SNMP

本章介绍如何配置简单网络管理协议 (SNMP) 来监控 ASA。

关于 SNMP

SNMP 是促进网络设备之间的管理信息交换的应用层协议，并且是 TCP/IP 协议套件的一部分。ASA 使用 SNMP 第 1、2c 和 3 版为网络监控提供支持，并且支持同时使用所有三个版本。利用在 ASA 接口上运行的 SNMP 代理，您可以通过诸如 HP OpenView 之类的网络管理系统 (NMS) 监控网络设备。ASA 通过发出 GET 请求来支持 SNMP 只读访问。不允许 SNMP 写访问，因此您无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

您可以将 ASA 配置为向 NMS 发送陷阱，即针对特定事件从托管设备发送到管理站的未经请求的消息（事件通知），也可以使用 NMS 浏览安全设备上的管理信息库 (MIB)。MIB 是定义的集合，而 ASA 维护由每个定义的值组成的数据库。浏览 MIB 意味着从 NMS 发出 MIB 树的一系列 GET-NEXT 或 GET-BULKGET 请求以确定值。

注释 对于密集型工作负载，部署超过 10 个 NMS 可能会影响设备的性能。为确保设备的稳定性和响应速度，我们建议您谨慎使用 NMS 进行 SNMP 漫游轮询和管理陷阱流量。

ASA 具有 SNMP 代理，用于在发生预定义为需要通知（例如，当网络中的链路开启或关闭时）的事件的情况下通知指定的管理站。它发送的通知包括用于向管理站表明其自身身份 SNMP OID。ASA 代理还会在管理站请求信息时进行回复。

SNMP 术语

下表列出在使用 SNMP 时常用的术语。

表 *1: SNMP* 术语

术语	说明
代理	在 ASA 上运行的 SNMP 服务器。SNMP 代理具有以下功能： • 对来自网络管理站的信息和操作请求作出响应。 • 控制对其管理信息库（即 SNMP 可以查看或更改的对象的集合）的访问。 • 不允许 SET 操作。
浏览	通过从设备上的 SNMP 代理轮询所需信息来从网络管理站监控该设备的运行状况。此活动可能包括从网络管理站发出 MIB 树的一系列 GET-NEXT 或 GET-BULK 请求以确定值。
管理信息库 (MIB)	用于收集有关数据包、连接、缓冲区、故障转移等的信息的标准化数据结构。MIB 由大多数网络设备使用的产品、协议和硬件标准来定义。SNMP 网络管理站可以浏览 MIB，并请求在出现特定数据或事件时将其发送。
网络管理站 (NMS)	设置 PC 或工作站是为了监控 SNMP 事件和管理设备，例如 ASA。
对象标识符 (OID)	用于向设备的 NMS 表明该设备的身份并向用户指示监控和显示的信息源的系统。
陷阱	用于生成从 SNMP 代理到 NMS 的消息的预定义事件。事件包括警报条件，例如链路开启、链路关闭、冷启动、热启动、身份验证或系统日志消息。

MIB 和陷阱

MIB 特定于标准或特定于企业。标准 MIB 由 IETF 创建并记录在各种 RFC 中。陷阱报告发生在网络设备上的重大事件，大多数情况下是错误或故障。SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 ASA 软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

从以下位置浏览思科 MIB、陷阱和 OID 的完整列表：

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

此外，从以下位置通过 FTP 下载思科 OID：

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

注释 在软件 7.2(1) 版、8.0(2) 版及更高版本中，通过 SNMP 访问的接口信息大约每 5 秒刷新一次。因此，我们建议在连续的轮询之间等待至少 5 秒。

在 MIB 中，并非所有 OID 都受支持。要获取特定 ASA 的受支持 SNMP MIB 和 OID 的列表，请输入以下命令：

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

注释 尽管 **oidlist** 关键字没有显示在 **show snmp-server** 命令的选项列表中，但它是可用的。但是，此命令仅供思科 TAC 使用。使用此命令之前，请联系思科 TAC。

以下是 **show snmp-server oidlist** 命令的输出示例:

```
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--
```

有关受支持 SNMP MIB 和 OID 的完整列表，请参阅 SNMP MIBs and OIDs.

SNMP 对象标识符

每个思科系统级产品都具有供用作 MIB-II sysObjectID 的 SNMP 对象标识符 (OID)。CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 包括可在 SNMPv2-MIB、Entity Sensor MIB 和 Entity Sensor Threshold Ext MIB 内的 sysObjectID 对象中报告的 OID。您可以使用此值标识型号。下表列出了不同型号 ASA 和 ISA 的 sysObjectID OID。

表 *2: SNMP* 对象标识符

产品标识符	**sysObjectID**	型号编号
ASA Virtual	ciscoASAv (ciscoProducts 1902)	思科自适应安全虚拟设备 (ASA Virtual)
ASA Virtual 系统情景	ciscoASAvsy (ciscoProducts 1903)	思科自适应安全虚拟设备 (ASA Virtual) 系统情景
ASA Virtual 安全情境	ciscoASAvsc (ciscoProducts 1904)	思科自适应安全虚拟设备 (ASA Virtual) 安全情景.

产品标识符	sysObjectID	型号编号
Cisco Secure Firewall 4200	ciscoFpr4215td (ciscoProducts 3043) ciscoFpr4225td (ciscoProducts 3042) ciscoFpr4245td (ciscoProducts 3041)	FPR4215, FPR4225, FPR4245
ISA 30004C 工业安全设备	ciscoProducts 2268	ciscoISA30004C
带有 4 GE 铜缆安全情景的思科 ISA30004C	ciscoProducts 2139	ciscoISA30004Csc
带有 4 GE 铜缆系统情景的思科 ISA30004C	ciscoProducts 2140	ciscoISA30004Csy
ISA 30002C2F 工业安全设备	ciscoProducts 2267	ciscoISA30002C2F
带有 2 GE 铜缆端口 + 2 GE 光纤安全情景的思科 ISA30002C2F	ciscoProducts 2142	ciscoISA30002C2Fsc
带有 2 GE 铜缆端口 + 2 GE 光纤系统情景的思科 ISA30002C2F	ciscoProducts 2143	ciscoISA30002C2Fsy
思科工业安全设备 (ISA) 30004C 机箱	cevChassis 1677	cevChassisISA30004C
思科工业安全设备 (ISA) 30002C2F 机箱	cevChassis 1678	cevChassisISA30002C2F
适用于 ISA30004C 铜缆 SKU 的中央处理单元温度传感器	cevSensor 187	cevSensorISA30004CCpuTempSensor
适用于 ISA30002C2F 光纤的中央处理单元温度传感器	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
适用于 ISA30004C 铜缆 SKU 的处理器卡温度传感器	cevSensor 192	cevSensorISA30004CPTS
适用于 ISA30002C2F 光纤 SKU 的处理器卡温度传感器	cevSensor 193	cevSensorISA30002C2FPTS
适用于 ISA30004C 铜缆 SKU 的电源卡温度传感器	cevSensor 197	cevSensorISA30004CPowercardTS
适用于 ISA30002C2F 光纤 SKU 的电源卡温度传感器	cevSensor 198	cevSensorISA30002C2FPowercardTS
适用于 ISA30004C 的端口卡温度传感器	cevSensor 199	cevSensorISA30004CPortcardTS
适用于 ISA30002C2F 的端口卡温度传感器	cevSensor 200	cevSensorISA30002C2FPortcardTS

