- MIB文件：IRONPORT-SMI.txt、ASYNCOS-MAIL-MIB.txt

配置SNMP

ESA上的SNMP配置通过CLI完成。要在Cisco ESA上启用SNMP，请访问CLI并运行snmpconfig。

默认设置包括：

- 启用SNMP服务
- 选择管理接口和端口（通常为161）
- 启用SNMPv3(默认安全：带SHA和AES的authPriv)
- 设置身份验证和隐私密码
- 启用SNMPv1/v2c，指定社区字符串（例如，ironport）
- 为SNMP请求定义允许的IPv4网络
- 配置SNMP陷阱版本和陷阱目标IP地址
- 设置系统位置和联系人信息

启用SNMP后，您可以看到类似如下所示的摘要：

```
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
```

启用并配置SNMP后，设备即可接受来自允许的源IP的SNMP查询。

Linux上的SNMP客户端设置和查询

在本示例中，使用了Debian服务器。请注意，安装步骤可能会因分发软件包管理器的不同而不同。

安装SNMP工具

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

验证是否已安装snmpwalk二进制。

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

加载MIB文件

将IronPort MIB文件放入/usr/share/snmp/mibs文件夹。

```
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

注意：MIB文件可以在本文档末尾共享的SNMP文章中找到。

使用OID监控CPU利用率

此命令可查询ESA了解其当前CPU利用率。OID直接指向MIB中定义的CPU度量。输出显示一个值，例如INTEGER:37，表示设备CPU使用率为37%。这使管理员能够实时监控设备性能，并在利用率超过可接受限制时进行干预。

```
snmpwalk -v2c -c ironport

      .1.3.6.1.4.1.15497.1.1.1.2
```

在SNMP命令中使用OID可以直接访问特定指标，以便进行有效的监控和故障排除。

启用符号名称

```
export MIBS=ALL
```

设置export MIBS=ALL允许SNMP工具使用MIB文件中定义的人可读名称，而不是长数字OID。这使得查询更易于编写、理解和故障排除，因为您可以使用有意义的名称（如workQueueMessages）而不是数字序列来引用对象。

运行SNMP查询

使用snmpwalk查询ESA以获取关键度量。SNMP查询允许您从Cisco ESA检索实时状态和性能数据。通过使用符号名称，您可以轻松监控特定对象，例如队列状态、许可证到期和硬件利用率，而无需参考复杂的数字OID。

工作队列消息

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

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

此输出显示ESA工作队列中当前没有消息。该值表示等待处理的电子邮件的实时数量。

CPU 利用率

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

这表示ESA的CPU当前使用率为37%。通过此值，您可以了解执行查询时设备的处理负载。

许可证密钥到期表

```
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:每个索引代表安装在Cisco ESA上的唯一功能密钥。
- keyDescription.X:提供每个功能密钥的名称或说明，例如“退回验证”、“防数据丢失”、“IronPort反垃圾邮件”和“Sophos防病毒”。
- keyIsPerpetual.X:指示每个功能的许可证是否为永久许可证。值true(1)表示许可证不会过期。
- keySecondsUntilExpire.X:显示许可证到期前剩余的秒数。值为0可确认许可证是永久许可证或已过期。

```
[]> 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
```

许可证示例

此输出确认设备的当前功能密钥、其说明和许可证状态。列出的所有许可证都是永久许可证，如keyIsPerpetual和keySecondsUntilExpire所示。此信息有助于确保基本安全功能在您的Cisco ESA上保持活动和有效。

数字OID和符号名称之间的区别

数字OID:

- 它们是通用的，并且始终可用，即使MIB文件未加载到系统上。
- 示例：.1.3.6.1.4.1.15497.1.1.1.2。
- 它们可读性较差，可能难以记忆。

符号名称：

- 这些是在MIB文件中定义的用户友好名称，例如perCentCPUUtiilization。
- 它们使命令更容易编写和理解。
- 它们需要正确加载MIB文件并配置MIB环境变量。
- 示例：snmpwalk -v2c -c ironport 10.31.124.165% CPUUilization。

还是一样吗？

这两种方法查询相同的度量并产生相同的结果，但符号名称更实用且易于阅读，而数字OID在无法存在或加载MIB文件的环境中更可靠。

相关信息

- 使用SNMP监控系统运行状况和状态
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。