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，第 1 页
- SNMP 准则，第 4 页
- 配置 SNMP，第 6 页
- 监控 SNMP，第 13 页
- SNMP 历史记录，第 14 页

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。

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。

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，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。
- 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。
- 对于防火墙 3100 ，**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。
- 如果 NMS 无法成功请求对象或者未在正确处理来自 ASA 的传入陷阱，则执行数据包捕获是确定的问题最实用方法。依次选择 **Wizards > Packet Capture Wizard**，然后遵循屏幕上的说明执行操作。
- 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。

配置 SNMP

本节介绍如何配置 SNMP。

过程

步骤 1 将 SNMP 管理站配置为接收来自 ASA 的请求。

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。

配置 SNMP 管理站

要配置 SNMP 管理站，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **SNMP**。默认情况下，SNMP 服务器已启用。

步骤 2 点击 **SNMP Management Stations** 窗格中的 **Add**。

系统将显示 **Add SNMP Host Access Entry** 对话框。

步骤 3 选择 SNMP 主机所在的接口。

步骤 4 输入 SNMP 主机 IP 地址。

步骤 5 输入 SNMP 主机 UDP 端口或保留默认值，即端口 162。

步骤 6 添加 SNMP 主机社区字符串。如果没有为管理站指定社区字符串，则会使用 **SNMP Management Stations** 窗格上的 **Community String**（默认）字段中设置的值。

步骤 7 选择 SNMP 主机使用的 SNMP 版本。

步骤 8 如果在上一步中选择 SNMP 第 3 版，请选择已配置的用户的名称。

步骤 9 要指定用于与此 NMS 进行通信的方法，请选中 **Poll** 或 **Trap** 复选框。

步骤 10 点击 **OK**。

系统将关闭 **Add SNMP Host Access Entry** 对话框。

步骤 11 点击 **Apply**。

系统将配置 NMS 并将更改保存到运行配置。有关 SNMP 第 3 版 NMS 工具的详细信息，请参阅以下 URL：

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

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

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **SNMP**。

步骤 2 点击 **Configure Traps**。

系统将显示 **SNMP Trap Configuration** 对话框。

步骤 3 选中 **SNMP Server Traps Configuration** 复选框。

默认配置已启用所有 SNMP 标准陷阱。如果不指定陷阱类型，则默认为 **syslog** 陷阱。默认 SNMP 陷阱随**系统日志**陷阱继续启用。默认情况下会禁用所有其他陷阱。要禁用陷阱，请取消选中适用的复选框。

陷阱分为以下类别：

a) **标准 SNMP 陷阱**，请选中所有适用项。

从**严重 CPU 温度**、**机箱温度**、和**机箱风扇故障**中选择。

注释 默认配置已启用所有 SNMP 标准陷阱。

b) **环境陷阱**，请选中所有适用项。

从“**身份验证**”、“**链路开启**”、“**链路关闭**”、“**冷启动**”和“**热启动**”中选择。

c) **Ikev2 陷阱**选中所有适用项。

从“**开始**”和“**停止**”中选择。

d) **实体 MIB 通知**。

选中此项目可接收有关可现场更换设备的通知。

e) **IPsec 陷阱**，请选中所有适用项。

从“**开始**”和“**停止**”中选择。

f) **远程访问陷阱**。

选中此项目可在建立的会话数超过设置的阈值时接收通知。

g) **资源陷阱**，选中所有适用项。

从**已达到连接上限**、**已达到内存阈值**和**接口阈值**中选择。

h) **NAT 陷阱**。

选中此项目可在由于映射空间不可用而被 NAT 丢弃 IP 数据包时接收通知。

i) 系统日志。

选中**启用系统日志陷阱**以在建立的会话数超过设置的阈值时接收通知。

要配置 **syslog** 陷阱严重性级别，请依次选择 **Configuration** > **Device Management** > **Logging** > **Logging Filters**。

j) **CPU 利用率陷阱**。

如果 CPU 使用率大于配置的**监控间隔**的配置的 **CPU 使用率阈值**，请选中**已达到 CPU 上升阈值**以接收通知。

k) **SNMP 接口阈值**。

选中**配置阈值和间隔**以在接口带宽利用率大于配置的 **SNMP 接口阈值**时接收通知。

有效阈值范围为 30% 到 99%。默认值为 70%。

l) **SNMP 内存阈值**。

选中**配置内存阈值**以在 CPU 使用率大于 **SNMP 内存阈值**的配置阈值时接收通知。

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内存阈值陷阱。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。