产品标识符	sysObjectID	型号编号
适用于 ISA30004C 铜缆 SKU 的中央处理单元	cevModuleCpuType 329	cevCpuISA30004C
适用于 ISA30002C2F 光纤 SKU 的中央处理单元	cevModuleCpuType 330	cevCpuISA30002C2F
模块 ISA30004C、ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C 工业安全设备固态硬盘	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
30002C2F 工业安全设备固态硬盘	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
思科 ISA30004C/ISA30002C2F 硬件旁路	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
FirePOWER 4140 安全设备，1U，带有内置安全模块 36	ciscoFpr4140K9 (ciscoProducts 2293)	FirePOWER 4140
FirePOWER 4120 安全设备，1U，带有内置安全模块 24	ciscoFpr4120K9 (ciscoProducts 2294)	FirePOWER 4120
FirePOWER 4K 风扇槽位	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K 电源槽位	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Cisco Secure Firewall Threat Defense Virtual、VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Firewall Threat Defense Virtual、AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

物理供应商类型值

每个思科机箱或独立系统都具有供 SNMP 使用的唯一类型编号。entPhysicalVendorType OID 在 CISCO-ENTITY-VENDORTYPE-OID-MIB 中进行定义。此值在 ASA、 ASA Virtual或 ASASM SNMP 代理的 entPhysicalVendorType 对象中返回。您可以使用此值标识组件的类型（模块、电源、风扇、传感器、CPU 等）。下表列出用于各型号 ASA 的物理供应商类型值。

表 *3:* 物理供应商类型值

项目	entPhysicalVendorType OID 说明
千兆以太网端口	cevPortGe (cevPort 109)
思科自适应安全虚拟设备	cevChassisASAv (cevChassis 1451)
Cisco Secure Firewall 4200-X (FPR4215/FPR4225/FPR4245)	cevFPRNM4X200Gng 和 cevFPRNM2X100Gng（为插槽 2 和插槽 3 添加的双 EPM 2X100G 和 4X200G）

MIB 中支持的表格和对象

下表列出对指定 MIB 支持的表和对象。

在多情景模式下，这些表和对象提供单个情景的信息。如果需要跨情景的数据，则需要对它们求和。例如，要获取整体内存使用率，请对每个情景的cempMemPoolHCUsed值求和。

表 *4: MIB* 中支持的表格和对象

MIB 名称和 OID	支持的表和对象
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。 对于 32 位内存系统，使用 32 位内存计数器进行轮询—cempMemPoolUsed、 cempMemPoolFree、cempMemPoolUsedOvrflw、 cempMemPoolFreeOvrflw、cempMemPoolLargestFree、 cempMemPoolLowestFree、cempMemPoolUsedLowWaterMark、 cempMemPoolAllocHit、cempMemPoolAllocMiss、 cempMemPoolFreeHit、cempMemPoolFreeMiss、 cempMemPoolLargestFreeOvrflw、cempMemPoolLowestFreeOvrflw、cempMemPoolUsedLowWaterMarkOvrflw、cempMemPoolSharedOvrflw。 对于 64 位内存系统，使用 64 位内存计数器进行轮询 - cempMemPoolHCUsed、cempMemPoolHCFree、cempMemPoolHCLargestFree、cempMemPoolHCLowestFree、cempMemPoolHCUsedLowWaterMark、cempMemPoolHCShared
CISCO-REMOTE-ACCESS-MONITOR-MIB; OID:1.3.6.1.4.1.9.9.392 注释 这三个MIB OID可用于跟踪远程访问连接失败的原因。	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 注释 ASA Virtual上不支持。	ctsxSxpGlobalObjects、ctsxSxpConnectionObjects、ctsxSxpSgtObjects

MIB 名称和 OID	支持的表和对象
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 注释 提供与物理传感器相关的信息，例如机箱温度，风扇RPM，电源电压等。 ASA Virtual 平台不支持。	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 注释 只有与 E2E 透明时钟模式对应的 MIB 受支持。	ciscoPtpMIBSystemInfo、cPtpClockDefaultDSTable、cPtpClockTransDefaultDSTable、cPtpClockPortTransDSTable
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 至 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	cpmCPUTotal1minRev cpmCPUTotal1minRev 的关联参数和值 示例： • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) - 聚合系统 CPU 使用率百分比（此值与单情景模式下 .3.6.1.4.1.9.9.109.1.1.1.1.7.1 中的系统 CPU 使用率相同）。 • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) - Snort 平均 CPU 使用率百分比（所有 snort 实例的总值） • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) - 系统进程平均百分比（“Sysproc”核心的平均值）

