SWA에서 SNMP 구성 및 문제 해결

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

SNMP 작동 방식

- MIB
- SNMP 트랩
- SNMPv3

SWA의 SNMP

- SNMPMonitor 구성
- SWA MIB 파일
- SWA SNMP 트랩
- 권장 모니터링 OID

SNMP 문제 해결

- 좁은 통로
  - Windows 운영 체제에 SNMPWALK 설치
  - Linux 커널에 SNMPWALK 설치
  - MacOS에 SNMPWALK 설치
- SNMPTRAP
- SWA의 SNMP 로그
- SNMP의 일반적인 문제
  - 일부 OIDS가 실패함(값 없음 또는 잘못된 값).

소개

이 문서에서는 SWA(Secure Web Appliance)의 SNMP(Simple Network Monitoring Protocol) 문제 해결 단계를 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SWA의 CLI(Command Line Interface) 액세스
- SWA에 대한 관리 액세스.
- SNMP에 대한 기본 지식

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

SNMP 작동 방식

SNMP는 네트워크 장치가 이러한 시스템 간에 또는 네트워크 외부의 다른 장치와 관리 정보를 교환할 수 있는 애플리케이션 레이어 통신 프로토콜입니다.

네트워크 관리자는 SNMP를 통해 네트워크 성능을 관리하고 네트워크 문제를 찾아 해결하고 네트워크 성장을 계획할 수 있습니다.

SNMP는 네트워크 모니터링을 비용 효율적으로 만들고 네트워크의 안정성을 높입니다. (SNMP에 대한 자세한 내용은 RFC 1065, 1066 및 1067을 참조하십시오.)

SNMP 관리 네트워크는 관리자, 에이전트 및 관리 대상 디바이스로 구성됩니다.

- Manager는 휴먼 네트워크 관리자와 관리 시스템 간의 인터페이스를 제공합니다.
- 에이전트는 관리자와 관리되는 디바이스 간의 인터페이스를 제공합니다
- 관리 시스템은 대부분의 관리 프로세스를 실행하며 네트워크 관리에 사용되는 대량의 메모리 리소스를 제공합니다.

에이전트는 각 관리되는 디바이스에 상주하며, 소프트웨어 트랩에 포착된 로컬 관리 정보 데이터(예: 성능 정보 또는 이벤트 및 오류 정보)를 관리 시스템을 위한 읽기 가능한 형태로 변환합니다.

SNMP 에이전트는 MIB(Management Information Base)(디바이스 매개변수 및 네트워크 데이터 저장소) 또는 오류 또는 변경 트랩에서 데이터를 캡처합니다.

MIB

MIB는 SNMP 네트워크 요소를 데이터 객체 목록으로 설명하는 데이터 구조입니다. SNMP 관리자는 SNMP 디바이스를 모니터링하기 위해 네트워크의 각 장비 유형에 대한 MIB 파일을 컴파일해야 합니다.

관리자와 에이전트는 MIB와 비교적 작은 명령 집합을 사용하여 정보를 교환합니다. MIB는 나뭇가지에 나뭇잎으로 표시되는 개별 변수와 함께 트리 구조로 구성됩니다.

OID(long numeric tag or object identifier)는 MIB 및 SNMP 메시지에서 각 변수를 고유하게 구별하는 데 사용됩니다. MIB는 각 OID를 읽기 가능한 레이블 및 객체와 관련된 다양한 기타 매개변수와 연결합니다.

그런 다음 MIB는 SNMP 메시지를 취합하고 해석하는 데 사용되는 데이터 사전 또는 코드북의 역할을 합니다.

SNMP 관리자는 경보 지점의 상태, 시스템 이름 또는 요소 가동 시간과 같은 객체의 값을 알고 싶을 때 각 관심 객체의 OID가 포함된 GET 패킷을 취합합니다.

이 요소는 요청을 받고 MIB(코드북)에서 각 OID를 조회합니다. OID가 발견되면(객체가 요소에서 관리됨) 응답 패킷이 어셈블되고 객체의 현재 값이 포함된 상태로 전송됩니다.

OID를 찾을 수 없는 경우 관리되지 않는 객체를 식별하는 특별한 오류 응답이 전송됩니다

SNMP 트랩

SNMP 트랩을 사용하면 에이전트가 요청하지 않은 SNMP 메시지를 통해 중요한 이벤트를 관리 스테이션에 알릴 수 있습니다.

SNMPv1 및 SNMPv2c는 관련 MIB와 함께 트랩 방향 알림을 장려합니다.

트랩 지향 알림의 기본 개념은 관리자가 많은 수의 디바이스를 담당하고, 각 디바이스에 많은 수의 개체가 있는 경우 관리자가 모든 디바이스의 모든 개체에서 정보를 폴링하거나 요청하는 것이 비실용적이라는 것입니다.

이 솔루션은 매니지드 디바이스의 각 에이전트가 요청 없이 관리자에게 알림을 보냅니다. 이를 위해 이벤트의 트랩이라고 하는 메시지를 전송합니다.

관리자는 이벤트를 수신한 후 이벤트를 표시하고 이를 기반으로 조치를 취할 수 있습니다. 예를 들어, 관리자는 에이전트를 직접 폴링하거나 관련된 다른 디바이스 에이전트를 폴링하여 이벤트를 더 잘 파악할 수 있습니다.

트랩 지정 알림은 경솔한 SNMP 요청을 제거함으로써 네트워크 및 에이전트 리소스를 크게 절약할 수 있습니다. 그러나 SNMP 폴링을 완전히 제거할 수는 없습니다.

SNMP 요청은 검색 및 토폴로지 변경에 필요합니다. 또한 매니지드 디바이스 에이전트는 디바이스에 치명적인 중단이 발생한 경우 트랩을 전송할 수 없습니다.