m) **故障转移陷阱**。

选中**启用故障转移相关陷阱**以接收 SNMP 系统日志陷阱以进行故障转移。

n) 集群陷阱。

选中启用集群相关陷阱以接收集群成员的SNMP系统日志陷阱。

o) **对等翻板陷阱**。

选中启用bgp / ospf peer-flap相关陷阱以接收集群对等MAC地址摆动的SNMP系统日志陷阱。

步骤 4 点击 **OK** 以关闭 **SNMP Trap Configuration** 对话框。

步骤 5 点击 **Apply**。

系统将配置 SNMP 陷阱配置并将更改保存到运行配置。

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 依次选择**配置** > **设备管理** > **管理访问** > **SNMP**。

步骤 2 如果使用的是 SNMP 第 1 版或第 2c 版，请在 **Community String**（默认）字段中输入默认社区字符串。输入 SNMP NMS 向 ASA 发送请求时所用的密码。SNMP 社区字符串是 SNMP NMS 和托管网

络节点之间的共享密钥。ASA 使用此密码确定传入的 SNMP 请求是否有效。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。密码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。默认值为 public。SNMP 第 2c 版允许为每个 NMS 设置单独的社区字符串。如果没有为任何 NMS 配置社区字符串，则默认情况下使用此处设置的值。

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　输入 ASA 系统管理员的名称。名称区分大小写，并且最多可以为 127 个字母字符。可包含空格，但多个空格将缩为一个空格。

步骤 4　输入正由 SNMP 管理的 ASA 的位置。文本区分大小写，并且最多可以为 127 个字符。可包含空格，但多个空格将缩为一个空格。

步骤 5　输入用于侦听来自 NMSes 的 SNMP 请求的 ASA 端口号；或保留默认端口号 161。

步骤 6　（可选）选中在遍历中启用全局共享池复选框以通过SNMP遍历操作查询可用内存和已用内存统计信息。

重要事项　当ASA查询内存信息时，SNMP进程可能会将CPU占用的时间过长，然后才将CPU释放给其他进程。这可能会导致与SNMP相关的CPU消耗导致丢包。

步骤 7　在 **SNMP Host Access List** 窗格中点击 **Add**。

系统将显示 **Add SNMP Host Access Entry** 对话框。

步骤 8　从下拉列表中选择从其发送陷阱的接口名称。

步骤 9　输入可以连接到 ASA 的 NMS 或 SNMP 管理器的 IP 地址。

步骤 10　输入 UDP 端口号。默认值为 162。

步骤 11　从下拉列表中选择您使用的 SNMP 版本。如果选择第 1 版或第 2c 版，则必须输入社区字符串。如果选择第 3 版，则必须从下拉列表中选择用户名。

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

步骤 12　选中 **Server Poll/Trap Specification** 区域中的 **Poll** 复选框，以将 NMS 限制为仅发送请求（轮询）。选中 **Trap** 复选框以将 NMS 限制为仅接收陷阱。您可以同时选中两个复选框以执行 SNMP 主机的两个功能。

步骤 13　点击 **OK** 以关闭 **Add SNMP Host Access Entry** 对话框。

新主机将显示在 **SNMP Host Access List** 窗格中。

步骤 14　点击 **Apply**。

系统将配置第 1、2c 或 3 版的 SNMP 参数并将更改保存到运行配置。

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 依次选择**配置** > **设备管理** > **管理访问** > **SNMP**。

步骤 2 依次点击 **SNMPv3 用户 (SNMPv3 Users)** 窗格中 **SNMPv3 用户/组 (SNMPv3 User/Group)**选项卡上的**添加 (Add)** > **SNMP 用户 (SNMP User)**，来向组中添加已配置的用户或新用户。删除组中的最后一个用户时，ASDM 会删除该组。

注释 创建用户后，不能更改该用户所属的组。

系统将显示 **Add SNMP User Entry** 对话框。

步骤 3 选择 SNMP 用户所属的组。可用的组如下：

- **Auth&Encryption**，其中用户已配置身份验证和加密
- **Authentication_Only**，其中用户仅配置了身份验证
- **No_Authentication**，其中用户未配置身份验证和加密

