SNMP 및 LINA MIB

이 장에서는 ASA를 모니터링하기 위한 SNMP(Simple Network Management Protocol) 구성 방법을 설명합니다.

SNMP 정보

SNMP는 네트워크 디바이스 간의 관리 정보 교환을 촉진하기 위한 애플리케이션 계층 프로토콜이며 TCP/IP 프로토콜 군의 일부입니다. ASA는 SNMP 버전 1, 2c 및 3을 사용하여 네트워크 모니터링을 지원하고 모든 3개 버전의 동시 사용도 지원합니다. ASA 인터페이스에서 실행되는 SNMP 에이전트를 사용하면 HP OpenView와 같은 NMS(네트워크 관리 시스템)을 통해 네트워크 디바이스를 모니터링할 수 있습니다. ASA는 GET 요청 발행을 통해 SNMP 읽기 전용 액세스를 지원합니다. SNMP 쓰기 액세스는 허용되지 않으므로 SNMP를 사용하여 변경할 수는 없습니다. 또한 SNMP SET 요청은 지원되지 않습니다.

ASA를 NMS로의 특정 이벤트(알림 포함)에 대해 관리 디바이스에서 관리 스테이션으로 전송되는 요청하지 않은 메시지인 트랩을 보내도록 구성하거나 NMS를 사용하여 보안 디바이스에서 MIB(관리 정보 기반)를 찾아볼 수 있습니다. MIB는 정의 모음이고 ASA은 각 정의에 대한 값 데이터베이스를 유지합니다. MIB를 찾아보는 것은 NMS에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 발행하는 것을 의미합니다.

참고 워크로드가 과중한 경우 10개 이상의 NMS를 구축하면 디바이스의 성능에 영향을 미칠 수 있습니다. 디바이스의 안정성과 응답성을 보장하기 위해 SNMP 워크 폴링을 수행하고 트랩 트래픽을 관리할 때 NMS를 신중하게 활용하는 것이 좋습니다.

ASA에는 예를 들어 네트워크 링크가 실행 또는 중단 상태로 전환될 때 알림이 필요하도록 사전 정의된 이벤트가 발생하는 경우 지정된 관리 스테이션에 알려주는 SNMP 에이전트가 있습니다. 이때 보내는 알림은 관리 스테이션에 스스로를 식별하는 SNMP OID를 포함합니다. ASA 에이전트는 관리 스테이션이 정보를 요구할 때 응답하기도 합니다.

SNMP 용어

다음 표는 SNMP에서 작업할 때 일반적으로 사용되는 용어를 나열합니다.

표 *1: SNMP* 용어

용어	설명
에이전트	ASA에서 실행되는 SNMP 서버입니다. SNMP 에이전트는 다음과 같은 특징을 갖습니다. • 정보 요청 및 네트워크 관리 스테이션의 작업에 대해 응답합니다. • SNMP 관리자가 보거나 변경할 수 있는 객체 모음인 MIB(관리 정보 기반)에 대한 액세스를 제어합니다. • SET 작업을 허용하지 않습니다.
찾아보기	디바이스의 SNMP 에이전트에서 필요한 정보를 폴링함으로써 네트워크 관리 스테이션에서 해당 디바이스의 상태를 모니터링합니다. 이 작업은 값을 결정하기 위해 네트워크 관리 스테이션에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 생성하는 것을 포함할 수 있습니다.
MIB(관리 정보 기반)	패킷, 연결, 버퍼, 장애 조치 등에 관한 정보를 수집하기 위한 표준화된 데이터 구조입니다. MIB는 대부분의 네트워크 디바이스에서 사용되는 제품, 프로토콜 및 하드웨어 표준으로 정의됩니다. SNMP 네트워크 관리 스테이션은 MIB를 찾아보고 특정 데이터나 이벤트 전송을 실시간으로 요청할 수 있습니다.
NMS(네트워크 관리 스테이션)	SNMP 이벤트를 모니터링하고 ASA 등의 디바이스를 관리하도록 설정된 PC나 워크스테이션입니다.
OID(객체 식별자)	NMS에서 디바이스를 식별하고 사용자에게 모니터링 및 표시되는 정보의 소스를 보여주는 시스템입니다.
트랩	SNMP 에이전트에서 NMS로 메시지를 생성하는 사전 정의된 이벤트입니다. 이벤트는 linkup, linkdown, coldstart, warmstart, authentication 또는 syslog 메시지와 같은 경보 조건을 포함합니다.

MIB 및 트랩

MIB는 표준이거나 기업별로 구분됩니다. 표준 MIB는 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. 트랩은 네트워크 디바이스에서 발생하는 중요 이벤트(대부분 오류나 장애)를 보고합니다. SNMP 트랩은 표준 또는 기업별 MIB로 정의됩니다. 표준 트랩은 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. SNMP 트랩은 ASA 소프트웨어로 컴파일됩니다.

필요한 경우 다음 위치에서 RFC, 표준 MIB 및 표준 트랩을 다운로드할 수 있습니다.

http://www.ietf.org/

다음 위치에서 Cisco MIB, 트랩 및 OID의 전체 목록을 검색하십시오.

https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html

또한 다음 위치에서 FTP를 통해 Cisco OID를 다운로드할 수 있습니다.

https://github.com/cisco/cisco-mibs/tree/main/oid

참고 소프트웨어 7.2(1), 8.0(2) 이후 버전에서는 SNMP를 통해 액세스하는 인터페이스 정보를 약 5초마다 새로 고칩니다. 따라서 연속 폴링 사이에 적어도 5초를 기다리는 것이 좋습니다.

MIB에 있는 모든 OID가 지원되지는 않습니다. 특정 ASA에 대해 지원되는 SNMP MIB 및 OID 목록을 얻으려면 다음 명령을 입력합니다.

```
ciscoasa(config)# show snmp-server oidlist
```

참고 **oidlist** 키워드는 **show snmp-server** 명령 도움말에 대한 옵션 목록에 나타나지 않더라도 사용할 수 있습니다. 그러나 이 명령은 Cisco TAC 전용입니다. 이 명령을 사용하기 전에 Cisco TAC에 문의하십시오.

다음은 **show snmp-server oidlist** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
```

```
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

SNMP Object Identifier

모든 Cisco 시스템 레벨 제품에는 MIB II sysObjectID로 사용하기 위한 SNMP OID(object identifier)가 있습니다. CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB는 SNMPv2-MIB, Entity Sensor MIB 및 Entity Sensor Threshold Ext MIB에서 sysObjectID 개체로 보고될 수 있는 OID를 포함합니다. 이 값을 사용하여 모델 유형을 식별할 수 있습니다. 다음 표에는 ASA 및 ISA 모델의 sysObjectID OID가 나와 있습니다.

표 *2: SNMP Object Identifier*

제품 **ID**	**sysObjectID**	모델 번호
ASA 가상	ciscoASAv(ciscoProducts 1902)	Cisco Adaptive Security Virtual Appliance(ASA 가상)
ASA 가상 시스템 상황	ciscoASAvsy(ciscoProducts 1903)	Cisco Adaptive Security Virtual Appliance(ASA 가상) 시스템 상황
ASA 가상 보안 상황	ciscoASAvsc(ciscoProducts 1904)	Cisco Adaptive Security Virtual Appliance(ASA 가상) 보안 컨텍스트
Secure Firewall 4200	ciscoFpr4215td(ciscoProducts 3043) ciscoFpr4225td(ciscoProducts 3042) ciscoFpr4245td(ciscoProducts 3041)	FPR4215, FPR4225, FPR4245
ISA 30004C Industrial Security Appliance	ciscoProducts 2268	ciscoISA30004C
4GE Copper Security Context가 포함된 CISCO ISA30004C	ciscoProducts 2139	ciscoISA30004Csc
4GE Copper System Context가 포함된 CISCO ISA30004C	ciscoProducts 2140	ciscoISA30004Csy
ISA 30002C2F Industrial Security Appliance	ciscoProducts 2267	ciscoISA30002C2F
2GE 구리 포트 + 2GE Fiber Security Context가 포함된 CISCO ISA30002C2F	ciscoProducts 2142	ciscoISA30002C2Fsc
2GE 구리 포트 + 2GE Fiber System Context가 포함된 CISCO ISA30002C2F	ciscoProducts 2143	ciscoISA30002C2Fsy
Cisco Industrial Security Appliance(ISA) 30004C Chassis	cevChassis 1677	cevChassisISA30004C
Cisco Industrial Security Appliance(ISA) 30002C2F Chassis	cevChassis 1678	cevChassisISA30002C2F
ISA30004C Copper SKU용 중앙 처리 장치 온도 센서	cevSensor 187	cevSensorISA30004CCpuTempSensor
ISA30002C2F Fiber용 중앙 처리 장치 온도 센서	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
ISA30004C Copper SKU용 프로세서 카드 온도 센서	cevSensor 192	cevSensorISA30004CPTS
ISA30002C2F Fiber SKU용 프로세서 카드 온도 센서	cevSensor 193	cevSensorISA30002C2FPTS

제품 **ID**	**sysObjectID**	모델 번호
ISA30004C Copper SKU용 전력 카드 온도 센서	cevSensor 197	cevSensorISA30004CPowercardTS
ISA30002C2F Fiber SKU용 전력 카드 온도 센서	cevSensor 198	cevSensorISA30002C2FPowercardTS
ISA30004C용 포트 카드 온도 센서	cevSensor 199	cevSensorISA30004CPortcardTS
ISA30002C2F용 포트 카드 온도 센서	cevSensor 200	cevSensorISA30002C2FPortcardTS
ISA30004C Copper SKU용 중앙 처리 장치	cevModuleCpuType 329	cevCpuISA30004C
ISA30002C2F Fiber SKU용 중앙 처리 장치	cevModuleCpuType 330	cevCpuISA30002C2F
모듈 ISA30004C, ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C Industrial Security Appliance Solid State Drive	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
30002C2F Industrial Security Appliance Solid State Drive	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
Cisco ISA30004C/ISA30002C2F Hardware Bypass	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
FirePOWER 4140 Security Appliance, 포함된 보안 모듈 36이 있는 1U	ciscoFpr4140K9(ciscoProducts 2293)	FirePOWER 4140
FirePOWER 4120 Security Appliance, 포함된 보안 모듈 24가 있는 1U	ciscoFpr4120K9(ciscoProducts 2294)	FirePOWER 4120
FirePOWER 4K Fan Bay	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K Power Supply Bay	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Secure Firewall Threat Defense Virtual, VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
시스코 Threat Defense Virtual, AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

물리적 공급업체 유형 값

각 Cisco 섀시 또는 독립형 시스템은 SNMP 사용을 위한 고유한 유형의 숫자를 갖습니다. entPhysicalVendorType OID는 CISCO-ENTITY-VENDORTYPE-OID-MIB에 정의되어 있습니다. 이 값은 ASA, ASA 가상 또는 ASASM SNMP 에이전트의 entPhysicalVendorType 개체에서 반환됩니다. 이

값을 사용하여 구성 요소의 유형(모듈, 전원 공급 장치, 팬, 센서, CPU 등)을 식별할 수 있습니다. 다음 표는 ASA 모델에 대한 실제 공급업체 유형 값을 나열합니다.

표 ***3:*** 물리적 공급업체 유형 값

항목	**entPhysicalVendorType OID** 설명
기가비트 이더넷 포트	cevPortGe(cevPort 109)
Cisco Adaptive Security Virtual Appliance	cevChassisASAv(cevChassis 1451)
Secure Firewall 4200-X (FPR4215/FPR4225/FPR4245)	cevFPRNM4X200Gng 및 cevFPRNM2X100Gng(슬롯 2 및 슬롯 3에 추가된 듀얼 EPM 2X100G 및 4X200G용)

MIB에서 지원되는 테이블 및 개체

다음 표에서는 지정된 MIB에 대해 지원되는 테이블 및 개체를 소개합니다.

멀티 컨텍스트 모드에서 이러한 테이블과 개체는 단일 컨텍스트에 대한 정보를 제공합니다. 컨텍스트 전반에 걸친 데이터를 원하는 경우 합산해야 합니다. 예를 들어 전체 메모리 사용량을 가져오려면 각 컨텍스트에 대해 cempMemPoolHCUsed 값을 합산합니다.