SNMPv1 트랩은 다음 필드를 사용하여 RFC 1157에 정의됩니다.

- Enterprise: 트랩을 생성하는 관리 객체의 유형을 식별합니다.
- 에이전트 주소: 트랩을 생성하는 관리되는 개체의 주소를 제공합니다.
- 일반 트랩 유형: 여러 일반 트랩 유형 중 하나를 나타냅니다.
- 특정 트랩 코드: 여러 특정 트랩 코드 중 하나를 나타냅니다.
- Time stamp: 마지막 네트워크 재초기화와 트랩 생성 사이에 경과된 시간을 제공합니다.
- 변수 바인딩: PDU를 포함하는 트랩의 데이터 필드입니다. 각 변수 바인딩은 특정 MIB 개체 인스턴스를 현재 값과 연결합니다.

SNMPv3

SNMPv3은 각 SNMP 엔터티를 고유하게 식별하는 SNMP "엔진 ID" 식별자를 지원합니다. 두

SNMP 엔터티에 중복된 EngineID가 있을 경우 충돌이 발생할 수 있습니다.

EngineID는 인증된 메시지에 대한 키를 생성하는 데 사용됩니다. (SNMPv3에 대한 자세한 내용은 RFC 2571-2575를 참조하십시오.)

대부분의 SNMP 제품은 SNMPv3에서 기본적으로 동일하지만 다음과 같은 새로운 기능을 통해 향상됩니다.

보안

- 인증
- 프라이버시

관리

- 권한 부여 및 액세스 제어
- 논리적 컨텍스트
- 엔티티, ID 및 정보 이름 지정
- 사람 및 정책
- 사용자 이름 및 키 관리
- 알림 대상 및 프록시 관계
- SNMP 작업을 통한 원격 구성

SNMPv3 보안 모델은 주로 Authentication(인증)과 Encryption(암호화)의 두 가지 형태로 제공됩니다.

인증은 의도한 수신자만 트랩을 읽는지 확인하는 데 사용됩니다. 메시지가 생성되면 엔티티 EngineID를 기반으로 특수 키가 제공됩니다. 키는 의도된 수신자와 공유되며 메시지를 수신하는 데 사용됩니다.
암호화, 프라이버시는 SNMP 메시지의 페이로드를 암호화하여 권한이 없는 사용자가 읽을 수 없도록 합니다. 왜곡된 문자로 가득 찬 모든 인터셉트트랩은 읽을 수 없습니다. 프라이버시는 SNMP 메시지가 인터넷을 통해 라우팅되어야 하는 응용 프로그램에서 특히 유용합니다.
SNMP 그룹에는 세 가지 보안 레벨이 있습니다.

noAuthnoPriv - 인증 및 프라이버시 없는 통신.
authNoPriv - 프라이버시 없이 인증과 통신 인증에 사용되는 프로토콜은 MD5(Message-Digest Algorithm 5) 및 SHA(Secure Hash Algorithm)입니다.
authPriv - 인증 및 개인 정보 보호와의 통신 인증에 사용되는 프로토콜은 MD5 및 SHA이며, 프라이버시의 경우 DES(Data Encryption Standard) 및 AES(Advanced Encryption Standard) 프로토콜을 사용할 수 있습니다.

SWA의 SNMP

AsyncOS 운영 체제는 SNMP를 통한 시스템 상태 모니터링을 지원합니다.

참고:

- SNMPisoffby는 기본적으로 사용됩니다.

- SNMPSET 작업(컨피그레이션)은 구현되지 않습니다.
- AsyncOS는 SNMPv1, v2 및 v3을 지원합니다.
- SNMPv3을 활성화할 경우 메시지 인증 및 암호화가 필수입니다. 인증 및 암호화의 암호는 서로 달라야 합니다.
- 암호화 알고리즘은 AES(권장) 또는 DES일 수 있습니다.
- 인증 알고리즘은 SHA-1(권장) 또는 MD5일 수 있습니다.
- snmpconfig 명령은 다음에 명령을 실행할 때 패스프레이즈를 "기억"합니다.
- AsyncOS 15.0 이전 릴리스의 경우 SNMPv3 사용자 이름은 v3get입니다.
- AsyncOS 릴리스 15.0 이상의 경우 defaultSNMPv3 사용자 이름은 v3get입니다. 관리자는 다른 사용자 이름을 선택할 수 있습니다.
- SNMPv1 또는 SNMPv2만 사용하는 경우 커뮤니티 문자열을 설정해야 합니다. 커뮤니티 문자열의 기본값은 public이 아닙니다.
- SNMPv1 및 SNMPv2의 경우 SNMPGET 요청을 수락할 네트워크를 지정해야 합니다.
- 트랩을 사용하려면 AsyncOS에 포함되지 않은 SNMPmanager가 실행 중이고 해당 IP 주소가 트랩 대상으로 입력되어야 합니다. (호스트 이름을 사용할 수 있지만 사용할 경우 DNS가 작동 중인 경우에만 트랩이 작동합니다.)

SNMPMonitor 구성

어플라이언스에 대한 시스템 상태 정보를 수집하도록 SNMP를 구성하려면 CLI에서 ssnmpconfig 명령을 사용합니다. 인터페이스에 대한 값을 선택하고 구성하면 어플라이언스는 SNMPv3 GET 요청에 응답합니다.

SNMP를 사용할 때 다음 사항을 고려하십시오.

