SNMP로 Cisco ESA 모니터링

소개

이 문서에서는 MIB 구조, OID 사용 및 실제 쿼리를 비롯하여 SNMP를 사용하여 Cisco Secure Email Gateway를 모니터링하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SNMP 프로토콜에 대한 기본 지식
- Cisco ESA 어플라이언스 액세스
- Linux 명령줄에 익숙함
- SNMP 서비스가 활성화된 Cisco ESA
- 설치된 SNMP 클라이언트(예: Net-SNMP 툴)
- 사용 가능 및 로드된 IronPort MIB 파일
- 커뮤니티 문자열 또는 SNMP v3 자격 증명

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ESA(Secure Email Gateway)
- Net-SNMP 툴을 사용하는 Linux 클라이언트
- MIB 파일: IRONPORT-SMI.txt, ASYNCOS-MAIL-MIB.txt

SNMP 구성

ESA의 SNMP 컨피그레이션은 CLI를 통해 수행됩니다. Cisco ESA에서 SNMP를 활성화하려면 CLI에 액세스하여 snmpconfig를 실행합니다.

기본 설정은 다음과 같습니다.

- SNMP 서비스 활성화
- 관리 인터페이스 및 포트 선택(일반적으로 161)
- SNMPv3 활성화(기본 보안: authPriv(SHA 및 AES 사용)
- 인증 및 개인 정보 보호 암호 설정
- 커뮤니티 문자열(예: ironport)을 지정하여 SNMPv1/v2c 활성화
- SNMP 요청에 대해 허용되는 IPv4 네트워크 정의
- SNMP 트랩 버전 및 트랩 대상 IP 주소 구성
- 시스템 위치 및 연락처 정보 설정

SNMP를 활성화하면 다음과 유사한 요약을 볼 수 있습니다.

```
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
```

SNMP를 활성화하고 구성하면 어플라이언스는 허용된 소스 IP에서 SNMP 쿼리를 받아들일 준비가 됩니다.

Linux에서 SNMP 클라이언트 설정 및 쿼리

이 예에서는 데비안 서버가 사용되었습니다. 설치 단계는 배포 패키지 관리자에 따라 다를 수 있습니다.

SNMP 도구 설치

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

snmpwalk 바이너리가 설치되어 있는지 확인합니다.

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

MIB 파일 로드

IronPort MIB 파일을 /usr/share/snmp/mibs 폴더에 배치합니다.

```
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
```

데비안 서버 oid

참고: MIB 파일은 이 문서의 끝에 공유되는 SNMP 문서에서 찾을 수 있습니다.

OID를 사용하여 CPU 사용률 모니터링

이 명령은 ESA에서 현재 CPU 사용률을 쿼리합니다. OID는 MIB에 정의된 CPU 메트릭을 직접 가리킵니다. 출력에 INTEGER와 같은 값이 표시됩니다. 37 - 디바이스 CPU 사용량이 37%임을 나타냅니다. 이를 통해 관리자는 디바이스 성능을 실시간으로 모니터링하고 사용률이 허용 한도를 초과하는 경우 개입할 수 있습니다.

```
snmpwalk -v2c -c ironport
```

```
      .1.3.6.1.4.1.15497.1.1.1.2
```

SNMP 명령에서 OID를 사용하면 효과적인 모니터링 및 문제 해결을 위해 특정 메트릭에 직접 액세스할 수 있습니다.

기호 이름 사용

```
export MIBS=ALL
```

export MIBS=ALL을 설정하면 SNMP 툴에서 긴 숫자 OID 대신 MIB 파일에 정의된 사람이 읽을 수 있는 이름을 사용할 수 있습니다. 이렇게 하면 숫자 시퀀스보다는 workQueueMessages와 같은 의미 있는 이름으로 개체를 참조할 수 있으므로 쿼리를 더 쉽게 작성하고 이해하고 문제를 해결할 수 있습니다.

SNMP 쿼리 실행

ESA에 주요 메트릭을 쿼리하려면 snmpwalk를 사용합니다. SNMP 쿼리를 사용하면 Cisco ESA에서 실시간 상태 및 성능 데이터를 검색할 수 있습니다. 기호 이름을 사용하면 복잡한 숫자 OID를 참조할 필요 없이 대기열 상태, 라이센스 만료 및 하드웨어 사용률과 같은 특정 객체를 쉽게 모니터링할 수 있습니다.

작업 대기열 메시지

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

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

이 출력은 현재 ESA 작업 대기열에 메시지가 없음을 보여줍니다. 이 값은 처리 대기 중인 전자 메일의 실시간 수를 나타냅니다.

CPU 사용률

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

이는 ESA의 CPU가 현재 사용률이 37%임을 나타냅니다. 이 값을 사용하면 쿼리가 실행되는 순간 어플라이언스의 처리 로드를 파악할 수 있습니다.

라이센스 키 만료 테이블

```
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: 각 인덱스는 Cisco ESA에 설치된 고유한 기능 키를 나타냅니다.
- keyDescription.X: '바운스 확인', '데이터 손실 방지', 'IronPort 안티스팸', 'Sophos 안티바이러스' 등 각 기능 키의 이름이나 설명을 제공합니다.
- keyIsPerpetual.X: 각 기능의 라이센스가 영구적인지 여부를 나타냅니다. 값이 true(1)이면 라이센스가 만료되지 않습니다.
- keySecondsUntilExpire.X: 라이센스가 만료될 때까지 남은 시간(초)을 표시합니다. 값이 0이면 라이센스가 영구 라이

센스이거나 이미 만료되었음을 확인합니다.

```
[]> 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
```

라이센스 예

이 출력은 어플라이언스의 현재 기능 키, 설명 및 라이센스 상태를 확인합니다. 나열된 모든 라이센스는 keyIsPerpetual 및 keySecondsUntilExpire에 표시된 대로 영구적입니다. 이 정보를 통해 Cisco ESA에서 필수 보안 기능이 활성 상태로 유지되고 유효한지 확인할 수 있습니다.

숫자 OID와 기호 이름의 차이점

숫자 OID:

- MIB 파일이 시스템에 로드되지 않은 경우에도 이 기능은 보편적이며 항상 작동합니다.
- 예: .1.3.6.1.4.1.15497.1.1.1.2
- 읽기 어렵고 기억하기 어려울 수 있습니다.

기호 이름:

- 이러한 이름은 perCentCPUUtilization과 같이 MIB 파일에 정의된 사용자 친화적인 이름입니다.
- 명령을 쉽게 작성하고 이해할 수 있도록 합니다.
- MIB 파일을 올바르게 로드하고 MIB 환경 변수를 구성해야 합니다.
- 예: snmpwalk -v2c -c ironport 10.31.124.165 perCentCPUUtilization

똑같은 가요?

두 방법 모두 동일한 메트릭을 쿼리하고 동일한 결과를 생성하지만 기호 이름은 보다 실용적이고 사람이 읽을 수 있는 반면, 숫자 OID는 MIB 파일이 없거나 로드될 수 없는 환경에서 더 안정적입니다.

관련 정보

- SNMP를 사용하여 시스템 상태 모니터링
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.