표 ***4: MIB***에서 지원되는 테이블 및 개체

MIB 이름 및 **OID**	지원되는 테이블 및 개체
ENTITY-MIB; OID: 1.3.6.1.2.1.47	entPhysicalTable, entPhysicalDescr, entPhysicalVendorType, entPhysicalName
CISCO-ENHANCED-MEMPOOL-MIB; OID:1.3.6.1.4.1.9.9.221	cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate, cempMemPoolValid. 32비트 메모리 시스템의 경우 32비트 메모리 카운터(cempMemPoolUsed, cempMemPoolFree,cempMemPoolUsedOvrflw, cempMemPoolFreeOvrflw, cempMemPoolLargestFree, cempMemPoolLowestFree, cempMemPoolUsedLowWaterMark, cempMemPoolAllocHit, cempMemPoolAllocMiss, cempMemPoolFreeHit, cempMemPoolFreeMiss, cempMemPoolLargestFreeOvrflw, cempMemPoolLowestFreeOvrflw, cempMemPoolUsedLowWaterMarkOvrflw, cempMemPoolSharedOvrflw)를 사용하여 폴링합니다. 64비트 메모리 시스템의 경우 64비트 메모리 카운터 (cempMemPoolHCUsed, cempMemPoolHCFree, cempMemPoolHCLargestFree, cempMemPoolHCLowestFree, cempMemPoolHCUsedLowWaterMark, cempMemPoolHCShared)를 사용하여 폴링합니다.

MIB 이름 및 **OID**	지원되는 테이블 및 개체
CISCO-REMOTE-ACCESS-MONITOR-MIB; OID:1.3.6.1.4.1.9.9.392 참고 이 3개의 MIB OID는 원격 액세스 연결이 실패하는 이유를 추적하는 데 사용할 수 있습니다.	crasNumTotalFailures, crasNumSetupFailInsufResources, crasNumAbortedSessions
CISCO-ENTITY-SENSOR-EXT-MIB; OID:1.3.6.1.4.1.9.9.745	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB; OID:1.3.6.1.4.1.9.9.480	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB; OID:1.3.6.1.4.1.9.9.720 참고 ASA 가상에서 지원되지 않음.	ctsxSxpGlobalObjects, ctsxSxpConnectionObjects, ctsxSxpSgtObjects
DISMAN-EVENT-MIB; OID:1.3.6.1.2.1.88	mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable
DISMAN-EXPRESSION-MIB; OID:1.3.6.1.2.1.90	expExpressionTable, expObjectTable, expValueTable
ENTITY-SENSOR-MIB; OID: 1.3.6.1.2.1.99 참고 섀시 온도, 팬 RPM, 전원 공급 장치 전압 등과 같은 물리적 센서와 관련된 정보를 제공합니다. ASA 가상 플랫폼에서는 지원되지 않습니다.	entPhySensorTable
NAT-MIB; OID:1.3.6.1.2.1.123	natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom, natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol, natAddrMapAddrUsed, natAddrMapRowStatus
CISCO-PTP-MIB; OID:1.3.6.1.4.1.9.9.760 참고 E2E 투명 클록 모드에 해당하는 MIB만 지원됩니다.	ciscoPtpMIBSystemInfo, cPtpClockDefaultDSTable, cPtpClockTransDefaultDSTable, cPtpClockPortTransDSTable

MIB 이름 및 **OID**	지원되는 테이블 및 개체
CISCO-PROCESS-MIB; 1.3.6.1.4.1.9.9.109.1.1.1.1.7.1 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	cpmCPUTotal1minRev 연결된 매개변수 및 cpmCPUTotal1minRev 값 예: • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) - 시스템 CPU 사용률 집계 %(이 값은 단일 컨텍스트 모드에서 .3.6.1.4.1.9.9.109.1.1.1.7.1의 시스템 CPU 사용률과 동일합니다.). • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) - Snort 평균 CPU 사용률 %(모든 Snort 인스턴스의 총 집계) • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) - 시스템 프로세스 평균 %("Sysproc" 코어의 평균)

지원되는 트랩(알림)

다음 표에서는 지원되는 트랩(알림) 및 해당 MIB를 소개합니다.

표 ***5:*** 지원되는 트랩*(*알림*)*

트랩 및 **MIB** 이름	**Varbind** 목록	설명
authenticationFailure (SNMPv2-MIB)	—	SNMP 버전 1 또는 2의 경우 SNMP 요청에서 제공된 커뮤니티 문자열이 바르지 않습니다. SNMP Version 3의 경우 auth 또는 priv 비밀번호나 사용자 이름이 바르지 않은 경우 트랩 대신 보고서 PDU가 생성됩니다. **snmp-server enable traps snmp authentication** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
bgpBackwardTransition	bgpPeerLastError, bgpPeerState	**snmp-server enable traps peer-flap** 명령은 BGP 피어 플랩 관련 트랩 전송을 활성화하는 데 사용됩니다.
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	ccmHistoryRunningLastChanged, ccmHistoryEventTerminalType	**snmp-server enable traps config** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-insert** 명령은 이 알림을 활성화하는 데 사용됩니다.
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-remove** 명령은 이 알림을 활성화하는 데 사용됩니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)	entPhysicalName, entPhysicalDescr, entPhySensorValue, entPhySensorType, ceSensorExtThresholdValue	**snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] 명령은 엔티티 임계값 알림 전송을 활성화하는 데 사용됩니다. 이 알림은 전원 공급 장치 장애에 대해 전송됩니다. 전송된 객체는 팬과 CPU 온도를 파악합니다. **snmp-server enable traps entity fan-failure** 명령은 팬 장애 트랩 전송을 활성화하는 데 사용됩니다.이 트랩은 Firepower 2100 Series에 적용되지 않습니다. **snmp-server enable traps entity power-supply-failure** 명령은 전원 공급 장치 장애 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity chassis-fan-failure** 명령은 섀시 팬 장애 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity cpu-temperature** 명령은 CPU 고온 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity power-supply-presence** 명령은 전원 공급 장치 감지 장애 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity power-supply-temperature** 명령은 전원 공급 장치 온도 임계값 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity chassis-temperature** 명령은 섀시 주변 온도 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity accelerator-temperature** 명령은 섀시 가속기 온도 트랩 전송을 활성화하는 데 사용됩니다.
cikeTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunLifeTime	**snmp-server enable traps ikev2 start** 명령은 ikev2 시작 트랩 전송을 활성화하는 데 사용됩니다.
cikeTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunActiveTime	**snmp-server enable traps ikev2 stop** 명령은 ikev2 스톱 트랩 전송을 활성화하는 데 사용됩니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	**snmp-server enable traps ipsec start** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	ccmHistoryEventCommandSource, ccmHistoryEventConfigSource, ccmHistoryEventConfigDestination	**snmp-server enable traps config** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions, crasNumUsers, crasMaxSessionsSupportable, crasMaxUsersSupportable, crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
ciscoUFwFailoverStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	gid, FOStatus	**snmp-server enable traps failover-state** 명령은 장애 조치 상태 트랩 전송을 활성화하는 데 사용됩니다.
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp	Syslog 메시지가 생성됩니다. clogMaxSeverity 객체의 값은 어떤 syslog 메시지가 트랩으로 전송되는지 결정하는 데 사용됩니다. **snmp-server enable traps syslog** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType, crlResourceLimitMax, clogOriginIDType, clogOriginID	**snmp-server enable traps connection-limit-reached** 명령은 connection-limit-reached 알림 전송을 활성화하는 데 사용됩니다. clogOriginID 객체는 트랩이 시작하는 상황 이름을 포함합니다.
coldStart (SNMPv2-MIB)	—	SNMP 구성 후 SNMP 에이전트가 시작할 때 발생하는 coldStart 트랩 입니다. 이 트랩은 시스템 재부팅 후 에이전트가 시작할 때도 발생합니다. 참고 클러스터 및 HA 노드의 경우 다시 로드를 게시하고 인터페이스 재부팅 시간이 5분(미리 설정된 임계값)을 초과하면 트랩이 삭제됩니다. 클러스터 와 HA 노드가 정상적으로 재부팅되면 다른 모든 트랩은 정상적으로 전송됩니다. **snmp-server enable traps snmp coldstart** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** 명령은 CPU 임계값 상승 알림 전송을 활성화하는 데 사용됩니다. cpmCPURisingThresholdPeriod 객체가 다른 객체와 함께 전송됩니다.
cufwClusterStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	status	**snmp-server enable traps cluster-state** 명령은 클러스터 상태 트랩 전송을 활성화하는 데 사용됩니다.
entConfigChange (ENTITY-MIB)	—	**snmp-server enable traps entity config-change fru-insert fru-remove** 명령은 이 알림을 활성화하는 데 사용됩니다. 참고 이 알림은 보안 컨텍스트가 생성되거나 삭제될 때 멀티 모드로만 전송됩니다.
linkDown (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	인터페이스에 대한 linkdown 트랩. **snmp-server enable traps snmp linkdown** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
linkUp (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	인터페이스에 대한 linkup 트랩. **snmp-server enable traps snmp linkup** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** 명령은 메모리 임계값 알림을 활성화하는 데 사용됩니다. mteHotOID는 cempMemPoolHCUsed로 설정됩니다. cempMemPoolName 및 cempMemPoolHCUsed 객체는 다른 객체와 함께 전송됩니다.
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName	**snmp-server enable traps interface-threshold** 명령은 인터페이스 임계값 알림을 활성화하는 데 사용됩니다. entPhysicalName 객체는 다른 객체와 함께 전송됩니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
natPacketDiscard (NAT-MIB)	ifIndex	**snmp-server enable traps nat packet-discard** 명령은 NAT 패킷 폐기 알림을 활성화하는 데 사용됩니다. 이 알림은 5분으로 속도가 제한되어 있으며 매핑 공간이 제공되지 않으므로 NAT가 IP 패킷을 버릴 때 생성됩니다. ifIndex는 매핑된 인터페이스의 ID를 제공합니다.
ospfNbrStateChange	ospfRouterId, ospfNbrIpAddr, ospfNbrAddressLessIndex, ospfNbrRtrId, ospfNbrState	**snmp-server enable traps peer-flap** 명령은 OSPF 피어 플랩 관련 트랩 전송을 활성화하는 데 사용됩니다.
warmStart (SNMPv2-MIB)	—	SNMP 에이전트를 처음으로 재시작할 때 발생하는 warmStart 트랩 입니다. 이 트랩은 모든 SNMP 호스트 설정이 제거되고 새 SNMP 설정이 수행되는 SNMP 구성 변경 후 에이전트가 다시 시작되는 경우에도 발생합니다. **snmp-server enable traps snmp warmstart** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.

인터페이스 유형 및 예

SNMP 트래픽 통계를 생산하는 인터페이스 유형은 다음을 포함합니다.

- 논리—소프트웨어 드라이버가 수집한 통계로 물리적 통계의 하위 집합.
- 물리—하드웨어 드라이버가 수집한 통계. 각 물리적 이름 지정 인터페이스에는 논리적 통계와 물리적 통계 집합이 연결되어 있습니다. 각 물리적 인터페이스에는 연결된 VLAN 인터페이스가 두 개 이상 있습니다. VLAN 인터페이스에는 논리적 통계만 있습니다.

참고 여러 VLAN 인터페이스가 연결된 물리적 인터페이스의 경우 ifInOctets 및 ifOutoctets OID에 대한 SNMP 카운터가 해당 물리적 인터페이스의 종합 트래픽 카운터와 일치하도록 주의하십시오.

- VLAN 전용—SNMP는 ifInOctets 및 ifOutOctets에 대해 논리적 통계를 사용합니다.

다음 표의 예에서는 SNMP 트래픽 통계의 차이점을 보여줍니다. 예 1은 **showinterface** 명령과 **show traffic** 명령에 대한 물리적 및 논리적 출력 통계의 차이를 보여 줍니다. 예 2는 **show interface** 명령과 **show traffic** 명령에 대한 VLAN 전용 인터페이스에 대한 출력 통계를 보여 줍니다. 예는 통계가 **show traffic** 명령에 대한 출력과 비슷함을 보여 줍니다.