- SNMP 버전 3에서 요청은 일치하는 패스프레이즈를 포함해야 합니다.
- 기본적으로 버전 1 및 2 요청은 거부됩니다.
- 활성화된 경우 버전 1 및 2 요청에 일치하는 커뮤니티 문자열이 있어야 합니다.

```
SWA_CLI> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP? [Y]> Y
```

```
Please choose an IP interface for SNMP requests.
1. Management (10.48.48.184/24 on Management: wsa125to15-man.amojarra.calo)
2. P1 (192.168.13.184/24 on P1: wsa1255p1.amojarra.calo)
3. P2 (192.168.133.184/24 on P2: wsa1255p2.amojarra.calo)
[1]> 1

Which port shall the SNMP daemon listen on?
[161]> 161

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 username or press return to leave it unchanged.
[w3get]> SNMPMUser

Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests? [N]> N

Enter the Trap target as a host name, IP address or list of IP addresses
separated by commas (IP address preferred). Enter "None" to disable traps.
[10.48.48.192]>

Enter the Trap Community string.
[ironport]> swa_community

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Disabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]> Y

Do you want to disable any of these traps? [Y]> N

Do you want to enable any of these traps? [Y]> Y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 6
```

```
Please enter the URL to check for connectivity failure, followed by the
checking interval in seconds, separated by a comma:
[http://downloads.ironport.com,5]>

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Enabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]>

Enter the System Location string.
[location]>

Enter the System Contact string.
[snmp@localhost]>

Current SNMP settings:
Listening on interface "Management" 10.48.48.184/24 port 161.
SNMP v3: Enabled.
SNMP v3 UserName: SNMPMUser
SNMP v3 Authentication type: SHA
SNMP v3 Privacy protocol: AES
SNMP v1/v2: Disabled.
Trap target: 10.48.48.192
Location: location
System Contact: snmp@localhost

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

SWA_CLI> commit
```

SWA MIB 파일

MIB 파일은 URL: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html에서 사용할 수 있습니다.

각 MIB 파일의 최신 버전을 사용합니다.

여러 MIB 파일이 있습니다.

- asyncoswebsecurityappliance-mib.txt는 보안 웹 어플라이언스용 엔터프라이즈 MIB에 대한 SNMPv2 호환 설명입니다.
- ASYNCOS-MAIL-MIB.txt는 Email Security Appliance용 엔터프라이즈 MIB에 대한 SNMPv2 호환 설명입니다.

- IRONPORT-SMI.txt 이 "관리 정보 구조" 파일은 asyncoswebsecurityappliance-mib의 역할을 정의합니다.

이 릴리스는 RFC 1213 및 1907에 정의된 대로 MIB-II의 읽기 전용 하위 집합을 구현합니다.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlto SNMP를 사용하는 어플라이언스의 CPU 사용량 모니터링에 대해 자세히 알아봅니다.

SWA SNMP 트랩

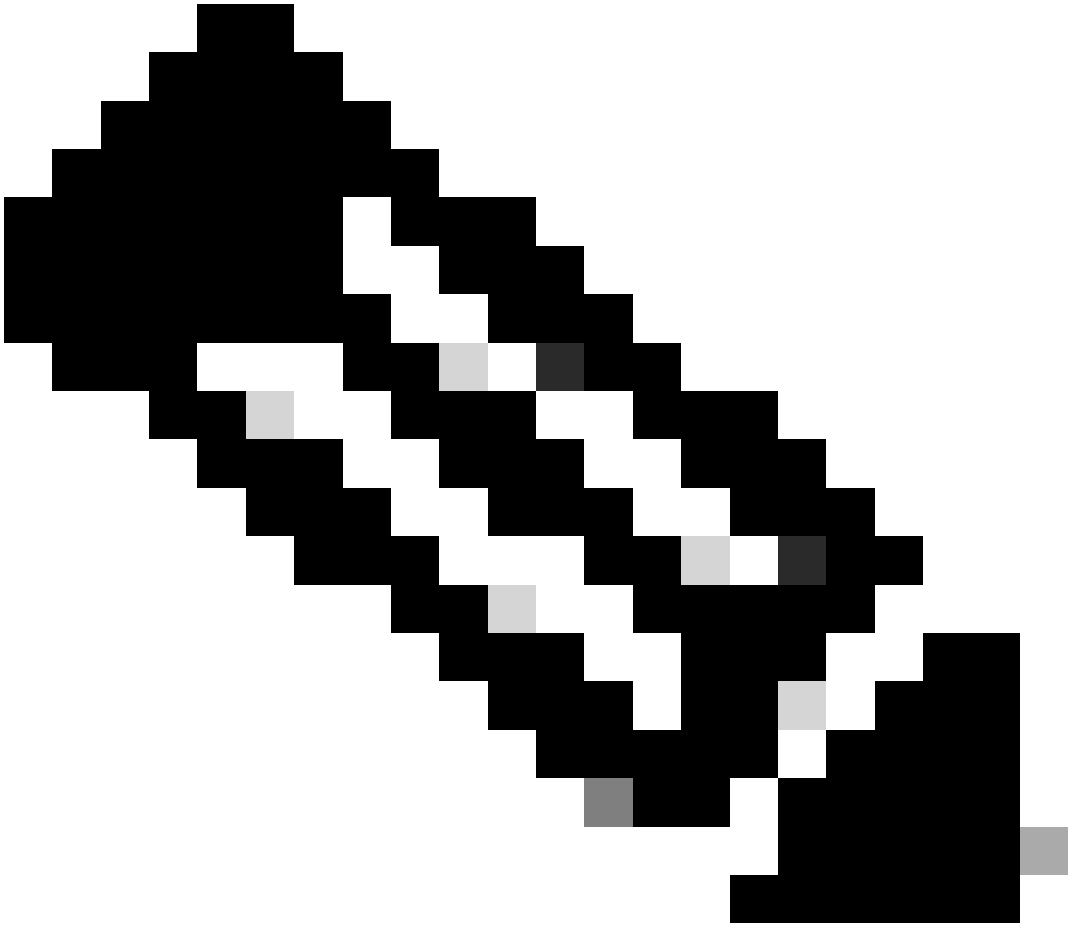
SNMP는 하나 이상의 조건이 충족되었을 때 관리 애플리케이션에 알리기 위해 트랩 또는 알림을 보낼 수 있는 기능을 제공합니다.