支持的陷阱（通知）

下表列出支持的陷阱（通知）及其关联 MIB。

表 *5:* 支持的陷阱（通知）

陷阱和 **MIB** 名称	**Varbind** 列表	说明
authenticationFailure (SNMPv2-MIB)	-	对于 SNMP 第 1 版或第 2 版，SNMP 请求中提供的社区字符串不正确。对于 SNMP 第 3 版，如果 auth 或 priv 关键字或用户名不正确，则会生成报告 PDU 而不是陷阱。 **snmp-server enable traps snmp authentication** 命令用于启用和禁用这些陷阱的传输。
bgpBackwardTransition	bgpPeerLastError、bgpPeerState	**snmp-server enable traps peer-flap** 命令用于启用此陷阱的传输。
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	ccmHistoryRunningLastChanged、ccmHistoryEventTerminalType	**snmp-server enable traps config** 命令用于启用此陷阱的传输。
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-insert** 命令用于启用此通知。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-remove** 命令用于启用此通知。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)	entPhysicalName、 entPhysicalDescr、 entPhySensorValue、 entPhySensorType、 ceSensorExtThresholdValue	**snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] 命令用于启用实体阈值通知的传输。系统会针对电源故障发送此通知。所发送的对象会识别风扇和 CPU 温度。 **snmp-server enable traps entity fan-failure** 命令用于启用风扇故障陷阱的传输。此陷阱不适用于 Firepower 2100 系列。 **snmp-server enable traps entity power-supply-failure** 命令用于启用电源故障陷阱的传输。此陷阱不适用于 Firepower 2100 系列。 **snmp-server enable traps entity chassis-fan-failure** 命令用于启用机箱风扇故障陷阱的传输。 **snmp-server enable traps entity cpu-temperature** 命令用于启用高CPU温度陷阱的传输。此陷阱不适用于 Firepower 2100 系列。 **snmp-server enable traps entity power-supply-presence** 命令用于启用电源状态故障陷阱的传输。 **snmp-server enable traps entity power-supply-temperature** 命令用于启用电源温度阈值陷阱的传输。 **snmp-server enable traps entity chassis-temperature** 命令用于启用机箱环境温度陷阱的传输。此陷阱不适用于 Firepower 2100 系列。 **snmp-server enable traps entity accelerator-temperature** 命令用于启用机箱加速器温度陷阱的传输。
cikeTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunLifeTime	**snmp-server enable traps ikev2 start** 命令用于启用此陷阱的传输。
cikeTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunActiveTime	**snmp-server enable traps ikev2 stop** 命令用于启用此陷阱的传输。
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	**snmp-server enable traps ipsec start** 命令用于启用此陷阱的传输。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** 命令用于启用此陷阱的传输。
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	ccmHistoryEventCommandSource, ccmHistoryEventConfigSource, ccmHistoryEventConfigDestination	**snmp-server enable traps config** 命令用于启用此陷阱的传输。
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions、 crasNumUsers、 crasMaxSessionsSupportable、 crasMaxUsersSupportable、 crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** 命令用于启用这些陷阱的传输。
ciscoUFwFailoverStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	gid, FOStatus	**snmp-server enable traps failover-state** 命令用于启用此陷阱的传输。
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility、 clogHistSeverity、 clogHistMsgName、 clogHistMsgText、 clogHistTimestamp	系统将生成系统日志消息。 clogMaxSeverity 对象的值用于决定哪些系统日志消息作为陷阱发送。 **snmp-server enable traps syslog** 命令用于启用和禁用这些陷阱的传输。
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType、 crlResourceLimitMax、 clogOriginIDType、clogOriginID	**snmp-server enable traps connection-limit-reached** 命令用于启用 connection-limit-reached 通知的传输。clogOriginID 对象包括陷阱源于的情景名称。
coldStart (SNMPv2-MIB)	-	配置 SNMP 后，SNMP 代理启动时发生的 coldStart 陷阱。当代理在系统重启后启动时，也会出现此陷阱。 **注释** 对于集群和HA节点，重载后，如果接口重启时间超过5分钟（预设阈值），陷阱就会被丢弃。当集群和HA节点重启成功后，所有其他陷阱都会按预期发送。 **snmp-server enable traps snmp coldstart** 命令用于启用和禁用这些陷阱的传输。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue、cpmCPUTotalMonIntervalValue、cpmCPUInterruptMonIntervalValue、cpmCPURisingThresholdPeriod、cpmProcessTimeCreated、cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** 命令用于启用 CPU threshold rising 通知的传输。cpmCPURisingThresholdPeriod 对象与其他对象一起发送。
cufwClusterStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	status	**snmp-server enable traps cluster-state** 命令用于启用此陷阱的传输。
entConfigChange (ENTITY-MIB)	-	**snmp-server enable traps entity config-change fru-insert fru-remove** 命令用于启用此通知。 注释 仅当创建或删除了安全情景时，才会以多模方式发送此通知。
linkDown (IF-MIB)	ifIndex、ifAdminStatus、ifOperStatus	接口的链路关闭陷阱。 **snmp-server enable traps snmp linkdown** 命令用于启用和禁用这些陷阱的传输。
linkUp (IF-MIB)	ifIndex、ifAdminStatus、ifOperStatus	接口的链路开启陷阱。 **snmp-server enable traps snmp linkup** 命令用于启用和禁用这些陷阱的传输。
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、cempMemPoolName、cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** 命令用于启用内存阈值通知。mteHotOID 设置为 cempMemPoolHCUsed。cempMemPoolName 和 cempMemPoolHCUsed 对象与其他对象一起发送。
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、ifHCInOctets、ifHCOutOctets、ifHighSpeed、entPhysicalName	**snmp-server enable traps interface-threshold** 命令用于启用接口阈值通知。entPhysicalName 对象将与其他对象一起发送。
natPacketDiscard (NAT-MIB)	ifIndex	**snmp-server enable traps nat packet-discard** 命令用于启用 NAT 数据包丢弃通知。此通知会受到时长为 5 分钟的速率限制，并且是在 IP 数据包因映射空间不可用而被 NAT 丢弃的情况下生成。ifIndex 提供映射接口的 ID。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
ospfNbrStateChange	ospfRouterId, ospfNbrIpAddr, ospfNbrAddressLessIndex, ospfNbrRtrId, ospfNbrState	**snmp-server enable traps peer-flap** 命令用于启用此陷阱的传输。 注释 对于 ASA5585 型号，SNMP 引擎已更改为使用 netsnmp 5.8 版库，库中不提供以下 OID： • ospfIfStateChange 1.3.6.1.2.1.14.16.2.16 • ospfVirtIfStateChange 1.3.6.1.2.1.14.16.2.1 • ospfVirtNbrStateChange 1.3.6.1.2.1.14.16.2.3
warmStart (SNMPv2-MIB)	-	SNMP 代理首次重启时发出的 warmStart 陷阱。当代理在 SNMP 配置更改后重新启动时，所有 SNMP 主机配置都会被移除，并重新进行 SNMP 配置，这时也会出现此陷阱。 **snmp-server enable traps snmp warmstart** 命令用于启用和禁用这些陷阱的传输。

接口类型和示例

产生 SNMP 流量统计信息的接口类型包括：

- 逻辑 - 由软件驱动程序收集的统计信息，它是物理统计信息的子集。
- 物理 - 由硬件驱动程序收集的统计信息。每个物理指定接口具有一组与其关联的逻辑和物理统计信息。每个物理接口可能具有多个与其关联的 VLAN 接口。VLAN 接口仅具有逻辑统计信息。

注释 对于具有多个与其关联的 VLAN 接口的物理接口，请注意，ifInOctets OID 和 ifOutoctets OID 的 SNMP 计数器会与该物理接口的汇聚流量计数器相匹配。

- VLAN 专用 - SNMP 使用 ifInOctets 和 ifOutOctets 的逻辑统计信息。

下表中的示例显示 SNMP 流量统计信息中的差异。示例 1 显示对于 **show interface** 命令和 **show traffic** 命令而言物理与逻辑输出统计信息中的差异。示例 2 显示对于 **show interface** 命令和 **show traffic** 命令而言 VLAN 专用接口的输出统计信息。示例表明统计信息接近于为 **show traffic** 命令显示的输出。

表 *6:* 物理接口和 ***VLAN*** 接口的 ***SNMP*** 流量统计信息

示例 1	示例 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 以下示例显示管理接口和物理接口的 SNMP 输出统计信息。ifInOctets 值接近于 **show traffic** 命令输出中显示的物理统计信息输出，但不接近于逻辑统计信息输出。 管理接口的 ifIndex： IF_MIB::ifDescr.6 = Adaptive Security Appliance ‘mgmt’ interface 对应于物理接口 统计信息的 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 VLAN 内部的 ifIndex： IF-MIB::ifDescr.9 = Adaptive Security Appli **IF-MIB::ifInOctets.9 = Counter32: 126318**

SNMP 第 3 版概述

SNMP 第 3 版提供第 1 版或第 2c 版中没有的安全增强功能。SNMP 第 1 版和第 2c 版以明文形式在 SNMP 服务器和 SNMP 代理之间传输数据。SNMP 第 3 版向安全协议操作中添加了身份验证和隐私选项。此外，此版本通过基于用户的安全模式 (USM) 和基于视图的访问控制模式 (VACM) 控制对 SNMP 代理和 MIB 对象的访问。ASA 还支持创建 SNMP 组和用户，以及为安全 SNMP 通信启用传输身份验证和加密所需的主机。

安全模型

为进行配置，身份验证和隐私选项会共同组成安全模式。安全模式应用于用户和组，它们分为以下三种类型：

- NoAuthPriv - 无身份验证且无隐私，意味着未对消息应用安全设置。
- AuthNoPriv - 有身份验证但无隐私，意味着消息会进行身份验证。
- AuthPriv - 有身份验证并有隐私，意味着消息会进行身份验证并加密。

SNMP 组

SNMP 组是可以将用户添加到的访问控制策略。每个 SNMP 组配置有安全模式，并与 SNMP 视图关联。SNMP 组内的用户必须与 SNMP 组的安全模式匹配。这些参数指定 SNMP 组内的用户使用的身份验证和隐私类型。每个 SNMP 组名称/安全模式对必须唯一。

