ASA SNMP功能增強實施

目錄

簡介

本檔案介紹軟體版本9.1.5和版本9.2.(1)及更新版本中思科調適型安全裝置(ASA)5500-X系列防火牆可用的新簡易網路管理通訊協定(SNMP)功能。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行Cisco ASA®軟體版本9.1.5和9.2.(1)及更新版本的Cisco ASA 5500-X系

列防火牆。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

在ASA 9.1.5和9.2.1版中，引入了以下SNMP增強功能：

- 新增了對128台SNMP主機的支援。
- 新增了對cpmCPUTotal5minRev SNMP對象識別符號(OID)的支援。
- 新增了對1,472位元組SNMP消息的支援。

支援128個SNMP主機

此功能允許ASA支援超過當前32台SNMP主機。

目的

目前，ASA的硬限製為32個SNMP主機。這包括可以配置陷阱和輪詢的主機。下一節將介紹此功能對單情景模式和多情景模式的影響。

單情景模式

- 允許配置的條目數（主機總數）明顯增加，超過4,096個。但是，在這些條目中，只有128個可用於陷阱。
- 出於輪詢配置目的，允許配置最多4,096個輪詢主機和128個陷阱主機。但是，輪詢系統的實際伺服器數量應限製為少於128台，因為更多主機對效能的影響是未知且不受支援的。

多情景模式

- 出於配置目的，每個情景最多允許4,000台主機，並且系統範圍的總主機數限製為64,000台。
- 在已配置的主機總數中，只有128台（每個情景）可用於陷阱，在多情景模式下陷阱的總系統限製為32,000。
- 雖然每個情景最多可以配置4,000台主機，但輪詢任何情景的實際伺服器數量應限製為128台。

說明

您可能更喜歡從大型SNMP主機池監控網路裝置。理想情況下，您希望能夠指定允許監控網路裝置的IP地址範圍和/或子網。ASA目前不提供這種靈活性，並將最大SNMP主機數限製為32。

此功能的支援涉及兩個方面：

- 為ASA提供處理多達128個SNMP主機的功能。

- 提供所需的配置命令，以便通過單個命令配置更多主機，如上一節中所述。

ASA上的當前設計允許通過CLI配置單個主機。對於此功能，考慮了以下附加設計要求：

- snmp-server host-**group CLI命令和snmp**-server host CLI**命令保留**的簡介。

- 條目可以同時來自**snmp-server host-group**和**snmp-server host** CLI命令。

- 對於SNMP版本3，介紹**snmp-server userlist** CLI命令和**snmp-server user** CLI**命令保留**功能。

- 還必須支援配置重疊。例如，對於網路對象中重疊的主機，可給出多個**host-group**命令。同樣，您可以指定一個IP地址與當前主機或主機組重疊的主機。這提供了一種機制，可用於覆蓋組中少數主機的引數，而無需重新配置整個組。

與此功能相關的一些軟體限制和警告如下：

- 作為**snmp-server host-group**命令的一部分，如果未指定**[trap|poll]**，則預設值為**poll**。還必須注意，對於此命令，不能為同一主機組同時啟用陷阱和輪詢。如果需要，思科建議您對相關主機使用**snmp-server host**命令。

- 可以指定在不同**host**-group命令中**重疊的網路對**象。在最後一個主機組中指定的值對不同網路對象中的一組常見主機生效。

以下是範例：

```
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
```

輸入**show snmp-server host**命令以檢視主機條目：

```
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
```

以下是關於此功能使用的一些重要說明：

- 如果刪除與其他主機組重疊的主機組或主機，則使用已配置主機組的值再次設定主機。
- 與主機相關聯的值或引數取決於命令的執行順序。
- 如果配置的使用者清單由特定主機組使用，則無法刪除該清單。
- 如果在特定使用者清單中引用了使用者，則無法刪除SNMP使用者。
- 如果網路對象由**host-group** CLI命令使**用，則無法**將其刪除。

設定

使用本節中介紹的資訊配置ASA，以便實施此新功能。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

CLI命令

對於SNMP版本3，管理員可以將各種使用者與指定的主機組相關聯。如果管理員希望一組使用者能夠從一組主機訪問ASA，這將非常有用。此CLI命令用於為多個使用者配置使用者清單：