트랩은 트랩을 전송하는 시스템의 구성 요소와 관련된 데이터를 포함하는 네트워크 패킷입니다.

SNMPagent에서 조건이 충족될 때 트랩이 생성됩니다(이 경우 CiscoSecure Web Appliance).

조건이 충족되면 SNMPagent는 SNMP 패킷을 형성하고 이를 SNMPmanagement 콘솔 소프트웨어를 실행하는 호스트로 전송합니다.

인터페이스에 대해 SNMP를 활성화할 때 SNMPtraps(특정 트랩 활성화 또는 비활성화)를 구성할 수 있습니다.

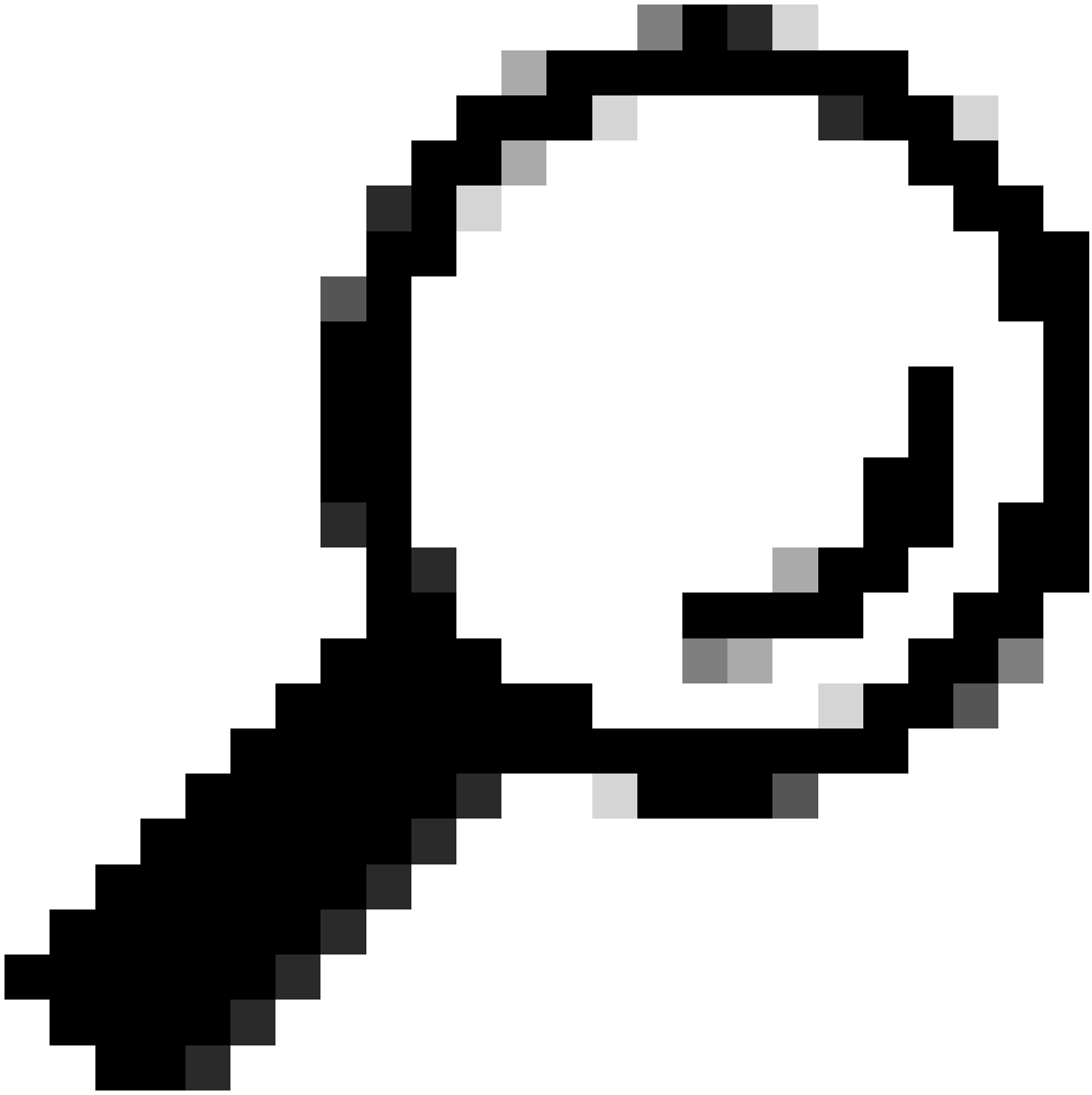


참고: 여러 트랩 대상을 지정하려면: 트랩 대상을 묻는 메시지가 표시되면 쉼표로 구분된 IP 주소를 최대 10개까지 입력할 수 있습니다.

---

connectivityFailure 트랩은 인터넷에 대한 어플라이언스 연결을 모니터링하기 위한 것입니다. 이를 위해 5초에서 7초마다 단일 외부 서버에 연결하고 HTTP GET 요청을 보냅니다. 기본적으로 모니터링되는 URL은 포트 80의 downloads.ironport.com입니다.

모니터링되는 URL 또는 포트를 변경하려면 snmpconfig 명령을 실행하고 connectivityFailure 트랩을 활성화하십시오(이미 활성화된 경우에도). URL을 변경하라는 프롬프트를 볼 수 있습니다.



팁: connectivityFailure 트랩을 시뮬레이션하려면 dnsconfig CLI 명령을 사용하여 작동하지 않는 DNS 서버를 입력할 수 있습니다. downloads.ironport.com에 대한 조회가 실패하고 5-7초마다 트랩이 전송됩니다. 테스트가 끝나면 DNS 서버를 다시 작업 서버로 변경해야 합니다.