SNMP 用户

SNMP 用户具有指定的用户名、用户所属的组、身份验证密码、加密密码，以及要使用的身份验证和加密算法。身份验证算法选项包括 SHA-1、SHA-224、SHA-256 HMAC 和 SHA-384。加密算法选项为 3DES 和 AES（在 128、192 和 256 版中可用）。创建用户时，必须将其与 SNMP 组相关联。然后，用户将继承该组的安全模式。

注释 配置 SNMP v3 用户账户时，请确保身份验证算法的长度等于或大于加密算法的长度。

SNMP 主机

SNMP 主机是 SNMP 通知和陷阱所发送到的 IP 地址。要配置 SNMP 第 3 版主机及目标 IP 地址，必须配置用户名，因为陷阱仅发送到已配置的用户。SNMP 目标 IP 地址和目标参数名称在 ASA 上必须唯一。每个 SNMP 主机只能具有一个与其关联的用户名。要接收 SNMP 陷阱，请在添加 **snmp-server host** 命令后，确保将 NMS 上的用户凭证配置为与 ASA 的凭证相匹配。

注释 最多可以添加 8192 台主机。但是，其中仅 128 台可用于陷阱。

ASA 和思科 IOS 软件之间的实施差异

ASA 中的 SNMP 第 3 版实施在以下方面不同于思科 IOS 软件中的 SNMP 第 3 版实施：

- 本地引擎和远程引擎 ID 为不可配置。本地引擎 ID 是在 ASA 启动时或者创建了情景时生成。
- 不支持基于视图的访问控制，导致 MIB 浏览不受限制。
- 支持限于以下 MIB：USM、VACM、FRAMEWORK 和 TARGET。
- 您必须使用正确的安全模式创建用户和组。
- 您必须按正确的顺序删除用户、组和主机。
- 使用 snmp - server host 命令创建 ASA 规则以允许传入 SNMP 流量。

SNMP 系统日志消息传递

SNMP 生成编号为 212*nnn* 的详细系统日志消息。系统日志消息向指定接口上的指定主机表明 SNMP 请求、SNMP 陷阱、SNMP 信道和来自 ASA 或 ASASM 的 SNMP 响应的状态。

有关系统日志消息的详细信息，请参阅系统日志消息指南。

注释 如果 SNMP 系统日志消息超过较高的速率（约 4000 条/秒），则 SNMP 轮询将失败。

应用服务和第三方工具

有关 SNMP 支持的信息，请参阅以下 URL：

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

有关使用第三方工具处理 SNMP 第 3 版 MIB 的信息，请参阅以下 URL：

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

SNMP 准则

本节介绍您在配置 SNMP 之前应查看的准则和限制。

故障转移和集群准则

- 将 SNMPv3 用于集群或故障转移时，如果在初始集群形成后添加新的集群设备或更换故障转移设备，则SNMPv3用户不会复制到新设备。您必须将SNMPv3用户重新添加到控制/主用设备，以强制用户复制到新设备；或者，也可以直接在新设备上添加用户（SNMPv3 用户和组是无法在集群数据设备上输入配置命令的规则的例外）。重新配置每个用户，方法是在控制/主用设备上输入 **snmp-server user***username group-name***v3** 命令，或者直接使用未加密形式的 *priv-password* 选项和 *auth-password* 选项连接到数据/备用设备。

IPv6 准则（所有 ASA 型号）

可以通过 IPv6 传输来配置 SNMP，以便 IPv6 主机能够执行 SNMP 查询，并从运行 IPv6 软件的设备接收 SNMP 通知。SNMP 代理和相关的 MIB 已进行增强，以支持 IPv6 寻址。

IPv6 Firepower 2100 准则

Firepower 2100 运行名为 FXOS的底层操作系统，并同时支持设备模式（默认）和平台模式；请参阅将 Firepower 2100 设置为设备或平台模式。

在平台模式下时，必须在 FXOS 中配置 IPv6 管理 IP 地址。以下示例配置 IPv6 管理接口和网关：

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
```

```
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
IPv6 Address Prefix IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

其他准则

- 在设备模式下运行的系统不会发出电源陷阱。
- 对于平台模式下的 Firepower 2100，无法轮询 EtherChannel 的成员接口，并且不会生成成员接口的陷阱。如果直接在 FXOS 中启用 SNMP，则支持此功能。设备模式不受影响。
- 对于平台模式下的 Firepower 2100，不支持单个端口成员的 ASA 陷阱；请参阅 思科 Firepower 2100 FXOS MIB 参考指南。
- 对于设备模式下的 Firepower 2100，无法轮询硬件型号和序列号，并且在 ASA 中不会为这些详细信息生成陷阱。因此，请在 FXOS 或机箱管理器上配置 SNMP 以轮询机箱管理 IP 而不是 ASA 实例上的接口。
- 您必须具有 Cisco Works for Windows 或其他符合 SNMP MIB-II 标准的浏览器才能接收 SNMP 陷阱或浏览 MIB。
- SNMP 不支持通过 VPN 隧道进行管理访问（**management-access** 命令）。 对于基于 VPN 的 SNMP，我们建议在环回接口上启用 SNMP。您无需启用管理访问功能即可在环回接口上使用 SNMP。环回接口也适用于 SSH。
- 不支持基于视图的访问控制，但是 VACM MIB 可供浏览以确定默认视图设置。
- ENTITY-MIB 在非管理情景中不可用。在非管理情景中改用 IF-MIB 执行查询。
- ENTITY-MIB 对 Firepower 9300不可用。相反，请使用 CISCO-FIREPOWER-EQUIPMENT-MIB 和 CISCO-FIREPOWER-SM-MIB。
- 在某些设备上，观察到 **snmpwalk** 输出中的接口 (ifDescr) 顺序在重新启动后发生变化。ASA 使用一种算法来确定 SNMP 查询的 ifIndex 表。当 ASA 启动时，接口将按 ASA 读取配置时加载的顺序添加到 ifIndex 表中。添加到 ASA 的新接口会附加到 ifIndex 表中的接口列表。随着接口的添加，删除或重命名，可能会影响重新启动时接口的顺序。
- 在 **snmpwalk** 命令中提供 OID 时，snmpwalk 工具会查询子树中指定 OID 下的所有变量并显示其值。因此，要查看设备上对象的全面输出，请确保在 **snmpwalk** 命令中提供 OID。
- 对于 AIP SSM 或 AIP SSC 不支持 SNMP 第 3 版。
- 不支持 SNMP 调试。
- 不支持 ARP 信息检索。
- 不支持 SNMP SET 命令。

- 使用 NET-SNMP 第 5.4.2.1 版时，仅支持 AES128 加密算法版本。不支持 AES256 或 AES192 加密算法版本。
- 如果结果导致 SNMP 处于不一致状态，则会对现有配置进行更改。
- 对于 SNMP 第 3 版，必须按以下顺序进行配置：组、用户、主机。
- 对于 Firepower 2100，当通过设备管理接口配置 SNMPv3 时，所有 SNMPv3 用户都可以轮询设备，即使它们未在主机配置中进行映射。
- 对于 Cisco Secure Firewall 模型， **snmpwalk** 命令仅从管理情景轮询 FXOS mib。
- 在删除组之前，您必须确保删除与该组关联的所有用户。
- 在删除用户之前，您必须确保未配置与该用户名关联的主机。
- 如果已使用特定安全模式将用户配置为属于特定组，并且如果该组的安全级别进行了更改，则必须按此顺序执行以下操作：
  - 从该组中删除用户。
  - 更改组安全级别。
  - 添加属于新组的用户。
- 不支持创建自定义视图来限制对 MIB 对象子集的用户访问。
- 所有的请求和陷阱只能在默认的 Read/Notify View 中获取。
- 在管理情景中生成 connection-limit-reached 陷阱。要生成此陷阱，您必须在已达到连接限制的用户情景中配置至少一个 SNMP 服务器主机。
- 您最多可以添加 4000 台主机。但是，其中仅 128 台可用于陷阱。
- 支持的活动轮询目标总数为 128。
- 您可以指定网络对象以指示要添加为主机组的个别主机。
- 您可以将多个用户与一台主机关联。
- 您可以在不同的 **host-group** 命令中指定重叠网络对象。为最后一个主机组指定的值会对不同网络对象中的公用主机集合生效。
- 如果删除主机组或与其他主机组重叠的主机，则系统会使用所配置的主机组中已指定的值再次设置主机。
- 主机获取的值取决于用于运行命令的指定序列。
- SNMP 发送的消息大小的限制为 1472 字节。
- ASA 支持每个情景的 SNMP 服务器陷阱主机数不受限制。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。