표 *6:* 물리 및 ***VLAN*** 인터페이스에 대한 ***SNMP*** 트래픽 통계

예 **1**	예 **2**
ciscoasa# **show interface GigabitEthernet3/2** interface GigabitEthernet3/2 description fullt-mgmt nameif mgmt security-level 10 ip address 10.7.14.201 255.255.255.0 management-only ciscoasa# **show traffic** (Condensed output) Physical Statistics GigabitEthernet3/2: received (in 121.760 secs) **36 packets 3428 bytes** 0 pkts/sec 28 bytes/sec Logical Statistics mgmt: received (in 117.780 secs) **36 packets 2780 bytes** 0 pkts/sec 23 bytes/sec 다음 예는 관리 인터페이스 및 물리 인터페이스에 대한 SNMP 출력 통계를 보여줍니다. ifInOctets 값은 **show traffic** 명령 출력에 나타나는 물리적 통계와 비슷하지만 논리적 통계 출력과는 다릅니다. ifIndex of the mgmt interface: IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface 물리적 인터페이스 통계에 대응하는 ifInOctets: **IF-MIB::ifInOctets.6 = Counter32:3246**	ciscoasa# **show interface GigabitEthernet0/0** interface GigabitEthernet0/0.100 vlan 100 nameif inside security-level 100 ip address 10.7.1.101 255.255.255.0 standby ciscoasa# **show traffic** inside received (in 9921.450 secs) **1977 packets 126528 bytes** 0 pkts/sec 12 bytes/sec transmitted (in 9921.450 secs) **1978 packets 126556 bytes** 0 pkts/sec 12 bytes/sec ifIndex of VLAN inside: IF-MIB::ifDescr.9 = Adaptive Security Appli **IF-MIB::ifInOctets.9 = Counter32: 126318**

SNMP Version 3 개요

SNMP Version 3에서는 SNMP Version 1 또는 Version 2c에 없는 향상된 보안을 제공합니다. SNMP 버전 1 및 2c는 일반 텍스트로 SNMP 서버와 SNMP 에이전트 간에 데이터를 전송합니다. SNMP 버전 3은 프로토콜 작동을 보호하기 위한 인증 및 프라이버시 옵션을 추가합니다. 또한 이 버전은 USM(사용자 기반 보안 모델) 및 VACM(보기 기반 제어 모델)을 통해 SNMP 에이전트와 MIB 객체에 대한 액세스를 제어합니다. 또한 ASA는 SNMP 그룹 및 사용자는 물론 호스트 생성을 지원하며 이는 안전한 SNMP 통신을 위한 전송 인증 및 암호화 활성화를 위해 필요합니다.

보안 모델

구성을 위해 인증 및 프라이버시 옵션은 보안 모델로 그룹화됩니다. 보안 모델은 사용자와 그룹에 적용되며 다음 3개 유형으로 나누어집니다.

- NoAuthPriv—No Authentication and No Privacy(인증 없음 및 개인정보 보호 없음)로 메시지에 보안이 적용되지 않음을 의미합니다.
- AuthNoPriv—Authentication but No Privacy(인증 있음 및 개인정보 보호 없음)로 메시지가 인증을 받음을 의미합니다.
- AuthPriv—Authentication and Privacy(인증 있음 및 개인정보 보호 있음)로 메시지가 인증을 받고 암호화됨을 의미합니다.

SNMP 그룹

SNMP 그룹은 사용자를 추가할 수 있는 액세스 제어 정책입니다. 각 SNMP 그룹은 보안 모델로 구성되며 SNMP 보기와 연결됩니다. SNMP 그룹 내의 사용자는 SNMP 그룹의 보안 모델과 일치해야 합니다. 이러한 파라미터는 SNMP 그룹 내 사용자가 이용하는 인증 및 프라이버시 유형을 지정합니다. 각 SNMP 그룹 이름 및 보안 모델 쌍은 고유해야 합니다.

SNMP 사용자

SNMP 사용자는 지정된 사용자 이름, 사용자가 속하는 그룹, 인증 비밀번호, 암호화 비밀번호 및 승인, 그리고 사용할 암호화 알고리즘을 가져야 합니다. 인증 알고리즘 옵션은 SHA-1, SHA-224, SHA-256 HMAC 및 SHA-384입니다. 암호화 알고리즘 옵션은 3DES 및 AES(128, 192, 256 버전으로 제공)입니다. 사용자를 생성할 때 반드시 SNMP 그룹과 연결해야 합니다. 그러면 사용자에게 그룹의 보안 모델이 상속됩니다.

참고 SNMP v3 사용자 계정을 구성할 때는 인증 알고리즘의 길이가 암호화 알고리즘의 길이와 같거나 더 길어야 합니다.

SNMP 호스트

SNMP 호스트는 SNMP 알림 및 트랩이 전송되는 IP 주소입니다. 트랩은 구성된 사용자에게만 전송되기 때문에 SNMP 버전 3 호스트를 대상 IP 주소와 함께 구성하려면 사용자 이름을 구성해야 합니다. SNMP 대상 IP 주소 및 대상 파라미터 이름은 ASA에서 고유해야 합니다. 각 SNMP 호스트는 연결된 하나의 사용자 이름만 가질 수 있습니다. SNMP 트랩을 수신하려면, **snmp-server host** 명령을 추가한 후, SNMP NMS를 구성하고, NMS의 사용자 자격 증명을 ASA에 대한 자격 증명과 일치하도록 구성해야 합니다.

참고 최대 8192개의 호스트를 추가할 수 있습니다. 하지만 이 중 128개만 트랩에 사용할 수 있습니다.

ASA와 Cisco IOS 소프트웨어의 구현 차이점

ASA의 SNMP 버전 3 구현은 Cisco IOS 소프트웨어에서의 SNMP 버전 3 구현과 다음과 같은 차이가 있습니다.

- 로컬 엔진 및 원격 엔진 ID를 구성할 수 없습니다. 로컬 엔진 ID는 ASA가 시작되거나 컨텍스트가 생성될 때 생성됩니다.
- 무제한 MIB 찾아보기를 야기하는 보기 기반 액세스 제어는 지원되지 않습니다.
- 지원은 다음 MIB로 제한됩니다. USM, VACM, FRAMEWORK 및 TARGET.
- 정확한 보안 모델로 사용자 및 그룹을 생성해야 합니다.
- 사용자, 그룹 및 호스트를 올바른 순서로 제거해야 합니다.
- snmp-server host 명령을 사용하면 들어오는 SNMP 트래픽을 허용하는 ASA 규칙이 생성됩니다.

SNMP Syslog 메시징

SNMP는 212*nnn* 형식으로 번호가 매겨지는 상세한 syslog 메시지를 생성합니다. Syslog 메시지는 ASA 또는 ASASM에서 특정 인터페이스의 지정된 호스트로 SNMP 요청, SNMP 트랩, SNMP 채널 및 SNMP 응답의 상태를 알려 줍니다.

syslog 메시지에 대한 자세한 설명은 syslog 메시지 가이드를 참고하십시오.

참고 SNMP syslog 메시지가 높은 속도(초당 약 4000)를 초과하면 SNMP 폴링이 실패합니다.

애플리케이션 서비스 및 서드파티 툴

SNMP 지원에 대한 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP Version 3 MIB를 위한 서드파티 툴 사용에 대한 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP를 위한 지침

이 섹션에는 SNMP를 구성하기 전에 검토해야 할 지침 및 제한사항이 포함되어 있습니다.

장애 조치 및 클러스터링 가이드라인

- 클러스터링 또는 장애 조치와 함께 SNMPv3를 사용하는 경우, 초기 클러스터 구성 후 새 클러스터 디바이스를 추가하거나 장애 조치 장치를 교체하는 경우 SNMPv3 사용자는 새 디바이스에 복제되지 않습니다. 사용자가 새 디바이스에 강제로 복제되도록 하려면 SNMPv3 사용자를 제어/

활성 디바이스에 다시 추가하거나 새 디바이스에 직접 사용자를 추가해야 합니다(SNMPv3 사용자 및 그룹은 클러스터 데이터 디바이스에 구성 명령을 입력할 수 없다는 규칙의 예외입니다). **snmp-server user** *username group-name* **v3** 명령을 제어/활성 유닛 또는 암호화되지 않은 형태의 *priv-password* 옵션 및 *auth-password* 옵션과 함께 데이타/스탠바이 유닛에 직접 입력하여 각 사용자를 다시 구성합니다.

IPv6 가이드라인(모든 ASA 모델)

IPv6 호스트가 IPv6 소프트웨어를 실행하는 디바이스에서 SNMP 쿼리를 수행하고 SNMP 알림을 수신할 수 있도록 IPv6 전송을 통해 SNMP를 구성할 수 있습니다. SNMP 에이전트 및 관련된 MIB는 IPv6 주소 지정을 지원하도록 기능이 향상되었습니다.

추가 지침

- 어플라이언스 모드에서 작동하는 시스템에 대해서는 전력 공급 장치 트랩이 실행되지 않습니다.
- Windows용 Cisco Works 또는 다른 SNMP MIB-II 규격 브라우저가 있어야 SNMP 트랩을 수신하거나 MIB를 찾아볼 수 있습니다.
- VPN 터널을 통한 관리 액세스는 SNMP(**management-access** 명령)에서 지원되지 않습니다. VPN을 통한 SNMP의 경우, 루프백 인터페이스에서 SNMP를 활성화하는 것이 좋습니다. 루프백 인터페이스에서 SNMP를 사용하기 위해 관리 액세스 기능을 활성화할 필요는 없습니다. 루프백은 SSH에 대해서도 작동합니다.
- 보기 기반 액세스 제어를 지원하지 않지만 VACM MIB를 이용한 찾아보기로 기본 보기 설정을 결정할 수 있습니다.
- ENTITY-MIB는 관리 이외 상황에서 이용할 수 없습니다. 관리 이외 상황에서는 IF-MIB를 대신 사용하십시오.
- ENTITY-MIB는 Firepower 9300에서 사용할 수 없습니다. 대신 CISCO-FIREPOWER-EQUIPMENT-MIB 및 CISCO-FIREPOWER-SM-MIB를 사용하십시오.
- 일부 디바이스에서 **snmpwalk** 출력의 인터페이스 순서(ifDescr)가 재부팅 후 변경되는 것으로 관찰되었습니다. ASA는 특정 알고리즘 을 사용하여 SNMP가 쿼리하는 ifIndex 테이블을 확인합니다. ASA가 부팅되면 ASA에서 구성을 읽을 때 로딩한 순서대로 ifIndex 테이블에 인터페이스가 추가됩니다. ASA에 추가된 새 인터페이스는 ifIndex 테이블의 인터페이스 목록에 추가됩니다. 인터페이스가 추가, 제거 또는 이름 변경될 때 재부팅 인터페이스의 순서에 영향을 줄 수 있습니다.
- **snmpwalk** 명령에서 OID를 제공하면 snmpwalk 도구는 지정된 OID 아래에 있는 하위 트리의 모든 변수를 쿼리하고 그 값을 표시합니다. 따라서 디바이스에서 개체의 포괄적인 출력을 보려면 **snmpwalk** 명령에 OID를 제공해야 합니다.
- AIP SSM 또는 AIP SSC를 위한 SNMP 버전 3을 지원하지 않습니다.
- SNMP 디버깅을 지원하지 않습니다.
- ARP 정보 검색을 지원하지 않습니다.
- SNMP SET 명령을 지원하지 않습니다.