권장 모니터링 OID

다음은 전체 목록이 아니라 모니터링해야 할 권장 MIB 목록입니다.

하드웨어 OID	이름
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raid상태

1.3.6.1.4.1.15497.1.1.1.18.1.4	raid마지막 오류
1.3.6.1.4.1.15497.1.1.1.10	팬 테이블
1.3.6.1.4.1.15497.1.1.1.9.1.2	섭씨 온도

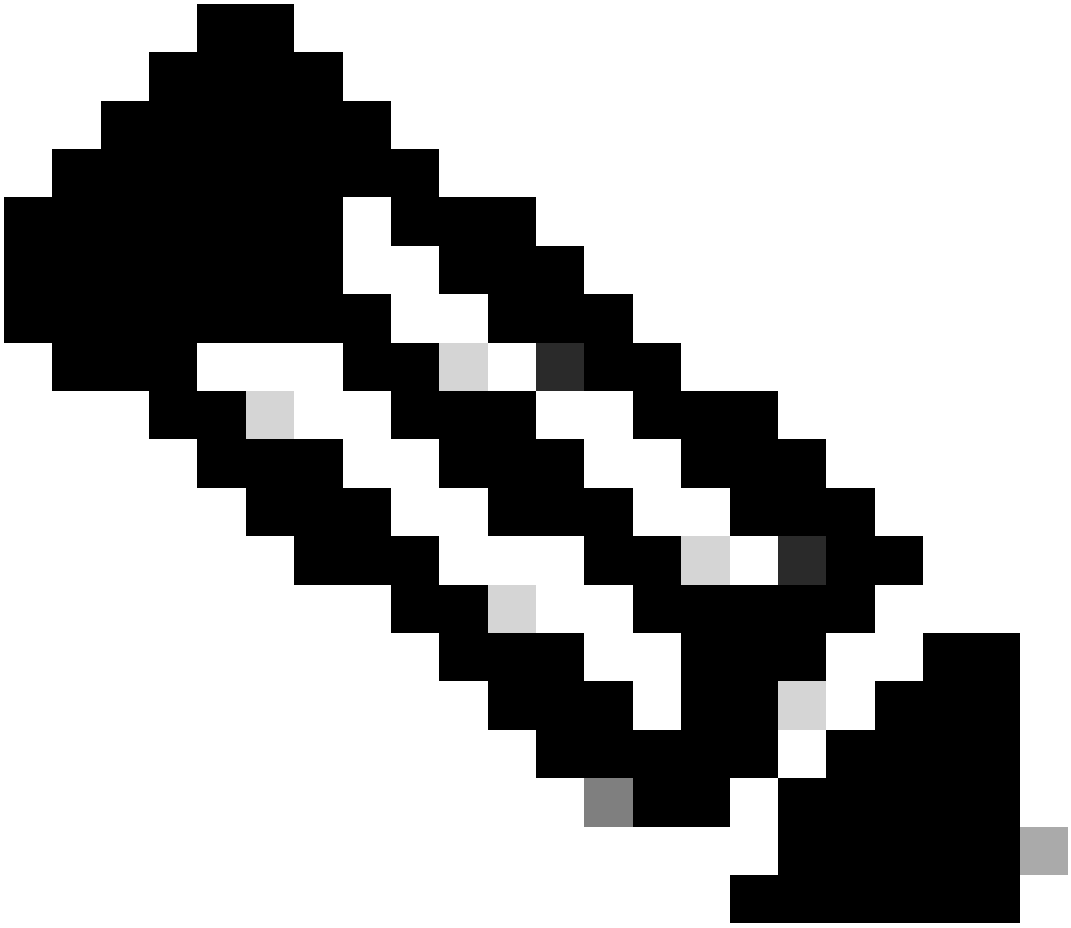
OID는 status detailCLI 명령의 출력에 직접 매핑되는 것입니다.

OID	이름	상태 세부사항 필드
시스템 리소스		
1.3.6.1.4.1.15497.1.1.1.2.0	PerCentCPU사용화	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	perCentMemory사용률	램
초당 트랜잭션		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	캐시처리	최근 1분 동안의 초당 평균 트랜잭션입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	지난 1시간 동안의 초당 최대 트랜잭션 수입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hr평균	지난 1시간 동안의 초당 평균 트랜잭션입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	프록시 재시작 이후 초당 최대 트랜잭션 수입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	프록시 재시작 이후 초당 평균 트랜잭션 수입니다.
Bandwidth		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	캐시현재 너비	지난 1분 동안의 평균 대역폭.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	지난 1시간 동안의 최대 대역폭입니다.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hr평균	지난 1시간의 평균 대역폭입니다.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	캐시너비TotalLifePeak	프록시 재시작 이후 최대 대역폭입니다.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	캐시너비 총 수명 평균	프록시 재시작 이후의 평균 대역폭입니다.
응답 시간		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	캐시 적중률	마지막 순간에 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hr최대	지난 1시간 동안의 최대 캐시 적중률입니다.

1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hr평균	지난 1시간의 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	캐시적중수명의	프록시 재시작 이후 최대 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	캐시 적중수명 평균	프록시 재시작 이후의 평균 캐시 적중률입니다.
캐시 적중률		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	캐시 적중률	마지막 순간에 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hr최대	지난 1시간 동안의 최대 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hr평균	지난 1시간의 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	캐시적중수명의	프록시 재시작 이후 최대 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	캐시 적중수명 평균	프록시 재시작 이후의 평균 캐시 적중률입니다.
연결		
1.3.6.1.4.1.15497.1.2.3.2.7.0	캐시클라이언트유휴 통화	유휴 클라이언트 연결
1.3.6.1.4.1.15497.1.2.3.3.7.0	캐시서버유휴 연결	유휴 서버 연결.
1.3.6.1.4.1.15497.1.2.3.2.8.0	캐시클라이언트총연결	총 클라이언트 연결 수
1.3.6.1.4.1.15497.1.2.3.3.8.0	캐시서버총연결	총 서버 연결 수

SNMP 문제 해결

SWA와 SNMP 관리자 간의 연결을 보려면 패킷을 캡처하는 것이 가장 좋습니다. 패킷 캡처 필터를 다음 위치에 둘 수 있습니다(포트 161 또는 포트 162).