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

要將使用者清單與主機組相關聯，請在CLI中輸入以下命令：

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

使用此命令，可以指定網路對象以指示應新增的多個主機。對於網路對象，您可以使用單個命令指定應新增的子網掩碼或IP地址範圍。列為網路對象一部分的所有IP地址均新增為SNMP主機條目。同樣，對於使用者清單中指定的每個使用者，都有一個單獨的SNMP主機條目。

使用這些命令可允許管理員清除和檢視SNMP伺服器的新配置選項：

- 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

組態範例

完成以下步驟，使用新的SNMP組選項並建立用於版本2c輪詢的SNMP伺服器主機組：

1. 建立網路對象：

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

2. 定義SNMP主機組：

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

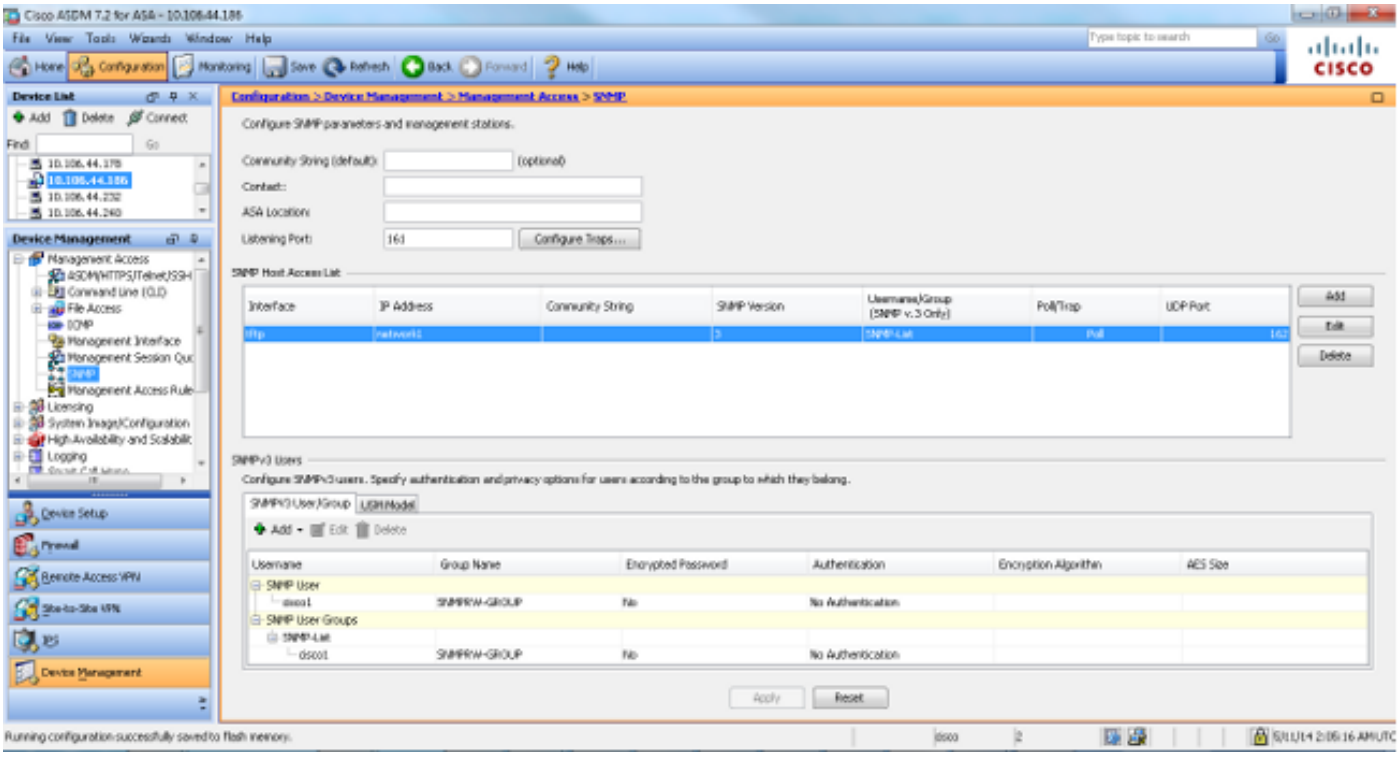
3. 定義SNMP版本3組：

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

4. 將組與使用者關聯：

```
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
```

此圖說明了在思科自適應安全裝置管理器(ASDM)中進行的更改：



支援cpmCPUTotal5minRev SNMP OID

此功能允許ASA支援**cpmCPUTotal5minRev** SNMP OID。

目的

此功能在ASA上新增對**cpmCPUTotal5minRev**和**cpmCPUTotal1minRev** OID的支援，並取消當前支援的OIDs **cpmCPUTotal5min**和**cpmCPUTotal1min**。這些OID的作用是監控CPU使用情況。當前支援的OID範圍從1到100，而新支援的OID範圍從0到100。因此，為較新的OID新增了支援，因為它們覆蓋範圍更廣。

