ASA SNMP功能增强实施

目录

简介

本文档介绍适用于软件版本9.1.5和9.2.(1)及更高版本中的思科自适应安全设备(ASA)5500-X系列防火墙的新简单网络管理协议(SNMP)功能。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行Cisco ASA®软件版本9.1.5和9.2.(1)及更高版本的Cisco ASA 5500-X系列

防火墙。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在ASA版本9.1.5和9.2.1中，引入了以下SNMP增强功能：

- 增加了对128台SNMP主机的支持。
- 添加了对cpmCPUTotal5minRev SNMP对象标识符(OID)的支持。
- 增加了对1,472字节SNMP消息的支持。

支持128台SNMP主机

此功能允许ASA支持的SNMP主机数超过当前的32台。

目的

目前，ASA的硬限制为总共32台SNMP主机。这包括可配置陷阱和轮询的主机。下一节介绍此功能对单情景和多情景模式的影响。

单情景模式

- 允许配置的条目数（主机总数）显着增加，最多4,096个。但是，在这些条目中，仅128个可用于陷阱。
- 出于轮询配置目的，最多可配置4,096个轮询主机和128个陷阱主机。但是，轮询系统的实际服务器数量应限制为少于128台，因为未知且不支持来自更多主机的性能影响。

多情景模式

- 出于配置目的，每个情景最多允许4,000台主机，并且系统范围限制总主机数为64,000台。
- 在已配置的主机总数中，仅128（每个情景）可用于陷阱，而多情景模式下陷阱的总体系统限制为32,000。
- 虽然每个情景最多可配置4,000台主机，但轮询任何情景的服务器实际数量应限制为128台。

描述

您可能更愿意从大型SNMP主机池监控网络设备。理想情况下，您希望能够指定允许监控网络设备的IP地址的IP范围和/或子网。ASA目前不提供这种灵活性，并将最大SNMP主机数限制为32台。

此功能的支持包括两个方面：

- 为ASA提供最多可处理128台SNMP主机的功能。

- 提供所需的配置命令，以便您可以通过单个命令配置数量高得多的主机，如上节所述。

ASA的当前设计是通过CLI配置单个主机。对于此功能，考虑了以下额外设计要求：

- 将snmp-server host-group **CLI命令与snmp-server host** CLI命**令保留一起**介绍。

- snmp-server host-group和snmp-server host **CLI命令中**的**条目**的能力。

- 对于SNMP第3版，引入了snmp-server userlist **CLI命令和**snmp-server user **CLI命令保**留功能。

- 还必须支持配置重**叠**。例如，可以为网络**对象中**重**叠**的主机指定多个host-group命令。同样，您也可以指定IP地址与当前主机或主机组重**叠**的主机。这提供了一种机制，可用于覆盖组中少数主机的参数，而无需重新配置整个组。

与此功能相关的一些软件限制和警告包括：

- 作为snmp-server host-group**命令的一部分**，如果未指定**[trap|poll]，则默认为poll**。另外，必须注意的是，对于此命令，不能为同一主机组同时启用陷阱和轮询。如果需要，Cisco建议您对相关主机使**用snmp-server host**命令。

- 可以指定在不同host-group命令中重**叠的网络**对象。在最后一个主机组中指定的值对不同网络对象中的一组公共主机生效。

示例如下：

```
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

输入**show snmp-server host命**令以查看主机条目：

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
host ip = 64.103.236.43, interface = inside  poll version 3 cisco1
host ip = 64.103.236.44, interface = inside  poll version 3 cisco1
host ip = 64.103.236.45, interface = inside  poll version 3 cisco1
host ip = 64.103.236.46, interface = inside  poll version 3 cisco1
host ip = 64.103.236.47, interface = inside  poll version 3 cisco1
host ip = 64.103.236.48, interface = inside  poll version 3 cisco1
host ip = 64.103.236.49, interface = inside  poll version 3 cisco1
```

```
host ip = 64.103.236.50, interface = inside  poll version 3 cisco1
host ip = 64.103.236.51, interface = inside  poll version 3 cisco1
host ip = 64.103.236.52, interface = inside  poll version 3 cisco1
host ip = 64.103.236.53, interface = inside  poll version 3 cisco1
host ip = 64.103.236.54, interface = inside  poll version 3 cisco1
host ip = 64.103.236.55, interface = inside  poll version 3 cisco1
```