- NET-SNMP 버전 5.4.2.1을 사용할 때는 AES128 버전의 암호화 알고리즘만 지원합니다. AES256 또는 AES192의 암호화 알고리즘 버전은 지원하지 않습니다.
- 기존 구성을 변경했을 때 SNMP 기능이 일관성을 잃게 되면 변경이 거부됩니다.
- SNMP 버전 3의 경우 그룹, 사용자, 호스트 순서로 구성이 이루어져야 합니다.
- Secure Firewall 모델의 경우, **snmpwalk** 명령은 관리자 상황에서만 FXOS mib를 폴링합니다.
- 그룹을 삭제하기 전에 해당 그룹에 연결된 모든 사용자가 삭제되었는지 확인해야 합니다.
- 사용자를 삭제하기 전에 해당 사용자 이름과 연결된 호스트가 구성되지 않았는지 확인해야 합니다.
- 사용자가 특정 보안 모델 내에서 특정 그룹에 속하도록 구성되어 있고 해당 그룹의 보안 수준이 변경되는 경우 다음을 순서대로 수행해야 합니다.
  - 해당 그룹에서 사용자를 제거합니다.
  - 그룹 보안 수준을 변경합니다.
  - 새 그룹에 속한 사용자를 추가합니다.
- MIB 객체 하위 집합에 대한 사용자 액세스를 제한하기 위한 맞춤 보기 생성은 지원되지 않습니다.
- 모든 요청 및 트랩은 기본 읽기/알림 보기에서만 이용 가능합니다.
- connection-limit-reached 트랩은 관리 상황에서 생성됩니다. 이 트랩을 생성하려면 연결 제한에 도달한 사용자 상황에서 SNMP 서버 호스트가 1개 이상 구성되어 있어야 합니다.
- NMS가 성공적으로 객체를 요청할 수 없거나 ASA로부터 수신 트랩을 제대로 처리할 수 없으면 패킷 캡처를 수행하는 것이 문제를 확인하는 유용한 방법입니다. **Wizards(**마법사**) > Packet Capture Wizard(**패킷 캡처 마법사**)**를 선택하고 화면상의 지침에 따릅니다.
- 최대 4000개의 호스트를 추가할 수 있습니다. 하지만 이 중 128개만 트랩에 사용할 수 있습니다.
- 지원되는 액티브 폴링 대상의 총수는 128개입니다.
- 호스트 그룹으로 추가할 개별 호스트를 나타내는 네트워크 객체를 지정할 수 있습니다.
- 둘 이상의 사용자를 하나의 호스트와 연결할 수 있습니다.
- 다른 **host-group** 명령에서 겹치는 네트워크 객체를 지정할 수 있습니다. 마지막 호스트 그룹에 대해 지정하는 값은 다른 네트워크 객체의 호스트 공통 집합에서 적용됩니다.
- 다른 호스트 그룹과 겹치는 호스트 그룹 또는 호스트를 삭제할 경우 호스트는 구성된 호스트 그룹에서 지정된 값으로 다시 설정됩니다.
- 호스트가 획득하는 값은 명령 실행에 사용하는 지정된 순서에 따라 다릅니다.
- SNMP가 보내는 메시지 크기의 한도는 1472바이트입니다.
- ASA에서 상황당 무제한 SNMP 서버 트랩 호스트를 지원합니다. **show snmp-server host** 명령 출력에는 정적으로 구성한 호스트와 함께 ASA를 폴링 중인 활성 호스트만 표시됩니다.

문제 해결 정보

- NMS로부터의 수신 패킷을 수신하는 SNMP 프로세스가 실행되도록 하려면 다음 명령을 입력하십시오.

```
ciscoasa(config)# show process | grep snmp
```

- SNMP에서 시스템 로그 메시지를 캡처하여 ASA 콘솔에 표시하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- SNMP 프로세스가 패킷을 송수신하도록 하려면 다음 명령을 입력하십시오.

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

  출력은 SNMPv2-MIB의 SNMP 그룹을 기준으로 합니다.

- SNMP 패킷이 ASA를 거쳐 SNMP 프로세스로 전달되는지 확인하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- NMS가 개체를 성공적으로 요청할 수 없거나 ASA에서 수신하는 트랩을 올바르게 처리하지 못하는 경우 패킷 캡처를 사용하여 다음 명령을 입력하여 문제를 격리합니다.

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- ASA가 예상대로 작동하지 않으면 다음을 수행하여 네트워크 토폴로지 및 트래픽에 대한 정보를 확보합니다.
  - NMS 구성의 경우 다음 정보를 확보합니다.

    시간 초과 횟수

    재시도 횟수

    엔진 ID 캐싱

    사용된 사용자 이름 및 비밀번호

  - 다음 명령을 수행:

    show block

    show interface

    show process

show cpu

show vm

- 치명적인 오류가 발생하는 경우 오류 재현에 도움이 되도록 역추적 파일과 **show tech-support** 명령 출력을 Cisco TAC로 보내십시오.
- SNMP 트래픽이 ASA 인터페이스를 통해 허용되지 않는 경우에는 **icmp permit** 명령을 사용하여 원격 SNMP 서버로부터의 ICMP 트래픽을 허용해야 할 수도 있습니다.
- **snmp-server enable oid**로 디바이스를 구성한 경우, SNMP 워크 작업을 수행할 때 ASA는 MEMPOOL_DMA 및 MEMPOOL_GLOBAL_SHARED 풀에서 메모리 정보를 쿼리합니다. 이로 인해 SNMP 관련 CPU 사용량이 많아져 패킷 삭제가 발생할 수 있습니다. 이 문제를 완화하려면 **snmp-server enable oid** 명령을 사용하여 전역 공유 풀과 관련된 OID를 폴링하지 마십시오. 비활성화된 경우 mempool OID는 0바이트를 반환합니다.
- 한 번의 폴링 요청에 많은 수의 OID가 포함된 SNMPGET을 사용하면 ASP 드롭 카운터 폴링을 반복적으로 수행해야 하므로 CPU 사용량이 증가합니다. 따라서 모니터링할 중요한 카운터를 식별하고 각 카운터에서 SNMPGET을 사용하여 CPU에 미치는 영향이 제한되도록 해당 값을 가져오는 것이 좋습니다.
- 추가적인 문제 해결 정보에 대해서는 다음 URL을 참조하십시오. http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

SNMP 구성

이 섹션에서는 SNMP 구성 방법을 설명합니다.

프로시저

단계 **1** SNMP 에이전트 및 SNMP 서버를 활성화합니다.
단계 **2** SNMP 관리 스테이션을 구성하여 ASA로부터 요청을 수신합니다.
단계 **3** SNMP 트랩을 구성합니다.
단계 **4** SNMP 버전 1 및 2c 파라미터 또는 SNMP 버전 3 파라미터를 구성합니다.

SNMP 에이전트 및 SNMP 서버 활성화

SNMP 에이전트 및 SNMP 서버를 활성화하려면 다음 단계를 수행합니다.

프로시저

ASA에서 SNMP 에이전트 및 SNMP 서버를 활성화. SNMP 서버는 기본적으로 활성화되어 있습니다.

snmp-server enable

예제**:**

```
ciscoasa(config)# snmp-server enable
```

SNMP 관리 스테이션 구성

SNMP 관리 스테이션을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**를 선택합니다. SNMP 서버는 기본적으로 활성화되어 있습니다.

단계 **2** **SNMP Management Stations(SNMP** 관리 스테이션**)** 창에서 **Add(**추가**)**를 클릭합니다.

Add SNMP Host Access Entry(SNMP 호스트 액세스 항목 추가**)** 대화 상자가 나타납니다.

단계 **3** SNMP 호스트가 상주하는 인터페이스를 선택합니다.

단계 **4** SNMP 호스트 IP 주소를 입력합니다.

단계 **5** SNMP 호스트 UDP 포트를 입력하거나 기본값인 포트 162를 유지합니다.

단계 **6** SNMP 호스트 커뮤니티 문자열을 추가합니다. 관리 스테이션에 대한 커뮤니티 문자열이 지정되지 않은 경우 **SNMP Management Stations(SNMP** 관리 스테이션**)** 창에서 **Community String(**커뮤니티 문자열**)**(기본) 필드에 설정된 값이 사용됩니다.

단계 **7** SNMP 호스트가 사용하는 SNMP 버전을 선택합니다.

단계 **8** 이전 단계에서 SNMP Version 3를 선택한 경우 구성된 사용자의 이름을 선택합니다.

단계 **9** 이 NMS와의 통신 방식을 지정하려면 **Poll(**폴링**)** 또는 **Trap(**트랩**)** 확인란을 선택합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

Add SNMP Host Access Entry(SNMP 호스트 액세스 항목 추가**)** 대화 상자가 닫힙니다.

단계 **11** **Apply(**적용**)**를 클릭합니다.

NMS가 구성되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다. SNMP Version 3 NMS 툴에 대한 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

SNMP 트랩 구성

SNMP 에이전트가 생성하는 트랩 및 이를 수집하여 NMS로 전송하는 방법을 지정하려면 다음 단계를 수행합니다.

참고 모든 SNMP 또는 syslog 트랩을 활성화하면 SNMP 프로세스가 에이전트 및 네트워크에서 초과 리소스를 소비하여 시스템이 중단될 수 있습니다. 시스템 지연, 완료되지 않은 요청 또는 시간 초과가 있는 경우 SNMP 및 syslog 트랩을 선택적으로 활성화할 수 있습니다. 예를 들어 정보 의 시스템 로그 트랩 심각도 레벨은 건너뛸 수 있습니다.

프로시저

단계 **1** 개별 트랩, 트랩 집합 또는 모든 트랩을 NMS로 보냅니다.

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart** | **warmstart**] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply**] | **chassis-temperature** | **power-supply-presence** | **power-supply-temperature** **l1-bypass-status**] | **ikev2** [**start** | **stop**] | **cluster-state** | **failover-state** | **peer-flap** | **ipsec** [**start** | **stop**] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [**packet-discard**]

예제**:**

```
ciscoasa(config)# snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
```

이 명령을 통해 syslog 메시지를 트랩으로서 NMS에 보낼 수 있습니다. 기본 구성에는 예에서와 같이 모든 SNMP 표준 트랩이 활성화되어 있습니다. 이 트랩을 비활성화하려면 **no snmp-server enable traps snmp** 명령을 사용합니다.

이 명령을 입력하고 트랩 유형을 지정하지 않으면 기본값은 **syslog** 트랩입니다. 기본적으로 **syslog** 트랩이 활성화됩니다. 기본 SNMP 트랩이 **syslog** 트랩과 함께 활성화를 유지합니다.

logging history 명령과 **snmp-server enable traps syslog** 명령을 모두 구성하여 syslog MIB로부터 트랩을 생성해야 합니다.

SNMP 트랩의 기본 활성화를 복원하려면 **clear configure snmp-server** 명령을 사용하십시오. 모든 다른 트랩은 기본적으로 비활성화되어 있습니다.

관리 상황에서만 이용 가능한 트랩:

- **connection-limit-reached**

- **entity**
- **memory-threshold**

시스템 상황에서 물리적으로 연결된 인터페이스에 대해서만 관리 상황을 통해 생성되는 트랩:

- **interface-threshold**

모든 다른 트랩은 단일 모드의 관리자 및 사용자 상황에서 이용 가능합니다.

config 트랩은 구성 모드를 종료한 후에 생성되는 ciscoConfigManEvent 알림 및 ccmCLIRunningConfigChanged 알림을 활성화합니다.

CPU 사용량이 구성된 모니터링 기간에 대한 구성된 임계값보다 큰 경우 **cpu threshold rising** 트랩이 생성됩니다.

사용된 시스템 상황 메모리가 전체 시스템 메모리의 80%에 도달하면 관리자 상황에서 **memory-threshold** 트랩이 생성됩니다. 다른 사용자 컨텍스트의 경우 이 트랩은 특정 컨텍스트에서 사용된 메모리가 전체 시스템 메모리의 80%에 도달할 때 생성됩니다.

일부 트랩은 특정 하드웨어 모델에 적용됩니다. 트랩 키워드 대신 ?을 사용하여 디바이스에서 사용할 수 있는 트랩을 확인합니다. 예를 들면 다음과 같습니다.

- Firepower 1000 Series는 엔티티 트랩 **chassis-temperature**, **config-change** 및 **cpu-temperature**만 지원합니다.

참고
SNMP에서는 전압 센서를 모니터링하지 않습니다.

단계 **2** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**를 선택합니다.

단계 **3** **Configure Traps(**트랩 구성**)**를 클릭합니다.

SNMP Trap Configuration(SNMP 트랩 구성**)** 대화 상자가 나타납니다.

단계 **4** **SNMP Server Traps Configuration(SNMP** 서버 트랩 구성**)** 확인란을 선택합니다.

기본 구성에서는 모든 SNMP 표준 트랩이 활성화되어 있습니다. 트랩 유형을 지정하지 않으면 기본값은 **syslog** 트랩입니다. 기본 SNMP 트랩이 **syslog** 트랩과 함께 활성화를 유지합니다. 모든 다른 트랩은 기본적으로 비활성화되어 있습니다. 트랩을 비활성화하려면 해당 확인란 선택을 취소합니다.

트랩은 다음 범주로 구분됩니다.

a) **Standard SNMP Traps(**표준 **SNMP** 트랩**)**에서 해당되는 것을 모두 선택합니다.

중요 **CPU** 온도, 섀시 온도, 및 섀시 팬 장애에서 선택합니다.

참고
기본 구성에서는 모든 SNMP 표준 트랩이 활성화되어 있습니다.

b) **Environment Traps(**환경 트랩**)**에서 해당하는 항목을 모두 선택합니다.