注释 不能更改组名。

步骤 4 点击 **USM 模式 (USM Model)** 选项卡以使用用户安全模式 (USM) 组。

步骤 5 点击**添加 (Add)**。

系统将显示 **Add SNMP USM Entry** 对话框。

步骤 6 输入组名称。

步骤 7 从下拉列表中选择安全级别。此设置允许将已配置的 USM 组作为安全级别分配给 SNMPv3 用户。

步骤 8 输入已配置的用户或新用户的名称。用户名对于所选 SNMP 服务器组必须唯一。

步骤 9 通过点击以下两个单选按钮之一指示要使用的密码类型：**Encrypted** 或 **Clear Text**。

步骤 10 指示身份验证的类型您想要通过点击四个单选按钮之一使用：**SHA**、**SHA224**、**SHA256** 或 **SHA384**。

步骤 11 输入要用于身份验证的密码。

步骤 12 通过点击以下三个单选按钮之一指示要使用的加密类型 两个单选按钮： **3DES** 或 **AES**。

步骤 13 如果选择 AES 加密，则选择要使用的 AES 加密级别：**128**、**192** 或 **256**。

步骤 14 输入要用于加密的密码。此密码允许的最大字母数字字符数为 64。

步骤 15 点击**确定 (OK)** 以创建组（如果这是该组中的第一个用户），在**组名称 (Group Name)** 下拉列表中显示该组，然后为该组创建用户。

系统将关闭 **Add SNMP User Entry** 对话框。

步骤 16 点击 **Apply**。

系统将配置第 3 版的 SNMP 参数并将更改保存到运行配置。

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

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **SNMP**。

步骤 2 依次点击 **SNMPv3 用户**窗格中 **SNMPv3 用户/组**选项卡上的**添加** > **SNMP 用户组**，来添加已配置的用户组或新用户组。删除组中的最后一个用户时，ASDM 会删除该组。

系统将显示 **Add SNMP User Group** 对话框。

步骤 3 输入用户组名。

步骤 4 点击 **Existing User/User Group** 单选按钮以选择现有用户或用户组。

步骤 5 点击 **Create new user** 单选按钮以创建新用户。

步骤 6 选择 SNMP 用户所属的组。可用的组如下：

- **Auth&Encryption**，其中用户已配置身份验证和加密
- **Authentication_Only**，其中用户仅配置了身份验证
- **No_Authentication**，其中用户未配置身份验证和加密

步骤 7 输入已配置的用户或新用户的名称。用户名对于所选 SNMP 服务器组必须唯一。

步骤 8 通过点击以下两个单选按钮之一指示要使用的密码类型：**Encrypted** 或 **Clear Text**。

步骤 9 通过点击以下三个单选按钮之一指示要使用的身份验证类型：**SHA**、**SHA224**、**SHA256** 或 **SHA384**。

步骤 10 输入要用于身份验证的密码。

步骤 11 确认要用于身份验证的密码。

步骤 12 通过点击以下三个单选按钮之一指示要使用的加密类型 两个单选按钮： **3DES** 或 **AES**。

步骤 13 输入要用于加密的密码。此密码允许的最大字母数字字符数为 64。

步骤 14 确认要用于加密的密码。

步骤 15 点击 **Add** 以将新用户添加到 **Members in Group** 窗格中的指定用户组。点击 **Remove** 以从 **Members in Group** 窗格中删除现有用户。

步骤 16 点击 **OK** 为指定用户组创建新用户。

系统将关闭 **Add SNMP User Group** 对话框。

步骤 17 点击 **Apply**。

系统将配置第 3 版的 SNMP 参数并将更改保存到运行配置。

监控 SNMP

请参阅以下用于监控 SNMP 的命令。您可以依次使用 **Tools > Command Line Interface** 输入这些命令。

- **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。

SNMP 历史记录

表 *2: SNMP* 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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
密码加密	8.3(1)	支持密码加密。
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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
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。

功能名称	版本	说明
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。
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。

功能名称	版本	说明
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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP。
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。
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。 修改了以下屏幕：Configuration > Device Management > Management Access > SNMP > Configure Traps > SNMP Trap Configuration。
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。

功能名称	版本	说明
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。 未修改任何 ASDM 屏幕。
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。 未修改任何 ASDM 屏幕。
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。
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。 新增或修改的菜单项：**配置** > **设备管理** > **管理访问** > **SNMP**
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。 我们未修改任何 ASDM 屏幕。
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。 新增或修改的菜单项：**配置** > **设备管理** > **管理访问** > **SNMP**

功能名称	版本	说明
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/修改的菜单项：**配置** > **设备管理** > **管理访问** > **SNMP**
对于9.14（1）+中的故障转移对，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。
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/修改的菜单项：**配置** > **设备管理** > **管理访问** > **SNMP**
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** 新增/修改的屏幕： **配置** > **设备设置** > **接口设置** > **接口** > **添回环接口** 7.19 中添加了 ASDM 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。