以下是有关此功能使用的一些重要说明：

- 如果删除与其他主机组重叠的主机组或主机，则使用配置的主机组所用的值再次设置主机。
- 与主机关联的值或参数取决于命令的执行顺序。
- 如果某个特定主机组使用该列表，则无法删除已配置的用户列表。
- 如果在特定用户列表中引用该用户，则无法删除该SNMP用户。
- 如果主机组CLI命令使用网络对象，则无**法将其**删除。

配置

使用本节中介绍的信息配置ASA，以便实施此新功能。

> **注意：**使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

CLI命令

对于SNMP第3版，管理员可以将不同用户与指定的主机组关联。如果管理员希望一组用户能够从一组主机访问ASA，则此功能非常有用。此CLI命令用于为多个用户配置用户列表：

```
ASA(config)# [no] snmp-server user-list
```

要将用户列表与主机组关联，请在CLI中输入以下命令：

```
[no] snmp-server host-group
```

使用此单个命令，可以指定网络对象以指示应添加的多台主机。使用网络对象，可以使用单个命令指定子网掩码或应添加的IP地址范围。列为网络对象一部分的所有IP地址都添加为SNMP主机条目。同样，对于在用户列表中指定的每个用户，都有单独的SNMP主机条目。

以下命令用于允许管理员清除和查看SNMP服务器的新配置选项：

- clear configure snmp-server user-list
- clear configure snmp-server host-group
- show running-config snmp-server user-list
- show running-config snmp-server host-group

配置示例

要使用新的SNMP组选项并为版本2c轮询创建SNMP服务器主机组，请完成以下步骤：

1. 创建网络对象：

```
asa(config)# object network network1
asa(config-network-object)# range 64.103.236.40 64.103.236.50
```