必須注意的是，由於ASA不再支援已過時的OID(**cpmCPUTotal5min**和**cpmCPUTotal1min**)，如果已升級ASA並輪詢已過時的OID，則ASA不會返回這些OID的任何資訊。在ASA升級後，現在需要監視**cpmCPUTotal5minRev**和**cpmCPUTotal1minRev**的CPU使用情況。

CLI命令

此新功能未引入CLI更改。

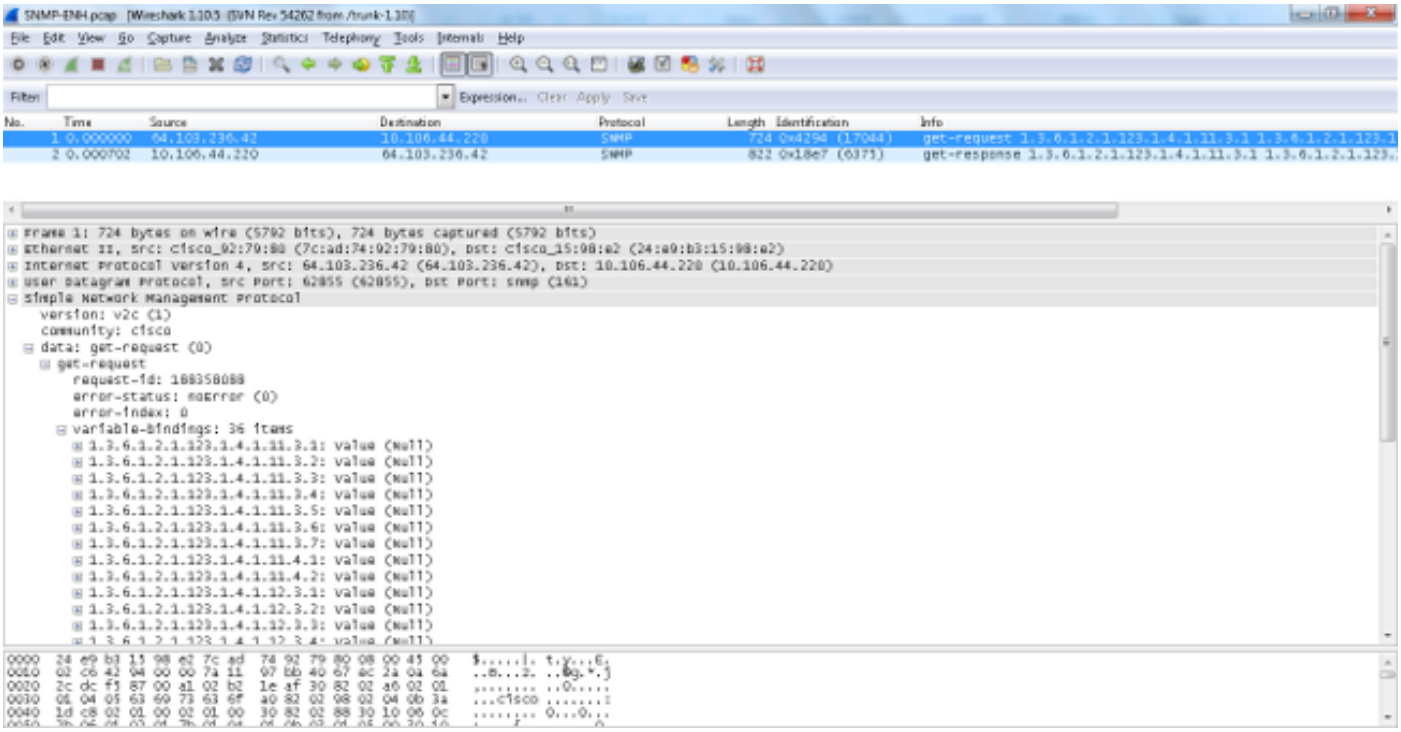
新OID

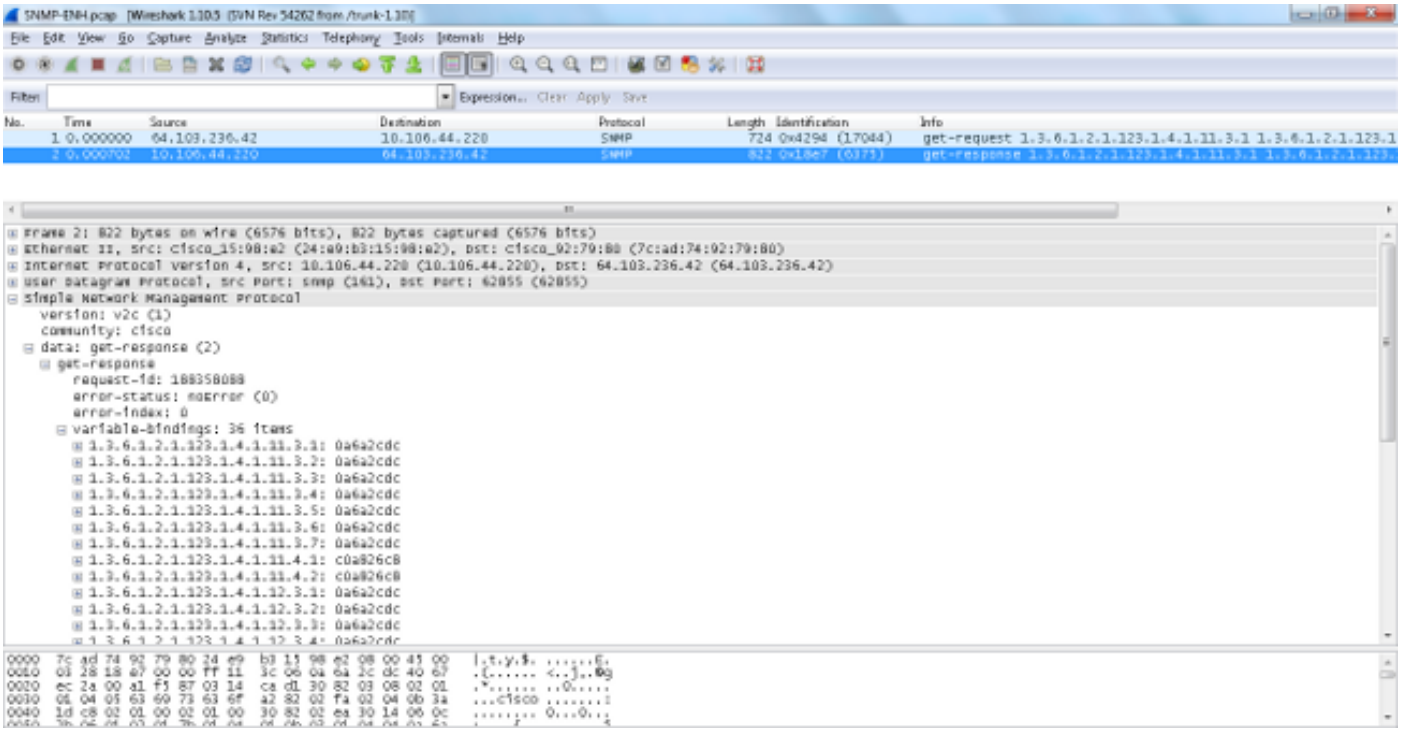
以下是已加入此功能的新OID:

- **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**

支援1,472位元組SNMP消息

ASA平台將SNMP請求的最大資料包大小限製為512位元組。當您在單個SNMP請求內對大量MIB OID執行批次查詢時，ASA上會生成SNMP連線超時和錯誤系統日誌。RFC3417建議SNMP請求的最大資料包大小應為1,472位元組。這是封包的SNMP負載大小。此外，必須新增乙太網報頭和IP報頭大小，才能計算資料包的總大小。





附註：此功能支援單情景和多情景模式。

疑難排解

本節提供的資訊可用於對ASA上的系統問題進行故障排除。

顯示命令

嘗試排除ASA上的問題時，以下**show**命令非常有用：

- 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命令顯示SNMP伺服器地址表中存在的條目，其中包括主機和主機組配置：

```
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
```

如圖所示，這些命令顯示通過**host-group**命令配置的所有主機。您可以使用此命令驗證是否所有條目都可用，也可以交叉驗證重疊的主機組。