故障排除提示

- 要确保接收来自 NMS 的传入数据包的 SNMP 进程，请输入以下命令：

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

- 要捕获来自 SNMP 的系统日志消息并将其显示在 ASA 控制台上，请输入以下命令：

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

- 要确保 SNMP 进程正在发送和接收数据包，请输入以下命令：

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

  输出基于 SNMPv2-MIB 的 SNMP 组。

- 要确保 SNMP 数据包通过 ASA 并指向 SNMP 进程，请输入以下命令：

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

- 如果 NMS 无法成功请求对象或者未正确处理来自 ASA 的传入陷阱，请使用数据包捕获确定问题，方法是输入以下命令：

```
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
```

- 如果 ASA 不按预期执行，请通过执行以下操作来获取有关网络拓扑和流量的信息：
  - 对于 NMS 配置，请获取以下信息：

    超时次数

    重试计数

    引擎 ID 缓存

    使用的用户名和密码

  - 发出以下命令：

    show block

    show interface

    show process

    show cpu

    show vm

- 如果发生严重错误，如要帮助重现错误，请将回溯文件和 **show tech-support** 命令的输出发送到思科 TAC。
- 如果不允许 SNMP 流量通过 ASA 接口，您可能还需要使用 **icmp permit** 命令允许来自远程 SNMP 服务器的 ICMP 流量。
- 如果您使用 **snmp-server enable oid** 配置了设备，在执行 SNMP 漫游操作时，ASA 将查询 MEMPOOL_DMA 和 MEMPOOL_Global_SHARED 池中的内存信息。这可能会导致与SNMP相关的CPU消耗导致丢包。要缓解此问题，请避免使用 **no snmp-server enable oid** 命令轮询与全局共享池相关的 OID。禁用时，内存池 OID 将返回 0 字节。
- 当您在一个请求中使用 SNMPGET 对大量 OID 进行轮询 ASP 丢弃计数器时，需要重复轮询 ASP 丢弃计数器，而这会导致更高的 CPU 占用率。因此，我们建议您确定要监控的重要计数器，并在每个计数器上使用 SNMPGET 来获取这些值，以减少对 CPU 的影响。
- 当在多情景 ASA 的多个情景中配置 SNMP 时，请按顺序轮询情景并使用 SNMPBULKGET 而不是 snmpwalk，以便减少与平台的连接数量。当同时轮询大量情景时，此方法可避免 SNMP 延迟或超时。
- 通过 SNMP 获取响应消息（例如 SNMPBULKGET）响应 SNMP 轮询时，ASA 会一致地设置不分片 (DF) 位，该位要求整个网络路径至少支持中配置的最大传输单位 (MTU) ASA。如果在网络路径上配置了较低的 MTU，其他设备可能会发送请求分片的互联网控制消息协议 (ICMP) 数据包。但是，由于 DF 位已设置，因此 ASA 不应答也不将数据包分片，从而导致 ASA 缺少响应。

  要解决此问题，您可以修改 ASA 上或整个网络路径中的 MTU，使用多个获取请求而不是 SNMPBULKGET，或者减小 SNMPBULKGET 请求中的批量大小。
- 有关更多故障排除信息，请参阅以下 URL：
  http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

配置 SNMP

本节介绍如何配置 SNMP。

过程

步骤 1 启用 SNMP 代理和 SNMP 服务器。

步骤 2 配置 SNMP 陷阱。

步骤 3 配置 SNMP 第 1 版和第 2c 版参数或 SNMP 第 3 版参数。

启用 SNMP 代理和 SNMP 服务器

要启用 SNMP 代理和 SNMP 服务器，请执行以下步骤：

过程

在 ASA 上启用 SNMP 代理和 SNMP 服务器。默认情况下，SNMP 服务器已启用。

snmp-server enable

示例：

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

配置 SNMP 陷阱

要指定 SNMP 代理生成哪些陷阱以及如何将其收集并发送到 NMS，请执行以下步骤：

注释 启用所有 SNMP 或系统日志陷阱时，SNMP 进程可能会消耗代理和网络中的过多资源，导致系统挂起。如果您发现系统延迟、未完成的请求或超，可以选择性地启用 SNMP 和系统日志陷阱。例如，您可以跳过信息系统日志陷阱严重性级别。

过程

将单个陷阱、陷阱集合或所有陷阱发送到 NMS。

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**]

示例：

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

通过此命令可以将系统日志消息作为陷阱发送到NMS。默认配置已启用所有SNMP标准陷阱，如示例所示。要禁用这些陷阱，请使用 **no snmp-server enable traps snmp** 命令。

如果输入此命令而不指定陷阱类型，则默认为 **syslog** 陷阱。默认情况下，会启用 **syslog** 陷阱。默认 SNMP 陷阱随**系统日志**陷阱继续启用。

您需要同时配置 **logging history** 命令和 the **snmp-server enable traps syslog** 命令才能从系统日志 MIB 生成陷阱。

要恢复 SNMP 陷阱的默认启用，请使用 **clear configure snmp-server** 命令。默认情况下会禁用所有其他陷阱。

仅在管理情景中可用的陷阱：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

仅通过管理情景为系统情景中物理连接的接口生成的陷阱：

- **interface-threshold**

在单一模式下，所有其他陷阱在管理情景和用户环境中都可用。

config 陷阱启用 ciscoConfigManEvent 通知和 ccmCLIRunningConfigChanged 通知，在退出配置模式后会生成这些通知。

如果 CPU 使用率大于所配置监控期的所配置阈值，则系统会生成 **cpu threshold rising** 陷阱。

当已用系统情景内存达到总系统内存的 80% 时，系统会从管理情景中生成 **memory-threshold** 陷阱。对于所有其他用户情景，当在该特定情景中已用内存达到总系统内存的 80% 时会生成此陷阱。

某些陷阱不适用于某些硬件型号。使用 ? 代替陷阱关键字来确定哪些陷阱可用于您的设备。例如：

- Firepower 1000 系列 仅支持以下实体陷阱：**chassis-temperature**、**config-change** 和 **cpu-temperature**。

注释
SNMP 不监控电压传感器。

配置 CPU 使用率阈值

要配置 CPU 使用率阈值，请执行以下步骤：

过程

为高 CPU 阈值和阈值监控期配置阈值。

snmp cpu threshold rising *threshold_value monitoring_period*

示例：

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

要清除阈值和 CPU 使用率的监控期间，请使用此命令的 **no** 形式。如果未配置 **snmp cpu threshold rising** 命令，则高阈值级别的默认值为超过 70%，临界阈值级别的默认值为超过 95%。默认监控期设置为 1 分钟。