2. 定义SNMP主机组：

```
asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
```

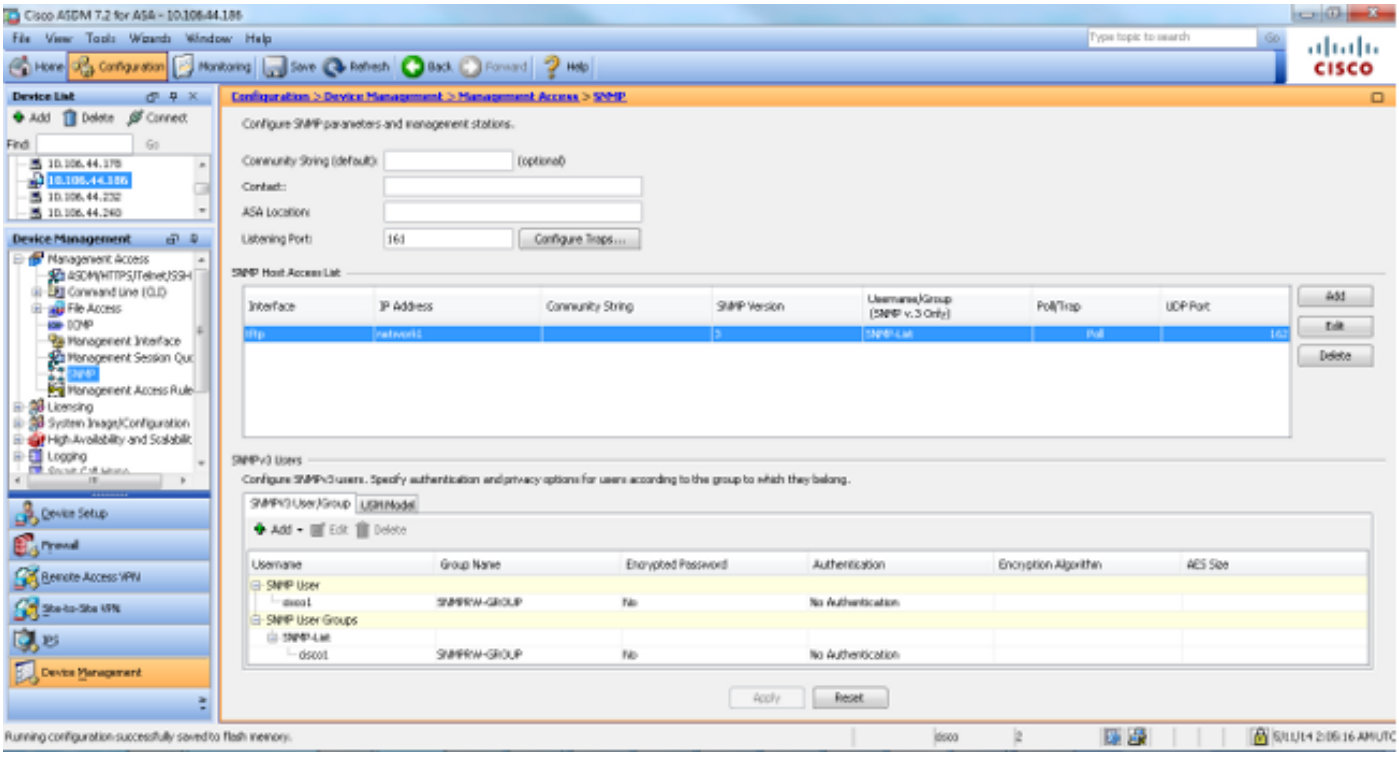
3. 定义SNMP第3版组：

```
asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
```

4. 将组与用户关联：

```
asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
asa(config)#snmp-server user-list SNMP-List username cisco1
asa(config)#snmp-server host-group inside  network1 poll version 3 user-list SNMP-List
```

下图说明了在思科自适应安全设备管理器(ASDM)中所做的更改：



支持cpmCPUTotal5minRev SNMP OID

此功能允许ASA支持**cpmCPUTotal5minRev** SNMP OID。

目的

此功能在ASA上增加了对**cpmCPUTotal5minRev**和**cpmCPUTotal1minRev** OID的支持，并弃用了当前支持的OID**cpmCPUTotal5min**和**cpmCPUTotal1min**。这些OID的目的是监控CPU的使用情况。当前支持的OID范围为1到100，而新支持的OID范围为0到100。因此，添加了对较新的OID的支持，因为它们覆盖的范围更广。

请注意，由于ASA不再支持已弃用的OID(**cpmCPUTotal5min**和**cpmCPUTotal1min**)，因此，如果ASA已升级且已轮询已弃用的OID，则ASA不会返回这些OID的任何信息。升级ASA后，现在需要监控CPU使用**cpmCPUTotal5minRev**和**cpmCPUTotal1minRev**。