참고: 이 필터는 기본 SNMP 포트로 인한 것입니다. 포트를 변경한 경우 구성된 포트 번호를 패킷 캡처 필터에 입력하십시오.

SWA에서 패킷을 캡처하는 단계:

1단계. GUI에 로그인

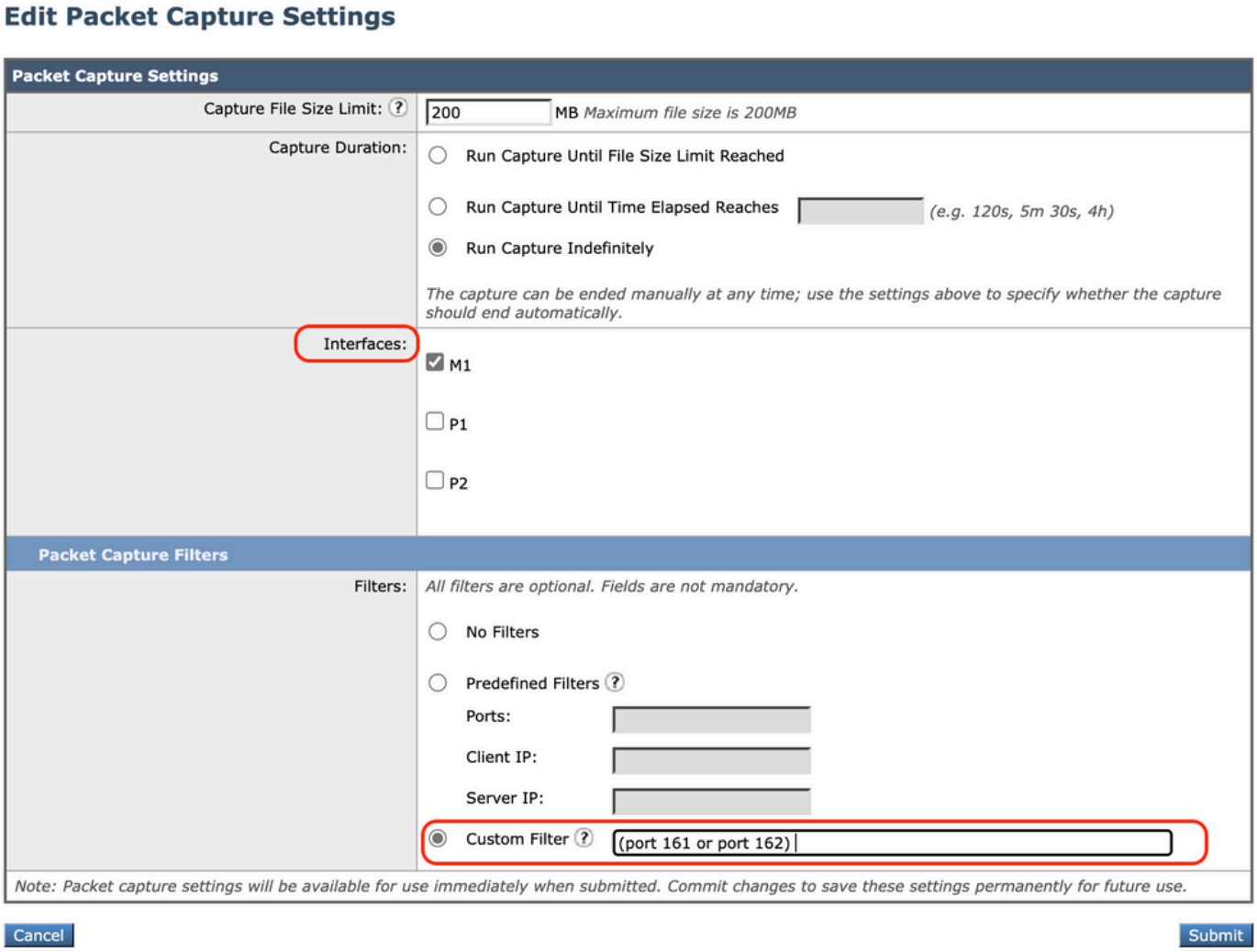
2단계. 오른쪽 상단에서 Support and Help(지원 및 도움말)를 선택합니다.

3단계. Packet Capture를 선택합니다

4단계. 설정 편집을 선택합니다

5단계. 올바른 인터페이스가 선택되었는지 확인합니다.