인증, 링크 업, 링크 다운, 콜드 스타트, 웜 스타트 중에서 선택합니다.

c) **Ikev2 Traps(Ikev2** 트랩**)**에서 적용되는 모든 항목을 선택합니다.

시작 및 중지를 선택합니다.

d) 엔터티 **MIB** 알림.

현장 교체 가능 유닛에 대한 알림을 받으려면 이 항목을 선택합니다.

e) **IPsec Traps(IPsec** 트랩**)**에서 해당하는 항목을 모두 선택합니다.

시작 및 중지를 선택합니다.

f) 원격 액세스 트랩.

설정된 세션 수가 설정된 임계값을 초과할 때 알림을 받으려면 이 항목을 선택합니다.

g) **Resource Traps(**리소스 트랩**)**에서 해당하는 것을 모두 선택합니다.

연결 제한 도달, 메모리 임계값 도달 및 인터페이스 임계값 도달 중에서 선택합니다.

h) **NAT** 트랩.

매핑 공간을 사용할 수 없어 NAT에서 IP 패킷을 폐기할 때 알림을 받으려면 이 항목을 선택합니다.

i) 시스템 로그.

설정된 세션 수가 설정된 임계값을 초과할 때 알림을 받으려면 시스템 로그 트랩 활성화를 선택합니다.

시스템 로그 트랩 심각도 레벨을 구성하려면 **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Logging(**로깅**)** > **Logging Filters(**로깅 필터**)**를 선택합니다.

j) **CPU** 사용률 트랩.

CPU 사용량이 구성된 모니터링 간격에 대해 구성된 **CPU** 사용률 임계값보다 클 때 알림을 받으려면 **CPU** 상승 임계값 도달에 체크합니다.

k) **SNMP** 트랩 인터페이스 임계값.

인터페이스 대역폭 사용률이 구성된 **SNMP** 인터페이스 임계값보다 클 때 알림을 받으려면 임계값 및 간격 구성에 체크합니다.

유효한 임계값 범위는 30~99%입니다. 기본값은 70%입니다.

l) **SNMP** 메모리 임계값.

CPU 사용량이 **SNMP** 메모리 임계값에 대해 구성된 임계값보다 클 때 알림을 받으려면 메모리 임계값 구성에 체크합니다.

사용된 시스템 컨텍스트 메모리가 전체 시스템 메모리의 80%에 도달하면 관리자 컨텍스트에서 메모리 임계값 트랩이 생성됩니다. 다른 사용자 컨텍스트의 경우 이 트랩은 특정 컨텍스트에서 사용된 메모리가 전체 시스템 메모리의 80%에 도달할 때 생성됩니다.

m) 장애 조치 트랩.

장애 조치에 대한 SNMP 시스템 로그 트랩을 수신하려면 **Enable Failover Related traps(**장애 조치 관련 트랩 활성화**)**에 체크합니다.

n) 클러스터 트랩.

클러스터 멤버에 대한 SNMP 시스템 로그 트랩을 수신하려면 **Enable cluster related traps(**클러스터 관련 트랩 활성화**)**에 체크합니다.

o) 피어 플랩 트랩.

클러스터 피어 MAC 주소 플랩에 대한 SNMP 시스템 로그 트랩을 수신하려면 **Enable bgp/ospf peer-flap Related traps(bgp/ospf** 피어 플랩 관련 트랩 활성화**)**에 체크합니다.

단계 **5** **OK(**확인**)**를 클릭하여 **SNMP Trap Configuration(SNMP** 트랩 구성**)** 대화 상자를 닫습니다.

단계 **6** **Apply(**적용**)**를 클릭합니다.

SNMP 트랩이 구성되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

CPU 사용량 임계값 구성

CPU 사용량 임계값을 구성하려면 다음 단계를 수행합니다.

프로시저

높음 CPU 임계값과 임계값 모니터링 지속 시간에 대한 임계값을 구성합니다.

snmp cpu threshold rising *threshold_value monitoring_period*

예제**:**

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

CPU 사용률의 임계값 및 모니터링 기간을 지우려면 이 명령의 **no** 형식을 사용합니다. **snmp cpu threshold rising** 명령이 구성되지 않은 경우 높음 임계값의 기본값은 70% 이상이고 심각 임계값의 기본값은 95% 이상입니다. 기본 모니터링 지속 시간은 1분으로 설정됩니다.

항상 95%로 유지되는 위험 CPU 임계값 수준은 구성할 수 없습니다. 높음 CPU 임계값의 유효한 범위는 10~94%입니다. 모니터링 기간에 대한 유효한 값은 1~60분입니다.

물리적 인터페이스 임계값 구성

물리적 인터페이스 임계값을 구성하려면 다음 단계를 수행합니다.

프로시저

SNMP 물리적 인터페이스에 대한 임계값을 구성합니다.

snmp interface threshold *threshold_value*

예제:

```
ciscoasa(config)# snmp interface threshold 75%
```

SNMP 물리적 인터페이스에 대한 임계값을 지우려면 이 명령의 **no** 형식을 사용합니다. 임계값은 인터페이스 대역폭 사용량의 백분율로 정의됩니다. 유효한 임계값 범위는 30~99%입니다. 기본값은 70%입니다.

snmp interface threshold 명령은 관리 상황에서만 사용할 수 있습니다.

물리적 인터페이스 사용량은 단일 모드 및 다중 모드에서 모니터링되고 시스템 컨텍스트의 물리적 인터페이스에 대한 트랩은 관리 컨텍스트를 통해 전송됩니다. 임계값 사용량 계산에는 물리적 인터페이스만 사용됩니다.

SNMP 버전 1 또는 2c에 대한 매개변수 구성

SNMP 버전 1 또는 2c에 대한 파라미터를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 1 SNMP 알림 수신자를 지정하고 트랩이 전송되는 인터페이스를 표기하며 ASA에 연결 가능한 NMS 또는 SNMP 관리자의 이름과 IP 주소를 식별합니다.

snmp-server host {*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** **2c**| *username*}] [**udp-port** *port*]

예제:

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

trap 키워드는 NMS를 트랩 수신으로만 제한합니다. **poll** 키워드는 NMS를 요청 전송(폴링)으로만 제한합니다. 기본적으로 SNMP 트랩은 활성화되어 있습니다. 기본적으로, UDP 포트는 162입니다. 커뮤니티 문자열은 ASA 및 NMS 사이의 공유 비밀 키입니다. 키는 대/소문자를 구분하며 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다. 기본 커뮤니티 문자열은 공개됩니다. ASA는 이 키를 사용하여 수신 SNMP 요청의 유효성을 판단합니다. 예를 들어, 커뮤니티 문자열로 사이트를 지정한 후 같은 문자열로 ASA 및 관리 스테이션을 구성할 수 있습니다. ASA는 지정된 문자열을 사용하고 커뮤니

티 문자열이 유효하지 않은 요청에는 응답하지 않습니다. 하지만 진단 인터페이스 대신 관리 인터페이스를 통해 SNMP 모니터링을 수행하는 경우 커뮤니티 문자열을 검증하는 ASA 없이 폴링이 이루어집니다. 암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템(예: CLI, ASDM, CSM 등)에 표시됩니다. 일반 텍스트 비밀번호는 표시되지 않습니다. 암호화된 커뮤니티 문자열은 항상 ASA에서 생성됩니다. 대개 입력 형식은 일반 텍스트 형식입니다.

version 키워드는 트랩 및 요청(폴링)에 사용할 SNMP 버전을 지정합니다. 서버와의 통신은 선택한 버전만을 사용하여 허용됩니다.

snmp-server host 명령을 추가한 후 트랩을 수신하려면, NMS의 사용자 자격 증명을 ASA에 구성된 자격 증명과 같게 구성해야 합니다.

단계 **2** SNMP 버전 1 또는 2c에 한해 사용할 커뮤니티 문자열을 설정합니다.

snmp-server community *community-string*

예제**:**

```
ciscoasa(config)# snmp-server community onceuponatime
```

참고
커뮤니티 문자열에 특수 문자(! ,@, #, $, %, ^, &, *, \)를 사용하지 않아야 합니다. 일반적으로 운영 체제에서 사용하는 기능용으로 예약된 특수 문자를 사용하면 예기치 않은 결과가 발생할 수 있습니다. 예를 들어 백슬래시 (\)는 이스케이프 문자로 해석되므로 커뮤니티 문자열에 사용해서는 안 됩니다.

단계 **3** SNMP 서버 위치 또는 연락처 정보를 설정합니다.

snmp-server [**contact** | **location**] *text*

예제**:**

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 인수는 연락 담당자 또는 ASA 시스템 관리자의 이름을 지정합니다. 이름은 대/소문자를 구분하며, 최대 127자까지 허용됩니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

단계 **4** SNMP 요청에 대한 듣기 포트를 설정합니다.

snmp-server listen-port *lport*

예제**:**

```
ciscoasa(config)# snmp-server lport 192
```

lport 인수는 수신 요청이 수락되는 포트입니다. 기본 수신 포트는 161입니다. **snmp-server listen-port** 명령은 관리자 상황에서만 사용 가능하며 시스템 상황에서는 사용할 수 없습니다. 현재 사용 중인 포트에서 **snmp-server listen-port** 명령을 구성한 경우 다음 메시지가 표시됩니다.

```
The UDP port port is in use by another feature. SNMP requests to the device
```

```
will fail until the snmp-server listen-port command is configured to use a different port.
```

기존 SNMP 스레드는 포트를 사용할 수 있을 때까지 60초마다 계속 폴링하며, 포트를 여전히 사용 중인 경우 syslog 메시지 %ASA-1-212001을 발행합니다.

단계 **5** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**를 선택합니다.

단계 **6** SNMP 버전 1 또는 2c를 사용 중인 경우 **Community String(**커뮤니티 문자열**)**(기본) 필드에 커뮤니티 문자열을 입력합니다. ASA에 요청을 보낼 때 SNMP NMS가 사용하는 비밀번호를 입력합니다. SNMP 커뮤니티 문자열은 SNMP NMS와 관리 대상 네트워크 노드 사이에서 비밀로 공유됩니다. ASA 이 비밀번호를 사용하여 수신 SNMP 요청이 유효한지 판단합니다. 하지만 진단 인터페이스 대신 관리 인터페이스를 통해 SNMP 모니터링을 수행하는 경우 커뮤니티 문자열을 검증하는 ASA 없이 폴링이 이루어집니다. 비밀번호는 대/소문자를 구분하며 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다. 기본값은 public입니다. SNMP 버전 2c에서는 각 NMS에 대해 별도의 커뮤니티 문자열을 설정할 수 있습니다. NMS에 대해 커뮤니티 문자열이 구성되지 않은 경우 기본적으로 여기서 설정된 값이 사용됩니다.

참고
커뮤니티 문자열에 특수 문자(! ,@, #, $, %, ^, &, *, \)를 사용하지 않아야 합니다. 일반적으로 운영 체제에서 사용하는 기능용으로 예약된 특수 문자를 사용하면 예기치 않은 결과가 발생할 수 있습니다. 예를 들어 백슬래시 (\)는 이스케이프 문자로 해석되므로 커뮤니티 문자열에 사용해서는 안 됩니다.

단계 **7** ASA 시스템 관리자의 이름을 입력합니다. 텍스트는 대/소문자를 구분하며 최대 127자의 영문자입니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

단계 **8** SNMP가 관리하는 ASA의 위치를 입력합니다. 텍스트는 대/소문자를 구분하며 최대 127자까지 가능합니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

단계 **9** NMS로부터 SNMP 요청을 듣는 ASA 포트의 번호를 입력하거나 기본값인 161번으로 유지합니다.

단계 **10** (선택 사항) **Enable Global-Shared pool in the walk(**탐색에서 전역 공유 풀 활성화**)** 확인란을 선택하여 SNMP 워크 작업을 통해 여유 메모리 및 사용된 메모리 통계를 쿼리합니다.

중요
ASA에서 메모리 정보를 쿼리할 때, CPU를 다른 프로세스에서 해제할 때까지 SNMP 프로세스에서 너무 오랫동안 보류할 수 있습니다. 이로 인해 SNMP 관련 CPU 사용량이 많아져 패킷 삭제가 발생할 수 있습니다.

단계 **11** **SNMP Host Access List(SNMP** 호스트 액세스 목록**)** 창의 **Add(**추가**)**를 클릭합니다.