CLI命令

此新功能未引入CLI更改。

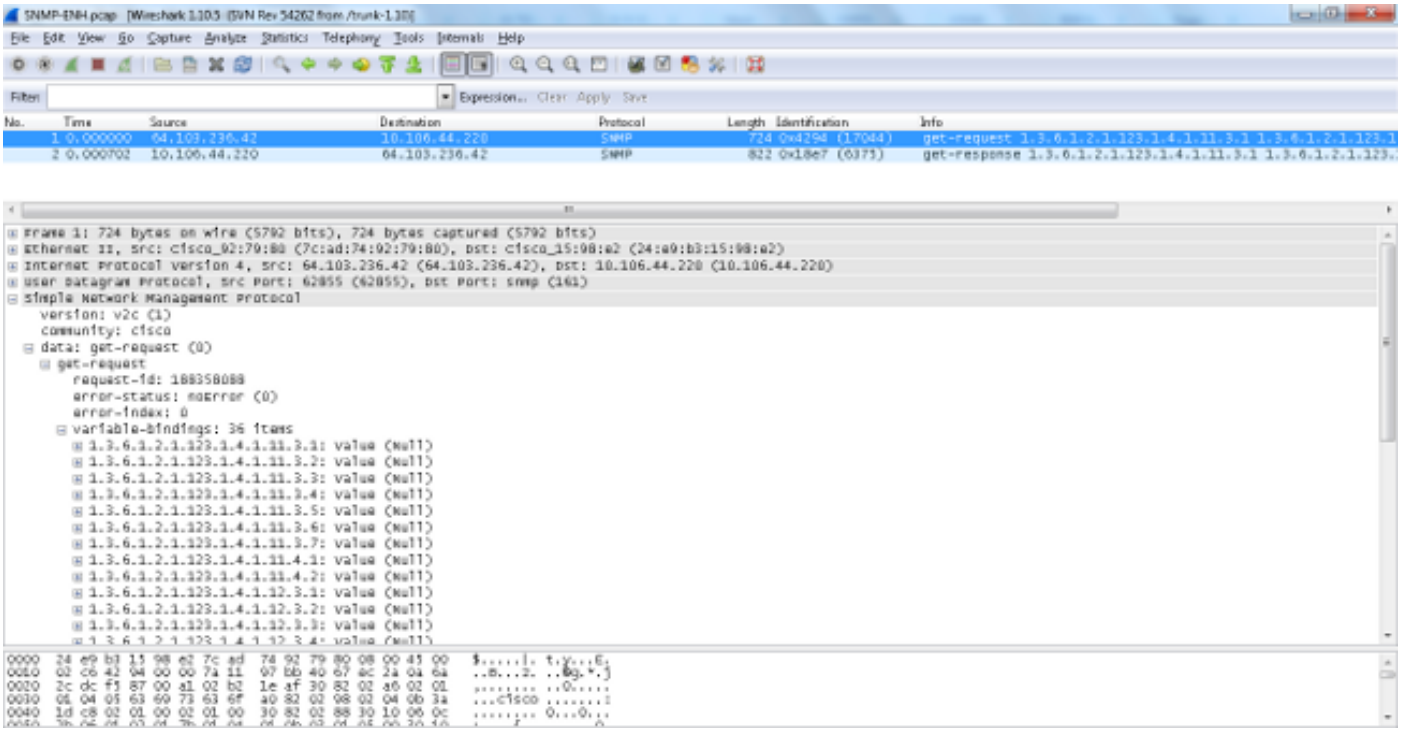
新OID

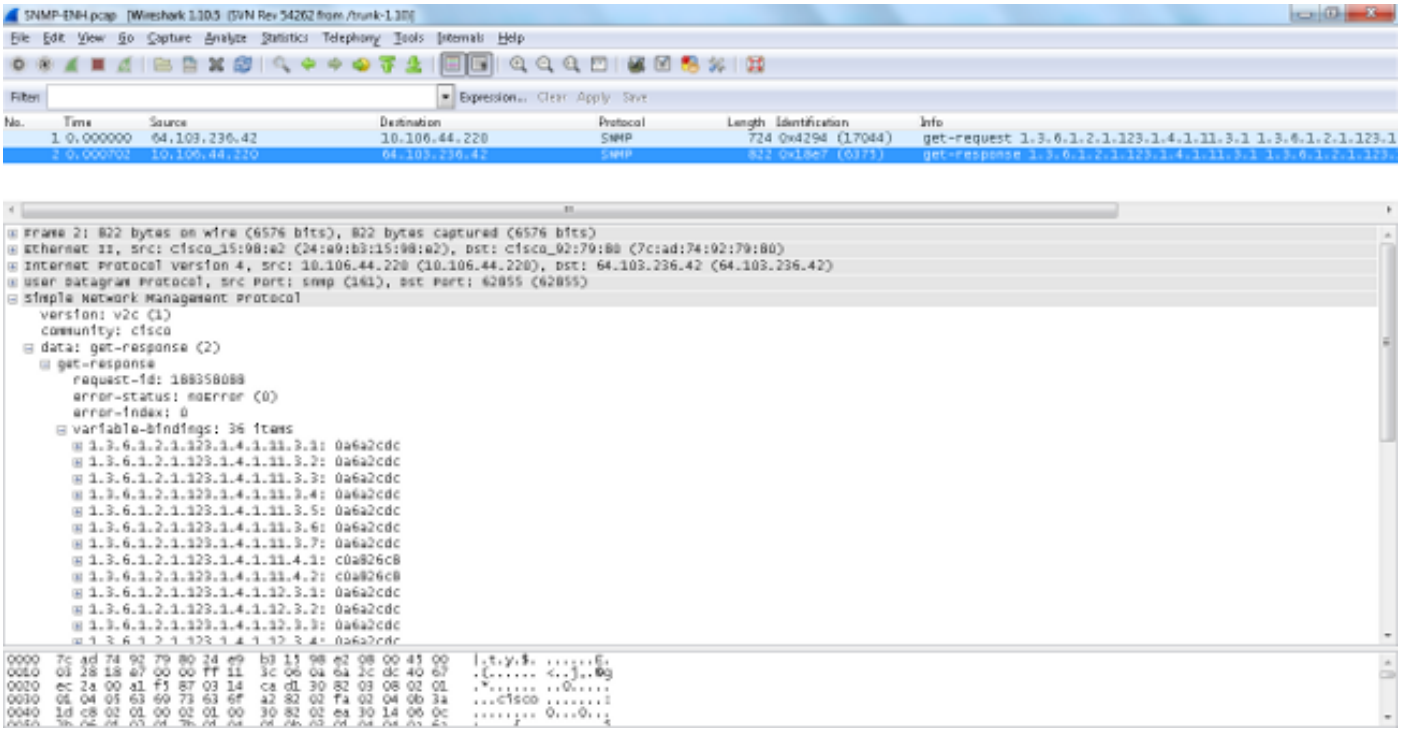
以下是随此功能添加的新OID:

- **1.3.6.1.4.1.9.9.109.1.1.1.1.7 的多播地址发送一次邻居消息。 cpmCPUTotal1minRev**
- **1.3.6.1.4.1.9.9.109.1.1.1.1.8 的多播地址发送一次邻居消息。 cpmCPUTotal5minRev**

支持1,472字节SNMP消息

ASA平台将SNMP请求的最大数据包大小限制为512字节。当您对单个SNMP请求中的大量MIB OID执行批量查询时，SNMP连接超时，ASA上会生成错误系统日志。RFC3417建议SNMP请求的最大数据包大小应为1,472字节。这是数据包的SNMP负载大小。此外，必须添加以太网报头和IP报头大小才能计算数据包的总大小。





注意：此功能支持单情景和多情景模式。

故障排除

本节提供可用于排除ASA上的系统问题的信息。

显示命令

当尝试对ASA上的问题进行故障排除时，以下**show**命令可能非常有用：

- asa#**show run snmp-server host-group**
  snmp-server host-group inside network1 poll version 3 user-list SNMP-List

- asa#**show run snmp-server user-list**
  snmp-server user-list SNMP-List username cisco1

- asa# **show snmp-server host**

此CLI命令显示SNMP服务器地址表中存在的条目，包括主机和主机组配置：

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
object network network3
range 64.103.236.60 64.103.236.70

ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
```

```
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact

ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
```

如图所示，这些命令显示通过host-group命令配置的所有主机。您可以使用此命令来验证所有条目是否都可用，并交叉验证重叠的主机组。