临界 CPU 阈值级别始终保持在 95%，无法配置。高 CPU 阈值的有效阈值范围为 10% 到 94%。监控期的有效值范围为 1 到 60 分钟。

配置物理接口阀值

要配置物理接口阈值，请执行以下步骤：

过程

配置 SNMP 物理接口的阀值。

snmp interface threshold *threshold_value*

示例：

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

要清除 SNMP 物理接口的阈值，请使用此命令的 **no** 形式。阈值定义为接口带宽利用率的百分比。有效阈值范围为 30% 到 99%。默认值为 70%。

snmp interface threshold 命令仅在管理情景中可用。

物理接口使用情况在单模和多模下受到监控，系统情景中物理接口的陷阱通过管理情景发送。仅物理接口用于计算阈值使用情况。

配置 SNMP 版本 1 或版本 2c 的参数

要配置 SNMP 第 1 版或第 2c 版的参数，请执行以下步骤：

过程

步骤 1 指定 SNMP 通知的接收者，指示从其发送陷阱的接口，并识别可以连接至 ASA 的 NMS 或 SNMP 管理器的名称和 IP 地址。

{interface hostname | ip_address} [|] [community-string] [{|用户名}] [端口] **snmp-server host trappollcommunity version1 2cudp-port**

示例：

```
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 关键字可将 NMS 限制为仅接收陷阱。**poll** 关键字可将 NMS 限制为仅发送请求（轮询）。默认情况下，SNMP 陷阱已启用。默认情况下，UDP 端口为 162。社区字符串是 ASA 与 NMS 之间的共享密钥。密钥是一个区分大小写的值，长度最多为32个字母数字字符。不允许使用空格。默认社区字符串为 public。ASA 使用此密钥确定传入的 SNMP 请求是否有效。例如，您可以使用某社区字符串来指定站点，然后使用同一字符串配置 ASA 和管理站。ASA 使用指定的字符串，并且不会对包含无效社区字符串的请求作出响应。但是，如果 SNMP 监控是通过管理接口而不是诊断接口，则无需 ASA 验证社区字符串即可进行轮询。在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。加密的社区字符串始终由 ASA 生成；您输入的一般是明文形式。

关键字指定用于陷阱和请求（轮询）的SNMP版本。**version** 仅允许使用所选版本与服务器通信。

要在添加 **snmp-server host** 命令后接收陷阱，请确保使用 ASA 上配置的凭证相同的凭证来配置 NMS 上的用户。

步骤 2 设置仅供与 SNMP 第 1 版或第 2c 版配合使用的社区字符串。

snmp-server community *community-string*

示例：

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

注释
您应避免使用特殊字符（！，@, #, $, %, ^, &, *, \) 在社区字符串。通常，使用为操作系统使用的功能保留的任何特殊字符可能会导致意外结果。例如，反斜线（\）被解释为转义字符，不应在社区字符串中使用。

步骤 3 设置 SNMP 服务器位置或联系人信息。

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

示例：

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

text 参数指定联系人或 ASA 系统管理员的名称。名称区分大小写，最多可包含 127 个字符。可包含空格，但多个空格将缩为一个空格。

步骤 4 设置 SNMP 请求的侦听端口。

snmp-server listen-port *lport*

示例：

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

lport 参数是接受传入请求的端口。默认侦听端口为 161。**snmp-server listen-port** 命令仅在管理情景中可用，在系统情景中不可用。如果在当前使用中的端口上配置 **snmp-server listen-port** 命令，系统将显示以下消息：

```
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.
```

现有 SNMP 线程会持续轮询（每 60 秒一次），直到端口可用，如果端口仍在使用中，则会发出系统日志 %ASA-1-212001。

配置 SNMP 第 3 版的参数

要配置 SNMP 第 3 版的参数，请执行以下步骤：

过程

步骤 1 指定仅供与 SNMP 第 3 版配合使用的新 SNMP 组。

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

示例：

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

配置社区字符串后，系统会自动生成具有与社区字符串相匹配的名称的另外两个组：一个表示第 1 版的安全模式，一个表示第 2 版的安全模式。**auth** 关键字可启用数据包身份验证。**noauth** 关键字表示未在使用数据包身份验证或加密。**priv** 关键字可启用数据包加密和身份验证。**auth** 或 **priv** 关键字不存在默认值。

步骤 2 为仅供与 SNMP 第 3 版配合使用的 SNMP 组配置新用户。

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*]]

示例：

```
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 参数是属于 SNMP 代理的主机上用户的名称。用户名最多输入 32 个字符。名称必须以字母开头。有效字符包括字母、数字、_（下划线）、.（句点）、@（邮箱符号）和 -（连字符）。

group-name 参数是用户所属的组的名称。**v3** 关键字指定应使用 SNMP 第 3 版安全模式并允许使用 **encrypted**、 **priv**和 **auth** 关键字。**engineID** 关键字是可选的，可指定用于本地化用户的身份验证和加密信息的 ASA 的 engineID。engineID 参数必须指定有效的 ASA engineID。

encrypted 关键字指定加密格式的密码。加密密码必须满足以下要求。

- 必须是十六进制格式。
- 必须包含最少 8 个字符，最多 80 个字符。
- 必须仅包含字母、数字和以下字符：~`!@#%^&*()_-+{}[]|\:;"'<,>./
- 不得包含以下符号：$（美元符号）、?（问号）或 =（等号）。
- 必须包含至少 5 个不同的字符。
- 不得包含过多连续递增或递减数字或字母。例如，字符串“12345”包含四个此类字符，字符串“ZYXW”包含三个此类字符。如果此类字符的总数超过某个限值（通常约大于 4 至 6 个字符），则简单性检查将会失败。

  注释
  在使用的非递增或递减字符数介于两者之间时，系统不会重置连续递增或递减字符计数。例如，abcd&!21 将致使密码检查失败，但 abcd&!25 不会。

auth 关键字指定应使用的身份验证级别（（**sha**、**sha224**、**sha256** 或 **sha384**）。**priv** 关键字指定加密级别。不存在 **auth** 或 **priv** 关键字或默认关键字的默认值。

对于加密算法，可以指定 **3des** 或 **aes** 关键字。您还可以指定要使用的 AES 加密算法版本：**128**、**192** 或 **256**。auth-password 参数指定身份验证用户密码。priv-password 参数指定加密用户密码。

如果忘记密码，则无法将其恢复，必须重新配置用户。您可以指定纯文本密码或本地化摘要。本地化摘要必须与为用户选择的身份验证算法（SHA、SHA-224、SHA-256 或 SHA-384）相匹配。当用户配置显示在控制台上或写入到文件（例如，启动配置文件）时，始终显示本地化身份验证和隐私摘要而非纯文本密码（参阅第二个示例）。密码的最小长度为 1 个字母数字字符；但是，出于安全原因，我们建议使用至少 8 个字母数字字符。

将 SNMPv3 用于集群或故障转移时，如果在初始集群形成后添加新的集群设备或更换故障转移设备，则 SNMPv3 用户不会复制到新设备。您必须将 SNMPv3 用户重新添加到控制/主用设备，以强制用户复制到新设备；或者，也可以直接在新设备上添加用户（SNMPv3 用户和组是无法在集群数据设备上输入配置命令的规则的例外）。重新配置每个用户，方法是在控制/主用设备上输入username group-name命令，或者直接在数据/备用设备上输入priv-password选项和auth-password选项（未加密形式）。**snmp-server user v3**