Add SNMP Host Access Entry(SNMP 호스트 액세스 항목 추가**)** 대화 상자가 나타납니다.

단계 **12** 드롭다운 목록에서 트랩이 전송되는 인터페이스 이름을 선택합니다.

단계 **13** ASA에 연결할 수 있는 NMS 또는 SNMP 관리자의 IP 주소를 입력합니다.

단계 **14** UDP 포트 번호를 입력합니다. 기본값은 162입니다.

단계 **15** 드롭다운 목록에서 사용 중인 SNMP 버전을 선택합니다. 버전 1 또는 버전 2c를 선택하면 커뮤니티 문자열을 입력해야 합니다. Version 3를 선택하면 드롭다운 목록에서 사용자 이름을 선택해야 합니다.

버전은 트랩 및 요청(폴링)에 사용할 SNMP 버전을 지정합니다. 서버와의 통신은 선택한 버전만을 사용하여 허용됩니다.

단계 **16** **Server Poll/Trap Specification(**서버 폴링/트랩 사양**)** 영역에서 **Poll(**폴링**)** 확인란을 선택하여 NMS를 요청 전송(폴링)으로만 제한합니다. NMS를 트랩 수신으로만 제한하려면 **Trap(**트랩**)** 확인란을 선택합니다. 두 확인란을 모두 선택하면 SNMP 호스트의 두 기능을 모두 수행할 수 있습니다.

단계 **17** **OK(**확인**)**를 클릭하여 **Add SNMP Host Access Entry(SNMP** 호스트 액세스 항목 추가**)** 대화 상자를 닫습니다.

새로운 호스트가 **SNMP Host Access List(SNMP** 호스트 액세스 목록**)** 창에 나타납니다.

단계 **18** **Apply** 버튼을 클릭합니다.

Version 1, 2c 또는 3에 대한 SNMP 매개변수가 구성되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

SNMP Version 3에 대한 매개변수 구성

SNMP 버전 3에 대한 파라미터를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 새로운 SNMP 버전 3에 한하여 사용할 수 있는 새 SNMP 그룹을 지정합니다.

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

예제**:**

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

커뮤니티 문자열이 구성될 때 커뮤니티 문자열과 일치하는 이름의 추가 그룹 2개가 자동으로 생성됩니다. 하나는 버전 1 보안 모델을 위한 것이고 다른 하나는 버전 2 보안 모델을 위한 것입니다. **auth** 키워드는 패킷 인증을 활성화합니다. **noauth** 키워드는 패킷 인증 또는 암호화가 사용되지 않음을 의미합니다. **priv** 키워드는 패킷 암호화와 인증을 활성화합니다. **auth** 또는 **priv** 키워드에 대한 기본값은 존재하지 않습니다.

단계 **2** SNMP 버전 3에서만 사용할 SNMP 그룹을 위한 새 사용자를 구성합니다.

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** {**sha** | **sha224** | **sha256** | **sha384**} *auth_password* [**priv** {**3des** | **aes** {**128** | **192** | **256**}} *priv_password*]]

예제**:**

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

username 인수는 SNMP 에이전트에 속하는 호스트의 사용자 이름입니다. username에 최대 32자까지 입력할 수 있습니다. 이름은 문자로 시작해야 합니다. 올바른 문자에는 글자, 숫자, _(밑줄)이 포함됩니다. (마침표), @(at 기호) 및 -(하이픈)을 지정할 수 있습니다.

group-name 인수는 사용자가 속하는 그룹의 이름입니다. **v3** 키워드는 SNMP 버전 3 보안 모델을 사용해야 함을 지정하고 **encrypted**, **priv** 및 **auth** 키워드의 사용을 활성화합니다. **engineID** 키워드는 선택 사항이며 사용자의 인증 및 암호화 정보를 현지화하는 데 사용된 ASA의 engineID를 지정합니다. EngineID 인수는 유효한 ASA engineID를 지정해야 합니다.

encrypted 키워드는 암호화된 형식으로 비밀번호를 지정합니다. 암호화된 비밀번호는 다음 요건을 충족해야 합니다.

- 16진수 형식이어야 합니다.
- 8자 이상, 80자 이하여야 합니다.
- 문자, 숫자 및 ~`!@#%^&*()_-+{}[]|\:;"'<,>./만 포함해야 합니다:
- 다음 기호는 포함할 수 없습니다. 예: $(달러 기호), ? (물음표) 또는 = (등호).
- 각기 다른 문자를 5자 이상 포함해야 합니다.
- 연속적으로 증가하거나 감소하는 문자나 숫자를 너무 많이 포함하면 안 됩니다. 예를 들어 "12345" 문자열에는 이러한 문자가 4개 포함되고 "ZYXW" 문자열에는 3개 포함됩니다. 증가/감소 문자의 총수가 특정 한도를 초과하는 경우(대개 해당 문자가 4~6개 이상 포함되는 경우) 단순성 검사에 실패하게 됩니다.

  참고
  연속적으로 증가하거나 감소하는 문자 사이에 증가하거나 감소하지 않는 문자가 사용되는 경우에는 증가/감소 문자 수가 재설정되지 않습니다. 예를 들어 abcd&!21의 경우 비밀번호 검사에 실패하지만 abcd&!25의 경우에는 비밀번호 검사에 통과합니다.

인증 수준(**sha**, **sha224**, **sha256**, 또는 **sha384**)을 지정하는 **auth** 키워드가 사용되어야 합니다. **priv** 키워드는 암호화 레벨을 지정합니다. **auth** 또는 **priv** 키워드에 대한 기본값 또는 기본 비밀번호가 존재하지 않습니다.

암호화 알고리즘의 경우 **3des** 또는 **aes** 키워드를 지정할 수 있습니다. 또한 **128**, **192** 또는 **256** 중에서 사용할 AES 암호화 알고리즘 버전을 지정할 수 있습니다. auth-password 인수는 인증 사용자 비밀번호를 지정합니다. priv-password 인수는 암호화 사용자 비밀번호를 지정합니다.

비밀번호를 잊어버린 경우 복구할 수 없으며 사용자를 다시 구성해야 합니다. 일반 텍스트 비밀번호 또는 현지화된 다이제스트를 지정할 수 있습니다. 현지화된 다이제스트는 사용자를 위해 선택한 인증 알고리즘과 일치해야 하며, SHA, SHA-224, SHA-256 또는 SHA-384가 될 수 있습니다. 사용자 구성이 콘솔에 표시되거나 파일에 작성된 경우(예를 들어 startup-configuration 파일) 일반 텍스트 비밀번호 대신 항상 현지화된 인증 및 프라이버시 다이제스트가 표시됩니다(두 번째 예시 참고). 비밀번호 최소 길이는 영숫자 1자이나 보안을 위해 8자 이상으로 사용하는 것이 좋습니다.

클러스터링 또는 장애 조치와 함께 SNMPv3를 사용하는 경우, 초기 클러스터 구성 후 새 클러스터 디바이스를 추가하거나 장애 조치 장치를 교체하는 경우 SNMPv3 사용자는 새 디바이스에 복제되지 않습니다. 사용자가 새 디바이스에 강제로 복제되도록 하려면 SNMPv3 사용자를 제어/활성 디바이스에 다시 추가하거나 새 디바이스에 직접 사용자를 추가해야 합니다(SNMPv3 사용자 및 그룹은 클

러스터 데이터 디바이스에 구성 명령을 입력할 수 없다는 규칙의 예외입니다). **snmp-server user** *username group-name* **v3** 명령을 제어/활성 유닛 또는 암호화되지 않은 형태의 *priv-password* 옵션 및 *auth-password* 옵션과 함께 데이타/스탠바이 유닛에 직접 입력하여 각 사용자를 다시 구성합니다.

encrypted 키워드를 사용하여 제어/활성 유닛에서 사용자를 입력한 경우 SNMPv3 사용자 명령이 복제되지 않음을 알리는 오류 메시지가 표시됩니다. 또한, 이 동작으로 인해 기존 SNMPv3 사용자 및 그룹 명령이 복제 중에 지워지지 않습니다.

예를 들어, 제어/활성 유닛에서 암호화된 키와 함께 입력한 명령을 사용하여:

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

예를 들어, 클러스터 복제 중 데이터 단위(구성에 **snmp-server user**명령이 있는 경우에만 표시됨):

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

단계 **3** SNMP 알림 수신자를 지정하십시오. 트랩이 전송된 인터페이스를 지정합니다. ASA에 연결할 수 있는 NMS 또는 SNMP 관리자의 이름과 IP 주소를 식별합니다.

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

예제**:**

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

trap 키워드는 NMS를 트랩 수신으로만 제한합니다. **poll** 키워드는 NMS를 요청 전송(폴링)으로만 제한합니다. 기본적으로 SNMP 트랩은 활성화되어 있습니다. 기본적으로, UDP 포트는 162입니다. 커뮤니티 문자열은 ASA 및 NMS 사이의 공유 비밀 키입니다. 키는 대/소문자를 구분하며 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다. 기본 커뮤니티 문자열은 public입니다. ASA는 이 키를 사용하여 수신 SNMP 요청의 유효성을 판단합니다. 예를 들어, 커뮤니티 문자열로 사이트를 지정한 후 같은 문자열로 ASA와 NMS를 구성할 수 있습니다. ASA는 지정된 문자열을 사용하고 커뮤니티 문자열이 유효하지 않은 요청에는 응답하지 않습니다. 암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템(예: CLI, ASDM, CSM 등)에 표시됩니다. 일반 텍스트 비밀번호는 표시되지 않습니다. 암호화된 커뮤니티 문자열은 항상 ASA에서 생성됩니다. 대개 입력 형식은 일반 텍스트 형식입니다.

version 키워드는 트랩 및 요청(폴링)에 사용할 SNMP 버전을 지정합니다. 서버와의 통신은 선택한 버전만을 사용하여 허용됩니다.

SNMP 버전 3 호스트가 ASA에 구성된 경우 사용자가 해당 호스트에 연결되어야 합니다.

snmp-server host 명령을 추가한 후 트랩을 수신하려면, NMS의 사용자 자격 증명을 ASA에 구성된 자격 증명과 같게 구성해야 합니다.

단계 **4** SNMP 서버 위치 또는 연락처 정보를 설정합니다.

snmp-server [**contact** | **location**] *text*

예제**:**

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 인수는 연락 담당자 또는 ASA 시스템 관리자의 이름을 지정합니다. 이름은 대/소문자를 구분하며, 최대 127자까지 허용됩니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

단계 **5** SNMP 요청에 대한 듣기 포트를 설정합니다.

snmp-server listen-port *lport*

예제**:**

```
ciscoasa(config)# snmp-server lport 192
```

lport 인수는 수신 요청이 수락되는 포트입니다. 기본 수신 포트는 161입니다. **snmp-server listen-port** 명령은 관리자 상황에서만 사용 가능하며 시스템 상황에서는 사용할 수 없습니다. 현재 사용 중인 포트에서 **snmp-server listen-port** 명령을 구성한 경우 다음 메시지가 표시됩니다.

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

기존 SNMP 스레드는 포트를 사용할 수 있을 때까지 60초마다 계속 폴링하며, 포트를 여전히 사용 중인 경우 syslog 메시지 %ASA-1-212001을 발행합니다.

단계 **6** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**를 선택합니다.

단계 **7** **Add(**추가**)** > **SNMP User(SNMP** 사용자**)**를 **SNMPv3 User/Group(SNMPv3** 사용자/그룹**)** 탭(**SNMPv3 Users(SNMPv3** 사용자**)** 창에 있음)에서 클릭하여 구성된 사용자 또는 신규 사용자를 그룹에 추가합니다. 그룹의 마지막 사용자를 제거하면 ASDM은 그룹을 삭제합니다.

참고
사용자가 생성된 후에는 해당 사용자가 속한 그룹을 변경할 수 없습니다.

Add SNMP User Entry(SNMP 사용자 항목 추가**)** 대화 상자가 나타납니다.

단계 **8** SNMP 사용자가 속해 있는 그룹을 선택합니다. 사용 가능한 그룹은 다음과 같습니다.

- **Auth&Encryption(**인증 및 암호화**)**: 사용자의 인증 및 암호화가 구성되어 있음
- **Authentication_Only(**인증만**)**: 사용자의 인증만 구성되어 있음
- **No_Authentication(**인증 없음**)**: 사용자의 인증이나 암호화가 구성되어 있지 않음

참고
그룹 이름은 변경할 수 없습니다.