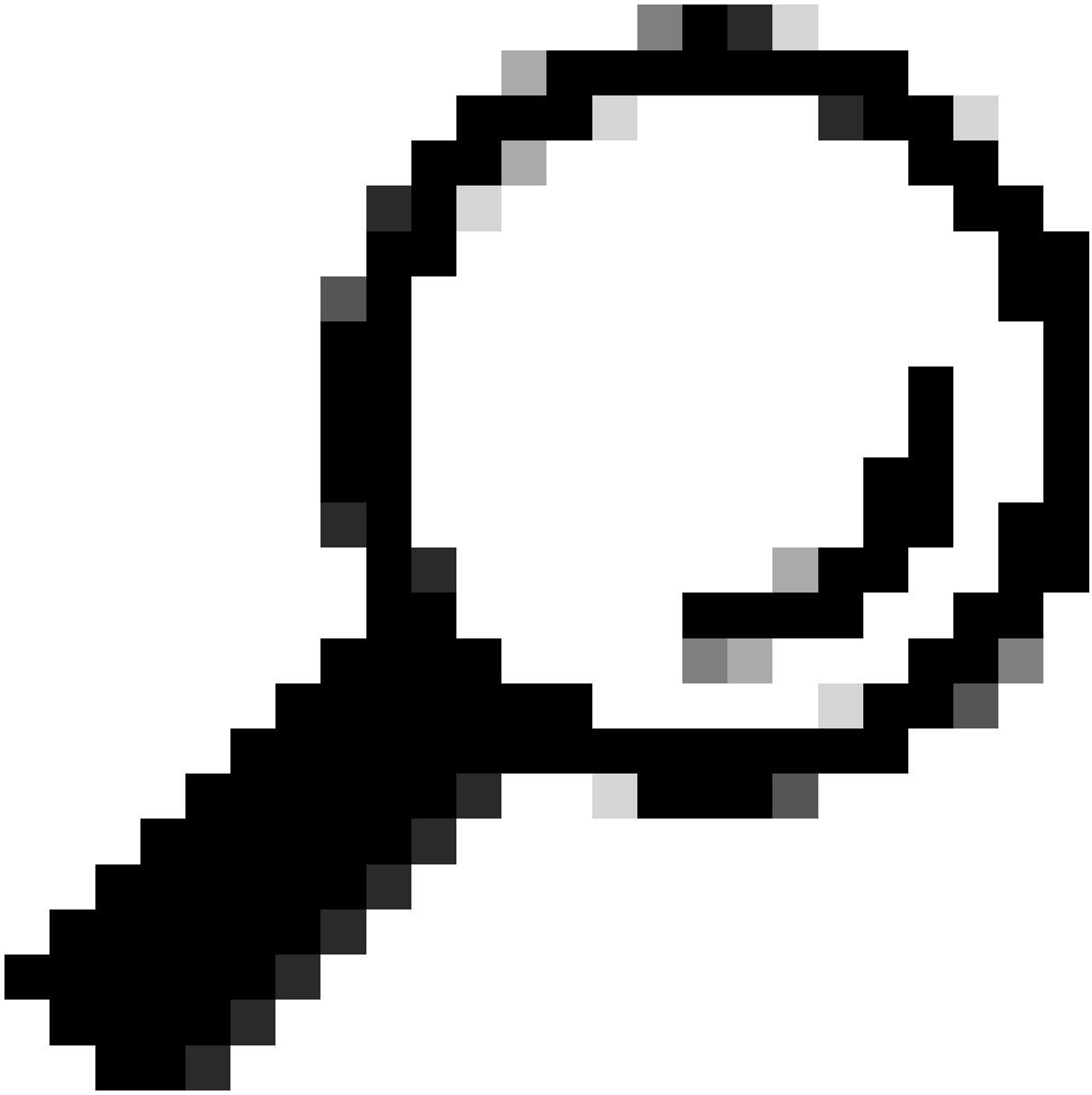
6단계. 필터 조건을 입력합니다.



이미지 - 패킷 캡처 필터 구성

7단계. 제출을 선택합니다

8단계. Start Capture를 선택합니다.



팁: Wireshark를 사용하여 SNMPv3 패킷 캡처를 해독할 수 있습니다. 자세한 내용은 다음 링크를 참조하십시오. How-to-decrypt-snmpv3-packets-using-wireshark

좁은 통로

snmpwalk는 여러 GET-NEXT 요청을 자동으로 실행하는 SNMP 애플리케이션에 지정된 이름입니다. SNMP GET-NEXT 요청은 활성화된 디바이스를 쿼리하고 디바이스에서 SNMP 데이터를 가져오는 데 사용됩니다. snmpwalk 명령을 사용하면 하위 트리 내의 모든 OID 또는 노드에 대해 고유한 명령을 입력할 필요 없이 GET-NEXT 요청을 함께 연결할 수 있으므로 이 명령이 사용됩니다

Windows 운영 체제에 SNMPWALK 설치

Microsoft Windows 사용자의 경우 먼저 도구를 다운로드해야 합니다.

Linux 커널에 SNMPWALK 설치

```
#For Redhat, Fedora, CentOs:
yum install net-snmp-utils

#For Ubuntu:
apt-get install snmp
```

