

ASA SNMP功能增强实施

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[128台SNMP主机的支持](#)

[目的](#)

[单一上下文模式](#)

[多个上下文模式](#)

[说明](#)

[配置](#)

[CLI命令](#)

[配置示例](#)

[为cpmCPUTotal5minRev SNMP OIDs支持](#)

[目的](#)

[CLI命令](#)

[新的OIDs](#)

[故障排除](#)

[显示命令](#)

简介

本文描述可用为Cisco可适应安全工具的新的简单网络管理协议(SNMP)功能(ASA) 5500-X系列防火墙在软件版本9.1.5和版本9.2.(1)及以后。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

[使用的组件](#)

本文档中的信息根据运行Cisco ASA[®]软件版本9.1.5和版本9.2.(1)及以后的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，这些SNMP增强介绍：

- 128台SNMP主机的支持被添加。
- 为cpmCPUTotal5minRev SNMP对象标识符(OIDs)支持被添加。
- 1,472字节SNMP消息的支持被添加。

128台SNMP主机的支持

此功能比当前允许ASA支持更多32台SNMP主机。

目的

目前，ASA有32台SNMP主机总计一硬限制。这包括可以配置为陷阱和为轮询的主机。以下部分描述此功能有在单个和多个上下文模式的影响。

单一上下文模式

- 极大允许将配置的一较高的值条目(总主机)，向上4,096。然而，在这些条目外面，仅128可以用于陷阱。
- 对于轮询的配置目的，4,096台轮询的主机和128台陷阱主机允许配置。然而，轮询系统应该限制到服务器的实际数量少于128，因为从主机较高的值的性能影响未知和不支持的。

多个上下文模式

- 为配置的目的地，每上下文4,000台主机允许，并且实施64,000台总主机一全系统的限制。
- 在总已配置的主机外面，仅128 (每上下文)可以用于陷阱和整个系统限制陷阱的在多个上下文模式是32,000。
- 虽然您能配置每上下文4,000台总主机，轮询所有上下文服务器的实际数量应该限制到128。

说明

您也许喜欢监控从SNMP主机的一个大池的网络设备。理论上讲，您想要能力指定IP范围和允许监控网络设备IP地址的子网。ASA当前不提供该灵活性并且限制最大数量SNMP主机到32。

此功能的支持介入两个方面：

- 为ASA提供功能处理128台SNMP主机。
- 提供必需的配置命令，以便您能极大配置主机一较高的值，详情参见前面部分通过单个命令。在ASA的当前设计是这样单个主机可以通过CLI配置。对于此功能，这些另外的设计需求考虑：

- **snmp-server主机组**的介绍CLI命令与**snmp-server host** CLI命令挽留。
- 条目的能力能来自**snmp-server主机组**和**snmp-server host** CLI命令。
- SNMP版本3， **snmp-server userlist**的介绍CLI命令与**snmp-server用户**CLI命令挽留。
- 必须也支持配置重叠。例如，多**主机组**命令可以用在网络对象交迭的主机给。同样地，您能指定一台主机用交叠以当前主机或主机组的IP地址。这提供能使用为了覆盖一些台主机的参数在组中的一机制，不用需要重新配置完整组。

关联与此功能的某些软件限制和警告是：

- 作为**snmp-server主机组**命令的部分，默认是**投票**，如果**[陷阱|投票]**没有指定。应该注意的是为此命令，陷阱和?不可能为同一主机组启用。如果这要求，Cisco建议您使用**snmp-server host**命令相关主机。
- 您能指定交迭用不同的**主机组**命令的网络对象。在最后一个主机组中指定的值生效普通的套的在不同的网络对象的主机。

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**snmp-server host**命令的显示为了查看主机条目：

```
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
```

这是关于使用的一些重要提示此功能：

- 如果交迭以其他主机组的主机组或主机删除，主机再设置使用已配置的主机组的值。
- 用主机关联的值或参数取决于命令命令被执行。
- 配置的用户列表不可能删除，如果特定主机组使用列表。
- 如果用户在特定用户用户列表，是指SNMP用户不可能删除。
- 如果CLI命令的主机组使用网络对象不可能删除。