如果在控制/主用设备上使用 **encrypted** 关键字输入用户，系统将显示一条错误消息，通知您 SNMPv3 用户命令不会被复制。此行为还意味着在复制期间不会清除现有 SNMPv3 用户和组命令。

例如，使用通过加密密钥输入的命令的控制/主动设备：

```
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.
```

例如，在集群复制期间的数据设备上（仅在配置中存在**snmp-server user** 命令的情况下才会显示）：

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

步骤 3 指定 SNMP 通知的接收方。指示从其发送陷阱的接口。确定可以连接到 ASA 的 NMS 或 SNMP 管理器的名称和 IP 地址。

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

示例：

```
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 关键字可将 NMS 限制为仅接收陷阱。**poll** 关键字可将 NMS 限制为仅发送请求（轮询）。默认情况下，SNMP 陷阱已启用。默认情况下，UDP 端口为 162。社区字符串是 ASA 与 NMS 之间的共享密钥。密钥是一个区分大小写的值，最多为32个字母数字字符。不允许使用空格。默认社区字符串为 public。ASA 使用此密钥确定传入的 SNMP 请求是否有效。例如，您可以使用某社区字符串来指定站点，然后使用同一字符串配置 ASA 和 NMS。ASA 使用指定的字符串，并且不会对包含无效社区字符串的请求作出响应。在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。加密的社区字符串始终由ASA生成；您输入的一般是明文形式。

关键字指定用于陷阱和请求（轮询）的SNMP版本。**version** 仅允许使用所选版本与服务器通信。

在 ASA 上配置 SNMP 第 3 版主机时，用户必须与该主机关联。

要在添加**snmp-server host** 命令后接收陷阱，请确保使用 ASA 上配置的凭证相同的凭证来配置 NMS 上的用户。

步骤 4 设置 SNMP 服务器位置或联系人信息。

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

示例：

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

text 参数指定联系人或 ASA 系统管理员的名称。名称区分大小写，最多可包含 127 个字符。可包含空格，但多个空格将缩为一个空格。

步骤 5 设置 SNMP 请求的侦听端口。

snmp-server listen-port *lport*

示例：

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

lport 参数是接受传入请求的端口。默认侦听端口为 161。**snmp-server listen-port** 命令仅在管理情景中可用，在系统情景中不可用。如果在当前使用中的端口上配置 **snmp-server listen-port** 命令，系统将显示以下消息：

```
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.
```

现有 SNMP 线程会持续轮询（每 60 秒一次），直到端口可用，如果端口仍在使用中，则会发出系统日志 %ASA-1-212001。

配置用户组

要配置其中含有一组指定用户的 SNMP 用户列表，请执行以下步骤：

过程

配置 SNMP 用户列表。

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

示例：

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

listname 参数指定用户列表的名称，长度可以为最多 33 个字符。**username***user_name* 关键字/参数对指定在用户列表中可以配置的用户。使用 **snmp-server user***username* 命令配置用户列表中的用户，仅在使用的是 SNMP 第 3 版的情况下该命令才可用。用户列表必须具有多个用户，并且能与主机名或 IP 地址范围关联。

将用户与网络对象关联

要将用户列表中的单个用户或用户组与网络对象相关联，请执行以下步骤：

过程

将用户列表中的单个用户或用户组与网络对象相关联。

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

示例：

```
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 参数指定用户或用户组与之关联的接口网络对象名称。

trap 关键字指定只能发送陷阱，并且不允许浏览此主机（轮询）。默认情况下，SNMP 陷阱处于启用状态。

poll 关键字指定允许浏览主机（轮询），但不能发送陷阱。

community 关键字指定来自 NMS 的请求需要非默认字符串，或是当生成发送至 NMS 的陷阱时需要非默认字符串。您只能将此关键字用于 SNMP 第 1 版或第 2c 版。*community-string* 参数指定类似密码的字符串，该字符串随通知一起发送或者在 NMS 发出的请求中发送。社区字符串最多可以包含 32 个字符。

version 关键字将 SNMP 通知版本设置为版本 1、2c 或 3 以用于发送陷阱和接受请求（投票）。默认版本为 1。

username 参数指定您在使用 SNMP 版本 3 时用户的名称。

user-list *list_name* 关键字/参数对指定用户列表的名称。

udp-port *port* 关键字/参数对指定必须将 SNMP 陷阱发送到非默认端口上的 NMS 主机并设置该 NMS 主机的 UDP 端口号。默认 UDP 端口为 162。

监控 SNMP

请参阅以下用于监控 SNMP 的命令。

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

  此命令可显示所有 SNMP 服务器配置信息。

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

  此命令可显示 SNMP 组配置设置。

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

  此命令可显示供 SNMP 用于控制发送到远程主机的消息和通知的配置设置。

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

  此命令可显示 SNMP 主机组配置。

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

  此命令可显示 SNMP 基于用户的配置设置。

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

  此命令可显示 SNMP 用户列表配置。

- **show snmp-server engineid**

  此命令可显示所配置的 SNMP 引擎的 ID。

- **show snmp-server group**

  此命令可显示已配置的 SNMP 组的名称。如果已经配置社区字符串，则默认情况下在输出中会显示两个额外的组。此行为是正常的。

- **show snmp-server statistics**

  此命令可显示已配置的 SNMP 服务器特征。要将所有 SNMP 计数器重置为零，请使用 **clear snmp-server statistics** 命令。

- **show snmp-server user**

  此命令可显示已配置的用户特征。

示例

以下示例说明如何显示 SNMP 服务器统计信息：

```
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
```

以下示例说明如何显示 SNMP 服务器运行配置：

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

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP 示例

下节提供了可用作所有 SNMP 版本的参考的示例。

SNMP 第 1 版和第 2c 版

下例显示了 ASA 如何从内部接口上的主机 192.0.2.5 接收 SNMP 请求，但又不向任何主机发送任何 SNMP 系统日志请求：

```
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 第 3 版

下例显示了 ASA 如何使用 SNMP 版本 3 安全模型接收 SNMP 请求，这要求配置遵循如下特定的顺序：组、用户、主机：

```
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 的历史记录

表 *7: SNMP* 的历史记录

功能名称	版本	说明
SNMP 第 1 版和第 2c 版	7.0(1)	通过明文社区字符串在 SNMP 服务器与 SNMP 代理之间传输数据来提供 ASA 网络监控及事件信息。
SNMP 第 3 版	8.2(1)	为最安全形式的受支持安全模式 SNMP 第 3 版提供 3DES 或 AES 加密和支持。通过使用USM，此版本允许配置用户、组和主机以及身份验证特征。此外，此版本还允许对代理和MIB对象进行访问控制，并且包含其他 MIB 支持。 引入或修改了以下命令：**show snmp-server engineid**、**show snmp-server group**、**show snmp-server user**、**snmp-server group**、**snmp-server user**、**snmp-server host**。