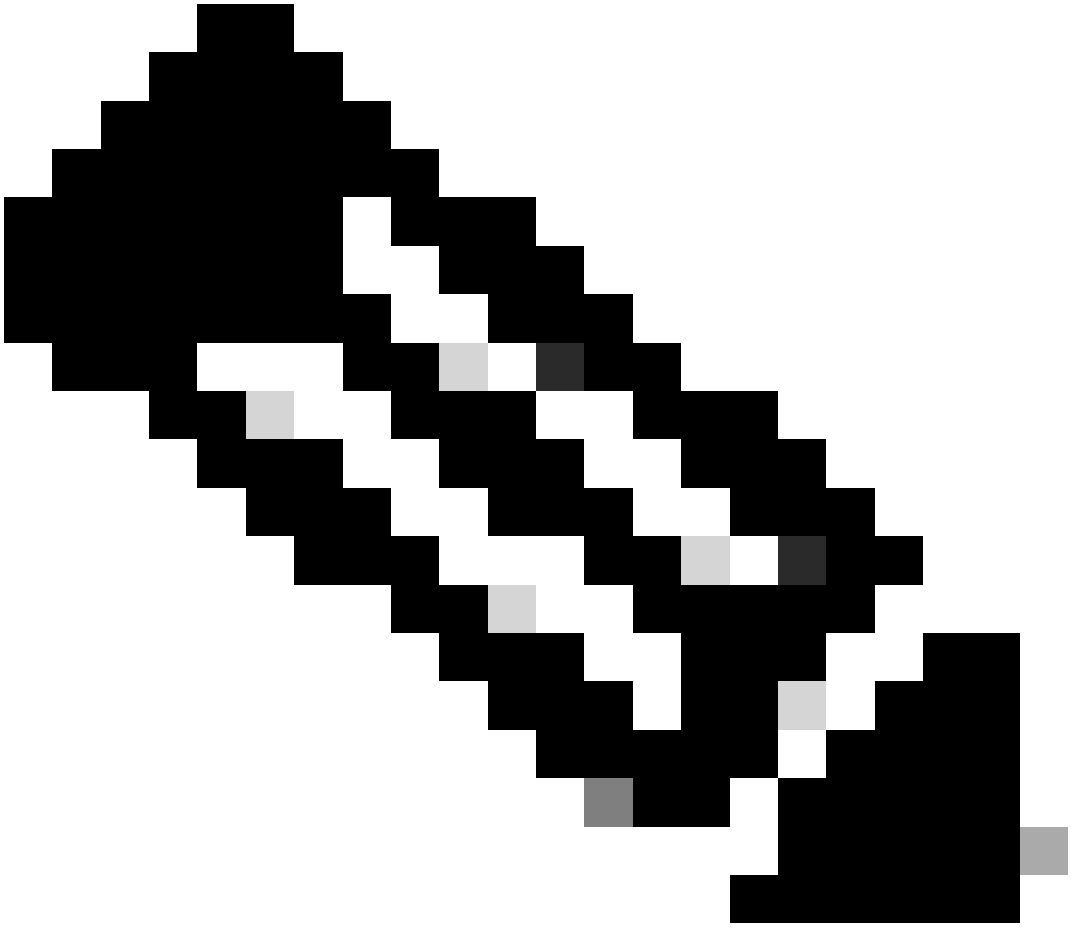
MacOS에 SNMPWALK 설치

기본적으로 snmpwalk는 MacOS에 설치됩니다

SNMP GET 요청을 생성하려면 SWA에 연결된 네트워크의 다른 컴퓨터에서 snmpwalk 명령을 사용할 수 있습니다. 다음은 snmpwalk 명령의 몇 가지 예입니다.

```
snmpwalk -v2c -c <Community Name>  <SWA IP Address>

snmpwalk -v3 -l authPriv  -u v3get  -a SHA -A <Password>  -x AES -X <Password>  <SWA IP Address>
```



참고: 보안 수준을 noAuthNoPriv 또는 authNoPriv 또는 authPriv로 설정은 SWA 구성에 따라 선택할 수 있습니다.

SNMPTRAP

snmptrap은 SWA에서 SNMP를 활성화해야 하는 숨겨진 CLI 명령입니다. 객체를 선택하고 트랩을 선택하여 SNMP 트랩을 생성할 수 있습니다. 예를 들면 다음과 같습니다.

```
SWA_CLI>nmptrap

1. CPUUtilizationExceeded
2. FIPSModeDisableFailure
3. FIPSModeEnableFailure
4. FailoverHealthy
5. FailoverUnhealthy
6. connectivityFailure
7. keyExpiration
8. linkUpDown
```

```
9. memoryUtilizationExceeded
10. updateFailure
11. upstreamProxyFailure
Enter the number of the trap you would like to send.
[]> 8

1. CPUUtilization
2. FIPSApplicationName
3. FailoverApplicationName
4. RAIDEvents
5. RAIDID
6. connectionURL
7. ifIndex
8. ip
9. keyDescription
10. memoryUtilization
11. raidStatus
12. updateServiceName
Enter the number of the object you would like to send.
[]> 8

Enter the trap value.
[]> 10.20.3.15

Enter the user name
[admin]> SNMPuser

Please select Trap Protocol version:
1. 2c
2. 3
[1]> 2
```

SWA의 SNMP 로그

SWA에는 SNMP와 관련된 두 개의 로그가 있습니다. 웹 프록시 구성 요소와 관련된 일부 로그 유형은 활성화되지 않습니다. 다음 위치에서 활성화할 수 있습니다.

- GUI에서 시스템 관리 > 로그 서브스크립션
- CLI에서: logconfig > new

로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
SNMP 로그	SNMP 네트워크 관리 엔진과 관련된 디버그 메시지를 기록합니다.	예	예
SNMP 모듈 로그	SNMP 모니터링 시스템과의 상호 작용과 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요

SNMP의 일반적인 문제

일부 OIDS가 실패함(값 없음 또는 잘못된 값).

이 문제는 SNMP 풀과 관련이 있습니다. 다음은 예상된 출력과 오류가 있는 출력의 두 가지 샘플입니다.

```
Sample Output without Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx prox
iso.3.6.1.4.1.15497.1.1.1.9.1.1.1 = INTEGER: 1
iso.3.6.1.4.1.15497.1.1.1.9.1.2.1 = INTEGER: 22
iso.3.6.1.4.1.15497.1.1.1.9.1.3.1 = STRING: "Ambient"

Sample Output with Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx prox
iso.3.6.1.4.1.15497.1.1.1.9 = No Such Instance currently exists at this OID
```

snmp_logs에서 "Application Faults"를 확인할 수 있습니다.

CLI에서 snmp_logs를 확인 > grep > snmp_logs와 관련 된 번호를 선택 할 수 있습니다.

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
37. "snmp_logs" Type: "SNMP Logs" Retrieval: FTP Poll
...
Enter the number of the log you wish to grep.
[]> 37

Enter the regular expression to grep.
[]>

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]> y

Do you want to paginate the output? [N]>
```

참조

AsyncOS 15.0 for Cisco Secure Web Appliance - LD 사용 설명서(제한적 배포) - 문제 해결 [Cisco Secure Web Appliance] - Cisco

SNMP를 사용하여 WSA에서 프록시 CPU 사용률 계산 - Cisco

snmpcmd(1)(freebsd)

snmptrap(freebsd)

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.