단계 **9** 사용자 보안 모델(USM) 그룹을 사용하려면 **USM Model(USM** 모델**)** 탭을 클릭합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

Add SNMP USM Entry(SNMP USM 항목 추가**)** 대화 상자가 나타납니다.

단계 **11** 그룹 이름을 입력합니다.

단계 **12** 드롭다운 목록에서 보안 수준을 선택합니다. 이 설정을 통해 구성된 USM 그룹을 보안 수준으로 SNMPv3 사용자에게 할당할 수 있습니다.

단계 **13** 구성된 사용자 또는 새로운 사용자의 이름을 입력합니다. 사용자 이름은 선택된 SNMP 서버 그룹에 대해 고유해야 합니다.

단계 **14** **Encrypted(**암호화됨**)** 또는 **Clear Text(**텍스트 지우기**)** 라디오 버튼 중 하나를 클릭하여 사용할 비밀번호 유형을 지정합니다.

단계 **15** **MD5** 또는 **SHA MD5**, **SHA1**또는 **SHA256 SHA**, **SHA224**, **SHA256**또는 **SHA384** 네 라디오 버튼 중 하나를 클릭하여 사용할 인증 유형을 표시.

단계 **16** 인증에 사용할 비밀번호를 입력합니다.

단계 **17** 두 라디오 버튼 **3DES**, **AES**또는 중 하나를 클릭하여 사용하려는 암호화 유형을 지정합니다.

단계 **18** AES 암호화를 선택할 경우 **128**, **192** 또는 **256** 중 사용할 AES 암호화 수준도 선택합니다.

단계 **19** 암호화에 사용할 비밀번호를 입력합니다. 이 비밀번호에 허용되는 영숫자 문자의 최대 길이는 64자입니다.

단계 **20** **OK(**확인**)**를 클릭하여 그룹을 생성하고(이 사용자가 해당 그룹의 첫 번째 사용자인 경우) 그룹을 **Group Name(**그룹 이름**)** 드롭다운 목록에 표시하고 해당 그룹에 대한 사용자를 생성합니다.

Add SNMP User Entry(SNMP 사용자 항목 추가**)** 대화 상자가 닫힙니다.

단계 **21** **Apply(**적용**)**를 클릭합니다.

Version 3에 대한 SNMP 매개변수가 구성되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

사용자 그룹 구성

지정된 사용자 그룹을 포함한 SNMP 사용자 목록을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** SNMP 사용자 목록을 구성합니다.

snmp-server user-list *list_name* **username** *user_name*

예제**:**

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

listname 인수는 최대 33자 길이의 사용자 목록 이름을 지정합니다. **username** *user_name* 키워드-인수 쌍은 사용자 목록에 구성될 수 있는 사용자를 지정합니다. SNMP 버전 3을 사용하는 경우에만 이용 가능한 **snmp-server user** *username* 명령으로 사용자 목록에서 사용자를 구성할 수 있습니다. 사용자 목록은 둘 이상의 사용자가 있어야 하며, 호스트 이름 또는 IP 주소 범위와 연결될 수 있습니다.

단계 **2** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**를 선택합니다.

단계 **3** **Add(**추가**)** > **SNMP User Group(SNMP** 사용자 그룹**)**을 **SNMPv3 User/Group(SNMPv3** 사용자/그룹**)** 탭(**SNMPv3 Users(SNMPv3** 사용자**)** 창에 있음)에서 클릭하여 구성된 사용자 그룹 또는 신규 사용자 그룹을 추가합니다. 그룹의 마지막 사용자를 제거하면 ASDM은 그룹을 삭제합니다.

Add SNMP User Group(SNMP 사용자 그룹 추가**)** 대화 상자가 나타납니다.

단계 **4** 사용자 그룹 이름을 입력합니다.

단계 **5** 기존 사용자 또는 사용자 그룹을 선택하려면 **Existing User/User Group(**기존 사용자/사용자 그룹**)** 라디오 버튼을 클릭합니다.

단계 **6** 새 사용자를 만들려면 **Create new user(**새 사용자 생성**)** 라디오 버튼을 클릭합니다.

단계 **7** SNMP 사용자가 속해 있는 그룹을 선택합니다. 사용 가능한 그룹은 다음과 같습니다.

- **Auth&Encryption(**인증 및 암호화**)**: 사용자의 인증 및 암호화가 구성되어 있음
- **Authentication_Only(**인증만**)**: 사용자의 인증만 구성되어 있음
- **No_Authentication(**인증 없음**)**: 사용자의 인증이나 암호화가 구성되어 있지 않음

단계 **8** 구성된 사용자 또는 새로운 사용자의 이름을 입력합니다. 사용자 이름은 선택된 SNMP 서버 그룹에 대해 고유해야 합니다.

단계 **9** **Encrypted(**암호화됨**)** 또는 **Clear Text(**텍스트 지우기**)** 라디오 버튼 중 하나를 클릭하여 사용할 비밀번호 유형을 지정합니다.

단계 **10** **SHA**, **SHA224**, **SHA256** 또는 **SHA384** 네 라디오 버튼 중 하나를 클릭하여 사용할 인증 유형을 지정합니다.

단계 **11** 인증에 사용할 비밀번호를 입력합니다.

단계 **12** 인증에 사용할 비밀번호를 확인합니다.

단계 **13** 두 라디오 버튼 **3DES**, **AES**또는 중 하나를 클릭하여 사용하려는 암호화 유형을 지정합니다.

단계 **14** 암호화에 사용할 비밀번호를 입력합니다. 이 비밀번호에 허용되는 영숫자 문자의 최대 길이는 64자입니다.

단계 **15** 암호화에 사용할 비밀번호를 확인합니다.

단계 **16** **Add(**추가**)**를 클릭하여 새로운 사용자를 **Members in Group(**그룹의 멤버**)** 창의 지정된 사용자 그룹에 추가합니다. **Remove(**제거**)**를 클릭하여 **Members in Group(**그룹의 멤버**)** 창에서 기존 사용자를 삭제합니다.

단계 **17** **OK(**확인**)**를 클릭하여 지정된 사용자 그룹에 대한 새로운 사용자를 생성합니다.

Add SNMP User Group(SNMP 사용자 그룹 추가**)** 대화 상자가 닫힙니다.

단계 **18** **Apply(**적용**)**를 클릭합니다.

Version 3에 대한 SNMP 매개변수가 구성되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

사용자와 네트워크 개체 연결

사용자 목록의 단일 사용자 또는 사용자 그룹을 네트워크 개체와 연결하려면 다음 단계를 수행합니다.

프로시저

사용자 목록의 단일 사용자 또는 사용자 그룹을 네트워크 개체와 연결합니다.

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

예제**:**

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 인수는 사용자 또는 사용자 그룹이 연결된 인터페이스 네트워크 개체 이름을 지정합니다.

trap 키워드는 트랩만 전송될 수 있으며 이 호스트는 찾아보기(폴링)가 허용되지 않음을 나타냅니다. SNMP 트랩은 기본적으로 활성화되어 있습니다.

poll 키워드는 이 호스트에서 찾아보기(폴링)가 허용되지만 트랩을 전송할 수 없음을 나타냅니다.

community 키워드는 NMS에서 요청을 수신할 때 또는 NMS로 전송되는 트랩을 생성할 때 기본값이 아닌 문자열이 필요함을 나타냅니다. SNMP 버전 1 또는 2c에만 이 키워드를 사용할 수 있습니다. *community-string* 인수는 알림과 함께 전송되거나 NMS의 요청에서 전송되는 비밀번호와 비슷한 커뮤니티 문자열을 지정합니다. 커뮤니티 문자열은 최대 32자까지 허용됩니다.

version 키워드는 트랩을 보내고 요청을 수락(폴링)하는 데 사용할 SNMP 알림 버전을 버전 1, 2c 또는 3으로 설정합니다. 기본 버전은 1입니다.

username 인수는 SNMP 버전 3을 사용할 경우 사용자의 이름을 지정합니다.

user-list *list_name* 키워드-인수 페어는 사용자 목록의 이름을 지정합니다.

udp-port *port* 키워드-인수 쌍은 SNMP 트랩이 기본값이 아닌 포트의 NMS 호스트로 전송되어야 함을 지정하고 NMS 호스트의 UDP 포트 번호를 설정합니다. 기본 UDP 포트는 162입니다.

SNMP 모니터링

SNMP 모니터링에 대한 내용은 다음 명령을 참고하십시오. **Tools(**툴**) > Command Line Interface(**명령행 인터페이스**)**를 사용하여 다음 명령을 입력할 수 있습니다.

- **show running-config snmp-server** [**default**]

  이 명령은 모든 SNMP 서버 구성 정보를 표시합니다.

- **show running-config snmp-server group**

  이 명령은 SNMP 그룹 구성 설정을 표시합니다.

- **show running-config snmp-server host**

  이 명령은 SNMP에서 원격 호스트로 전송되는 메시지 및 알림을 제어하는 데 사용되는 구성 설정을 표시합니다.

- **show running-config snmp-server host-group**

  이 명령은 SNMP 호스트 그룹 구성을 표시합니다.

- **show running-config snmp-server user**

  이 명령은 SNMP 사용자 기반 구성 설정을 표시합니다.

- **show running-config snmp-server user-list**

  이 명령은 SNMP 사용자 목록 구성을 표시합니다.

- **show snmp-server engineid**

  이 명령은 구성된 SNMP 엔진의 ID를 표시합니다.

- **show snmp-server group**

  이 명령은 구성된 SNMP 그룹의 이름을 표시합니다. 커뮤니티 문자열이 이미 설정 구성된 경우 기본적으로 출력에 2개의 추가 그룹이 표시됩니다. 이는 정상입니다.

- **show snmp-server statistics**

  이 명령은 SNMP 서버의 구성된 특성을 표시합니다. 모든 SNMP 카운터를 0으로 재설정하려면 **clear snmp-server statistics** 명령을 사용하십시오.

- **show snmp-server user**

  이 명령은 사용자의 구성 특성을 표시합니다.

예

다음 예는 SNMP 서버 통계를 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
```

```
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

다음 예는 SNMP 서버 실행 구성을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP의 예

다음 섹션에서는 모든 SNMP Version의 참조로 사용할 수 있는 예를 제공합니다.

SNMP 버전 1 및 2c

다음 예는 ASA가 내부 인터페이스의 호스트 192.0.2.5으로부터 SNMP 요청을 받되 호스트로 SNMP syslog 요청을 전송하지 않는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP 버전 3

다음 예는 ASA가 SNMP 버전 3 보안 모델(그룹, 사용자, 호스트 순으로 구성해야 함)을 사용하여 SNMP 요청을 수신하는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

SNMP 기록

표 *7: SNMP* 기록

기능 이름	버전	설명
SNMP 버전 1 및 2c	7.0(1)	일반 텍스트 커뮤니티 문자열을 통해 SNMP 서버와 SNMP 에이전트 간에 데이터를 전송하여 ASA 네트워크 모니터링 및 이벤트 정보를 제공합니다. 다음 화면을 수정했습니다. Configuration(구성) > Device Management(디바이스 관리) > Management Access(관리 액세스) > SNMP
SNMP 버전 3	8.2(1)	3DES 또는 AES 암호화를 제공하고 지원 보안 모델 중 가장 안전한 SNMP 버전 3을 지원합니다. 이 버전에서는 USM을 사용하여 사용자, 그룹 및 호스트는 물론 인증 특성도 구성할 수 있습니다. 또한 이 버전은 에이전트 및 MIB 객체에 대한 액세스 제어가 가능하며 추가 MIB 지원을 포함합니다. 다음 명령을 도입 또는 수정했습니다. **show snmp-server engineid**, **show snmp-server group**, **show snmp-server user**, **snmp-server group**, **snmp-server user**, **snmp-server host**. 다음 화면을 수정했습니다. Configuration(구성) > Device Management(디바이스 관리) > Management Access(관리 액세스) > SNMP
비밀번호 암호화	8.3(1)	비밀번호 암호화를 지원합니다. 다음 명령을 수정했습니다. **snmp-server community**, **snmp-server host**.