功能名称	版本	说明
密码加密	8.3(1)	支持密码加密。 修改了以下命令：**snmp-server community** 和 **snmp-server host**。
SNMP 陷阱和 MIB	8.4(1)	支持以下其他关键字：**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**。 entPhysicalTable 报告传感器、风扇、电源和相关组件的条目。 支持以下其他 MIB：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。 支持以下其他陷阱：ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart。 引入或修改了以下命令：**snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable traps**。
IF-MIB ifAlias OID 支持	8.2(5) / 8.4(2)	ASA 现在支持 ifAlias OID。浏览 IF-MIB 时，ifAlias OID 将设置为已为接口说明设置的值。
ASA 服务模块 (ASASM)	8.5(1)	ASASM 支持 8.4(1) 中提供的所有 MIB 和陷阱，但以下项目除外： 8.5(1) 中不受支持的 MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（仅支持 entPhySensorTable 组下的对象）。 • ENTITY-SENSOR-MIB（仅支持 entPhySensorTable 组中的对象）。 • DISMAN-EXPRESSION-MIB（仅支持 expExpressionTable、expObjectTable 和 expValueTable 组中的对象）。 8.5(1) 中不受支持的陷阱： • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)。此陷阱仅用于电源故障、风扇故障和高 CPU 温度事件。 • InterfacesBandwidthUtilization。

功能名称	版本	说明
SNMP 陷阱	8.6(1)	支持 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X 的以下其他关键字：**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure**、**entity power-supply-temperature**。 修改了以下命令：**snmp-server enable traps**。
VPN 相关 MIB	9.0(1)	已实施更新版本的 CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB 来支持下一代加密功能。 已为 ASASM 启用以下 MIB： • 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)	添加了对以下 MIB 的支持：CISCO-TRUSTSEC-SXP-MIB。
SNMP OID	9.1(1)	已添加五个新的 SNMP 物理供应商类型 OID 来支持 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X。
NAT MIB	9.1(2)	添加了 cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 来支持 xlate_count 和 max_xlate_count 条目，相当于允许使用 **show xlate count** 命令进行轮询。
SNMP 主机、主机组和用户列表	9.1(5)	最多可以添加 4000 台主机。支持的活动轮询目标数量为 128。您可以指定网络对象以指示要添加为主机组的个别主机。您可以将多个用户与一台主机关联。 引入或修改了以下命令：**snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server**。
SNMP 消息大小	9.2(1)	SNMP 发送的消息大小限制已增大为 1472 字节。
SNMP OID 和 MIB	9.2(1)	ASA 现在支持 cpmCPUTotal5minRev OID。 ASA Virtual 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 中。 CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 已更新为支持新的 ASA Virtual 平台。 已添加用于监控 VPN 共享许可证使用情况的新 SNMP MIB。

功能名称	版本	说明
SNMP OID 和 MIB	9.3(1)	已为 ASASM 添加 CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) 支持。
SNMP MIB 和陷阱	9.3(2)	CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 均已更新，以支持 ASA 5506-X。 ASA 5506-X 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 表中。 ASA 现在支持 CISCO-CONFIG-MAN-MIB，它使您能够执行以下操作： • 了解已为特定配置输入的命令。 • 在运行配置发生更改后通知 NMS。 • 跟踪与上一次更改或保存运行配置相关的时间戳。 • 跟踪命令的其他更改，例如，终端详细信息和命令源。 修改了以下命令：**snmp-server enable traps**。
SNMP MIB 和陷阱	9.4(1)	ASA 5506W-X、ASA 5506H-X、ASA 5508-X 和 ASA 5516-X 已作为新产品添加到 SNMP sysObjectID OID 与 entPhysicalVendorType OID 表中。
每个情景的 SNMP 服务器陷阱主机数没有限制	9.4(1)	ASA 对于每个情景支持无限制的 SNMP 服务器陷阱主机数。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。 修改了以下命令：**show snmp-server host**。
添加了对 ISA 3000 的支持	9.4(1.225)	现在，SNMP 支持 ISA 3000 产品系列。我们为此平台添加了新的 OID。**snmp-server enable traps entity** 命令已修改为包括新变量 *l1-bypass-status*。这样将支持硬件旁路状态更改。 修改了以下命令：**snmp-server enable traps entity**。
在 CISCO-ENHANCED-MEMPOOL-MIB 中支持 cempMemPoolTable	9.6(1)	现在支持 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable。这是一个内存池表，监控受管系统上所有物理实体的条目。 **注释** CISCO-ENHANCED-MEMPOOL-MIB 使用 64 位计数器，并且支持报告 RAM 超过 4GB 的平台上的内存。
对于精确时间协议 (PTP) 支持 E2E 透明时钟模式 MIB	9.7(1)	现在支持与 E2E 透明时钟模式对应的 MIB。 **注释** 仅支持 SNMP get、bulkget、getnext 和 walk 操作。

功能名称	版本	说明
基于 IPv6 的 SNMP	9.9(2)	ASA 现在支持基于 IPv6 的 SNMP，包括通过 IPv6 与 SNMP 服务器通信，允许通过 IPv6 执行查询和陷阱，以及支持现有 MIB 使用 IPv6 地址。我们添加了以下新的 SNMP IPv6 MIB 对象，如 RFC 8096 中所述。 • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30) - 包含每个接口 IPv6 特定的信息。 • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32) - 包含由此实体获知的所有前缀。 • ipAddressTable (OID: 1.3.6.1.2.1.4.34) - 包含与实体接口相关的寻址信息。 • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35) - 包含从 IP 地址到物理地址的映射。 新增或修改的命令：**snmp-server host** 注释 **snmp-server host-group** 命令不支持 IPv6。
支持在SNMP审核操作期间启用和禁用可用内存和已用内存统计信息的结果	9.10(1)	为避免 CPU 资源的过度占用，您可以启用和禁用通过 SNMP 审核操作收集的可用内存和已用内存统计数据的查询。 新增/修改的命令：**snmp-server enable oid**
支持在SNMP审核操作期间启用和禁用可用内存和已用内存统计信息的结果	9.12(1)	为避免 CPU 资源的过度占用，您可以启用和禁用通过 SNMP 审核操作收集的可用内存和已用内存统计数据的查询。 未修改任何命令。
SNMPv3 身份验证	9.14(1)	现在，您可以使用 SHA-256 HMAC 验证用户身份。 新增/修改的命令：**snmp-server user**
对于9.14（1）+中的故障转移对等体，ASA不再与其对等体共享SNMP客户端引擎数据。	9.14(1)	ASA 再与其对等体共享 SNMP 客户端引擎数据。
通过站点间 VPN 进行 SNMP 轮询	9.14(2)	对于通过站点间 VPN 进行安全 SNMP 轮询，请将外部接口的 IP 地址包含在加密映射访问列表中作为 VPN 配置的一部分。
已弃用对于 CISCO-MEMORY-POOL-MIB OID 的支持	9.15(1)	对于使用 64 位计数器的系统，已弃用 CISCO-MEMORY-POOL-MIB OID（ciscoMemoryPoolUsed、ciscoMemoryPoolFree）。 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable 为使用 64 位计数器的系统提供内存池监控条目。

功能名称	版本	说明
SNMPv3 身份验证	9.16（1）	您现在可以使用 SHA-224 和 SHA-384 进行用户身份验证。您不能再使用 MD5 进行用户身份验证。 您不能再使用 DES 进行加密。 新增/修改的命令：**snmp-server user**
基于 IPv6 的 SNMP	9.17(1)	**snmp-server host-group** 命令现在支持 IPv6 主机、范围和子网对象。
环回接口支持 SNMP	9.18(2)	您现在可以添加环回接口并用于 SNMP： 新增/修改的命令： **interface loopback**、**snmp-server host**
SNMP MIB 和陷阱	9.20(1)	Cisco Secure Firewall 4200 型号设备（FPR4215、FPR4225 和 FPR4245）已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 表中。添加了对这些 Cisco Secure Firewall 4200 系列设备的两个 EPM 卡（4X200G 和 2X100G）的 SNMP 支持。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。