配置

请使用在此部分描述为了配置ASA的信息，以便此新特性实现。

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版本3，管理员能连结多种用户与主机的一个指定的组。如果管理员希望一套用户有能力访问从主机的一组的，ASA这是有用的。此CLI命令用于为了配置多个用户的一份用户列表：

```
ASA(config)# [no] snmp-server user-list <list_name> username <user_name>
```

为了连结用户列表与主机组，请输入此命令到CLI：

```
[no] snmp-server host-group <interface> <network-object> [trap|poll]
[community [enc_type] <text>] [version {1 | 2c | 3 [user name | user-list
<list-name>]]] [udp-port <port_number>]
```

用此单个命令，您能指定网络对象为了指示应该添加的多台主机。使用网络对象，您能指定应该添加的一个子网掩码或IP地址范围，与使用单个命令。列出作为网络对象的部分的所有IP地址被添加作为SNMP主机条目。同样地，为在用户列表指定，有分开的SNMP主机条目的其中每一个用户。

这些命令用于为了允许管理员清除和查看SNMP服务器的新的配置选项：

- **结算配置snmp-server用户列表**
- **结算配置snmp-server主机组**
- **show running-config snmp-server用户列表**
- **show running-config snmp-server主机组**

配置示例

完成这些步骤为了使用新的SNMP组选项和为版本2c?创建SNMP服务器主机组：

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版本3组：

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

4. 附加组给用户：

```
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
```

此镜像说明在Cisco Adaptive Security Device Manager的变动(ASDM)内做：

为cpmCPUTotal5minRev SNMP OIDs支持

此功能允许ASA支持cpmCPUTotal5minRev SNMP OIDs。

目的

此功能添加cpmCPUTotal5minRev的支持和在ASA的cpmCPUTotal1minRev OIDs并且贬抑当前支持的OIDs cpmCPUTotal5min和cpmCPUTotal1min。这些OIDs目的将监控CPU使用情况。从1的当前支持的OIDs范围到100，当从0的新支持的OIDs范围到100时。因此，支持为更新的OIDs被添加了，他们报道一个大范围。

请注意，因为(cpmCPUTotal5min和cpmCPUTotal1min) ASA不再支持贬抑的OIDs，如果ASA升级，并且贬抑的OIDs轮询，ASA不返回那些OIDs的任何信息。在ASA的升级，您当前要求监控cpmCPUTotal5minRev和cpmCPUTotal1minRev CPU使用情况的后。

CLI命令

没有CLI更改介绍与此新特性。

新的OIDs

添加与此功能的这些是新的OIDs：

- 1.3.6.1.4.1.9.9.109.1.1.1.1.7. cpmCPUTotal1minRev
- 1.3.6.1.4.1.9.9.109.1.1.1.1.8. cpmCPUTotal5minRev

1,472字节SNMP消息的支持

ASA平台对512个字节限制SNMP请求的最大数据包大小。当您执行很大数量的MIB OIDs的一大批查询在单个SNMP请求内时，SNMP连接暂停，并且错误Syslog在ASA生成。RFC3417建议SNMP请求的最大数据包大小应该是1,472个字节。这是SNMP有效负载的大小数据包的。另外，必须添加以太网报头和IP报头大小为了计算数据包的总大小。

注意：单一上下文和多个上下文模式支持与此功能。

故障排除

此部分提供您能使用为了排除故障在ASA的系统问题的信息。

显示命令

当尝试被做排除故障在ASA时的问题这些显示命令可以是有用的：

- **asa# show run snmp-server主机组**
snmp-server主机组在network1投票版本3用户列表SNMP列表里面
- **asa# show run snmp-server用户列表**
snmp-server用户列表SNMP列表用户名cisco1
- **asa#显示snmp-server host**

此CLI命令显示是存在SNMP服务器地址表里，包括主机和主机组配置的条目：

```
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 64.103.236.70ciscoasa/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 contactciscoasa/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
```

如显示，主机这些show命令通过主机组命令配置的全部。您能使用此命令为了验证所有条目是否是可用的并且交叉验证交迭的主机组。