기능 이름	버전	설명
SNMP 트랩 및 MIB	8.4(1)	다음 추가 키워드를 지원합니다. **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. 센서, 팬, 전원 공급 장치 및 관련 구성 요소에 대한 entPhysicalTable 보고 항목. 다음 추가 MIB를 지원합니다. CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB. 다음 추가 트랩을 지원합니다. ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart. 다음 화면을 수정했습니다. Configuration(구성) > Device Management(디바이스 관리) > Management Access(관리 액세스) > SNMP 다음 명령을 도입 또는 수정했습니다. **snmp cpu threshold rising**, **snmp interface threshold**, **snmp-server enable traps**.
IF-MIB ifAlias OID 지원	8.2(5) / 8.4(2)	이제 ASA가 ifAlias OID를 지원합니다. IF-MIB를 찾아볼 때 ifAlias OID는 인터페이스 설명에 설정된 값으로 설정됩니다.
ASA 서비스 모듈(ASASM)	8.5(1)	ASASM은 다음을 제외하고 8.4(1)의 모든 MIB 및 트랩을 지원합니다. 8.5(1)에서 지원되지 않는 MIB: • CISCO-ENTITY-SENSOR-EXT-MIB(entPhySensorTable 그룹의 객체만 지원됨). • ENTITY-SENSOR-MIB(entPhySensorTable 그룹의 객체만 지원됨). • DISMAN-EXPRESSION-MIB(expExpressionTable, expObjectTable 및 expValueTable 그룹의 객체만 지원됨). 8.5(1)에서 지원되지 않는 트랩: • ceSensorExtThresholdNotification(CISCO-ENTITY-SENSOR-EXT-MIB). 이 트랩은 전원 공급 장치 및 팬 고장, CPU 고온 이벤트에만 사용됩니다. • InterfacesBandwidthUtilization.

기능 이름	버전	설명
SNMP 트랩	8.6(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X에 대해 다음 추가 키워드를 지원합니다. **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**. 다음 명령을 수정했습니다. **snmp-server enable traps**
VPN 관련 MIB	9.0(1)	차세대 암호화 기능 지원을 위해 업데이트된 버전의 CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB가 구현되었습니다. 다음 MIB가 ASASM에 대해 활성화되었습니다. • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	다음 MIB가 추가되었습니다. CISCO-TRUSTSEC-SXP-MIB.
SNMP OID	9.1(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 지원을 위해 5개의 새로운 SNMP 물리적 공급업체 유형 OID가 추가되었습니다.
NAT MIB	9.1(2)	xlate_count 및 max_xlate_count 항목 지원을 위해 cnatAddrBindNumberOfEntries 및 cnatAddrBindSessionCount OID가 추가되었습니다. 이는 **show xlate count** 명령을 사용한 폴링 허용과 대등합니다.
SNMP 호스트, 호스트 그룹 및 사용자 목록	9.1(5)	이제 호스트를 최대 4000개까지 추가할 수 있습니다. 지원되는 활성 폴링 대상 수는 128개입니다. 호스트 그룹으로 추가할 개별 호스트를 나타내는 네트워크 객체를 지정할 수 있습니다. 둘 이상의 사용자를 하나의 호스트와 연결할 수 있습니다. 다음 명령을 도입 또는 수정했습니다. **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**. 다음 화면을 수정했습니다. Configuration(구성) > Device Management(디바이스 관리) > Management Access(관리 액세스) > SNMP
SNMP 메시지 크기	9.2(1)	SNMP가 전송하는 메시지 크기 제한이 1472바이트로 증가했습니다.

기능 이름	버전	설명
SNMP OID 및 MIB	9.2(1)	이제 ASA가 cpmCPUTotal5minRev OID를 지원합니다. ASA 가상가 SNMP sysObjectID OID 및 entPhysicalVendorType OID에 새로운 제품으로 추가되었습니다. CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB가 업데이트되어 새로운 ASA 가상 플랫폼을 지원합니다. VPN 공유 라이센스 사용량 모니터링을 위한 새로운 SNMP MIB가 추가되었습니다.
SNMP OID 및 MIB	9.3(1)	ASASM에 대한 CISCO-REMOTE-ACCESS-MONITOR-MIB(OID 1.3.6.1.4.1.9.9.392) 지원이 추가되었습니다.
SNMP MIB 및 트랩	9.3(2)	CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB는 ASA 5506-X를 지원하도록 업데이트되었습니다. ASA 5506-X가 SNMP sysObjectID OID 및 entPhysicalVendorType OID 테이블에 새로운 제품으로 추가되었습니다. 이제 ASA에서 CISCO-CONFIG-MAN-MIB를 지원하므로 다음 작업을 수행할 수 있습니다. • 특정 구성에 대해 어떤 명령이 입력되었는지 알 수 있습니다. • 구성 실행 중 변경이 발생하면 NMS에게 알립니다. • 실행 중인 구성이 마지막으로 변경되거나 저장된 시간에 대한 타임스탬프를 추적합니다. • 터미널 정보 및 명령 소스와 같은 기타 명령 변경 사항을 추적합니다. 다음 명령을 수정했습니다. **snmp-server enable traps** 다음 화면을 수정했습니다. Configuration(구성) > Device Management(디바이스 관리) > Management Access(관리 액세스) > SNMP > Configure Traps(트랩 구성) > SNMP Trap Configuration(SNMP 트랩 구성)
SNMP MIB 및 트랩	9.4(1)	ASA 5506W-X, ASA 5506H-X, ASA 5508-X 및 ASA 5516-X가 SNMP sysObjectID OID 및 entPhysicalVendorType OID 테이블에 새 제품으로 추가되었습니다.
상황당 무제한 SNMP 서버 트랩 호스트	9.4(1)	ASA는 상황별로 무제한 SNMP 서버 트랩 호스트를 지원합니다. **show snmp-server host** 명령 출력에는 정적으로 구성한 호스트와 함께 ASA를 폴링 중인 활성 호스트만 표시됩니다. 다음 명령을 수정했습니다. **show snmp-server host** ASDM 화면은 수정하지 않았습니다.

기능 이름	버전	설명
ISA 3000에 대한 지원 추가됨	9.4(1.225)	ISA 3000 제품군이 이제 SNMP에 대해 지원됩니다. 이 플랫폼에 대한 새 OID를 추가했습니다. **snmp-server enable traps entity** 명령이 새로운 변수인 *l1-bypass-status*를 포함하도록 수정되었습니다. 이렇게 하면 하드웨어 우회 상태 변경이 활성화됩니다. 다음 명령을 수정했습니다. **snmp-server enable traps entity**. ASDM 화면은 수정하지 않았습니다.
CISCO-ENHANCED-MEMPOOL-MIB에서 cempMemPoolTable에 대한 지원	9.6(1)	이제 CISCO-ENHANCED-MEMPOOL-MIB의 cempMemPoolTable이 지원됩니다. 이는 매니지드 시스템의 모든 물리적 엔티티에 대한 항목을 모니터링하는 메모리 풀의 테이블입니다. 참고 CISCO-ENHANCED-MEMPOOL-MIB는 64비트 카운터를 사용하고 4GB 이상의 RAM을 사용하는 플랫폼에서 메모리 보고 기능을 지원합니다.
PTP(Precision Time Protocol)에 대한 E2E 투명 클록 모드 MIB를 지원합니다.	9.7(1)	E2E 투명 클록 모드에 해당하는 MIB가 이제 지원됩니다. 참고 SNMP get, bulkget, getnext, walk 작업만 지원됩니다.
IPv6를 통한 SNMP	9.9(2)	이제 ASA에서는 IPv6를 통한 SNMP 서버와의 통신, IPv6를 통한 쿼리 및 트랩 실행, 기존 MIB에 대한 IPv6 주소 지원을 비롯하여 IPv6를 통한 SNMP를 지원합니다. RFC 8096에 설명된 대로 다음과 같은 새로운 SNMP IPv6 MIB 개체가 추가되었습니다. • ipv6InterfaceTable(OID: 1.3.6.1.2.1.4.30) — 인터페이스별 IPv6 특정 정보를 포함합니다. • ipAddressPrefixTable(OID:1.3.6.1.2.1.4.32) — 이 엔티티에서 확인한 모든 접두사를 포함합니다. • ipAddressTable(OID: 1.3.6.1.2.1.4.34) — 엔티티의 인터페이스와 관련된 주소 지정 정보를 포함합니다. • ipNetToPhysicalTable(OID: 1.3.6.1.2.1.4.35) — IP 주소에서 실제 주소로의 매핑을 포함합니다. 신규 또는 수정된 명령: **snmp-server host** 참고 **snmp-server host-group** 명령은 IPv6를 지원하지 않습니다. 신규 또는 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**

기능 이름	버전	설명
SNMP 워크 작업 중 사용 가능한 메모리 및 사용된 메모리 통계에 대한 결과 활성화 및 비활성화 지원	9.10(1)	CPU 리소스의 과도한 사용을 방지하기 위해 SNMP 워크 작업을 통해 수집된 사용 여유 메모리 및 사용 중인 메모리 통계의 쿼리를 활성화하거나 비활성화할 수 있습니다. 신규 또는 수정된 명령: **snmp-server enable oid** ASDM 화면은 수정하지 않았습니다.
SNMP 워크 작업 중 사용 가능한 메모리 및 사용된 메모리 통계에 대한 결과 활성화 및 비활성화 지원	9.12(1)	CPU 리소스의 과도한 사용을 방지하기 위해 SNMP 워크 작업을 통해 수집된 사용 여유 메모리 및 사용 중인 메모리 통계의 쿼리를 활성화하거나 비활성화할 수 있습니다. 명령은 수정하지 않았습니다. 신규 또는 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**
SNMPv3 인증	9.14(1)	이제 사용자 인증에 SHA-256 HMAC를 사용할 수 있습니다. 신규/수정된 명령: **snmp-server user** 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**
9.14(1) 이상의 장애 조치 쌍의 경우 ASA는 더 이상 SNMP 클라이언트 엔진 데이터를 피어와 공유하지 않습니다.	9.14(1)	ASA는 더 이상 SNMP 클라이언트 엔진 데이터를 피어와 공유하지 않습니다.
사이트 간 VPN을 통한 SNMP 폴링	9.14(2)	사이트 간 VPN을 통한 보안 SNMP 폴링의 경우, VPN 구성의 일부로 암호화 맵 access-list에 외부 인터페이스의 IP 주소를 포함합니다.
CISCO-MEMORY-POOL-MIB OID에 대한 지원이 더 이상 제공되지 않습니다.	9.15(1)	CISCO-MEMORY-POOL-MIB OID(ciscoMemoryPoolUsed, ciscoMemoryPoolfree)는 64비트 카운터를 사용하는 시스템에서 더 이상 사용되지 않습니다. CISCO-ENHANCED-MEMPOOL-MIB의 cempMemPoolTable은 64비트 카운터를 사용하는 시스템에 대한 메모리 풀 모니터링 항목을 제공합니다.
SNMPv3 인증	9.16(1)	이제 사용자 인증에 SHA-224 및 SHA-384를 사용할 수 있습니다. 사용자 인증에 MD5를 더 이상 사용할 수 없습니다. 암호화 에 DES를 더 이상 사용할 수 없습니다. 신규/수정된 명령: **snmp-server user** 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Management Access(**관리 액세스**)** > **SNMP**
IPv6를 통한 SNMP	9.17(1)	**snmp-server host-group** 명령 은 이제 IPv6 호스트, 범위 및 서브넷 개체를 지원합니다.

기능 이름	버전	설명
SNMP에 대한 루프백 인터페이스 지원	9.18(2)	이제 루프백 인터페이스를 추가하여 SNMP에 사용할 수 있습니다. 신규/수정된 명령: **interface loopback**, **snmp-server host** 신규/수정된 화면: **Configuration(**구성**)** > **Device Setup(**디바이스 설정**)** > **Interface Settings(**인터페이스 설정**)** > **Interfaces(**인터페이스**)** > **Add Loopback Interface(**루프백 인터페이스 추가**)** 7.19에 ASDM 지원이 추가되었습니다.
SNMP MIB 및 트랩	9.20(1)	Secure Firewall 4200 모델 디바이스(FPR4215, FPR4225, FPR4245)가 SNMP sysObjectID OID 및 entPhysicalVendorType OID 테이블에 새 제품으로 추가되었습니다. 이러한 Secure Firewall 4200 Series 디바이스의 2개의 EPM 카드(4X200G 및 2X100G)에 대한 SNMP 지원이 추가되었습니다.