

# 在Firepower NGFW裝置上配置SNMP

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [背景資訊](#)

### [設定](#)

#### [FPR4100/FPR9300 的機箱 \(FXOS\) SNMP](#)

[透過 GUI 設定 FXOS SNMPv1/v2c](#)

[透過命令列介面 \(CLI\) 設定 FXOS SNMPv1/v2c](#)

[透過 GUI 設定 FXOS SNMPv3](#)

[透過 CLI 設定 FXOS SNMPv3](#)

#### [FPR4100/FPR9300 的 FTD \(LINA\) SNMP](#)

[設定 LINA SNMPv2c](#)

[設定 LINA SNMPv3](#)

[MIO刀片SNMP統一\(FXOS 2.12.1、FTD 7.2、ASA 9.18.1\)](#)

#### [FPR2100 中的 SNMP](#)

#### [FPR2100 的機箱 \(FXOS\) SNMP](#)

[設定 FXOS SNMPv1/v2c](#)

[設定 FXOS SNMPv3](#)

#### [FPR2100 的 FTD \(LINA\) SNMP](#)

### [驗證](#)

#### [驗證 FPR4100/FPR9300 的 FXOS SNMP](#)

[FXOS SNMPv2c 驗證](#)

[FXOS SNMPv3 驗證](#)

#### [驗證 FPR2100 的 FXOS SNMP](#)

[FXOS SNMPv2 驗證](#)

[FXOS SNMPv3 驗證](#)

#### [驗證 FTD SNMP](#)

#### [允許 SNMP 流量進入 FPR4100/FPR9300 的 FXOS](#)

[透過 GUI 設定全域存取清單](#)

[透過 CLI 設定全域存取清單](#)

[驗證](#)

#### [使用 OID 物件導覽器](#)

### [疑難排解](#)

[無法輪詢 FTD LINA SNMP](#)

[無法輪詢 FXOS SNMP](#)

[要使用什麼 SNMP OID 值？](#)

[無法取得 SNMP 設陷](#)

[無法透過 SNMP 監控 FMC](#)

[Firepower Device Manager \(FDM\) 的 SNMP 組態](#)

[SNMP 疑難排解速查表](#)

---

## 簡介

本檔案介紹如何在下一代防火牆(NGFW) FTD裝置上設定簡易網路管理通訊協定(SNMP)並對其進行疑難排解。

## 必要條件

### 需求

閱讀本文件需具備 SNMP 通訊協定的基本知識。

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

Firepower NGFW 設備可以分成 2 個主要子系統：

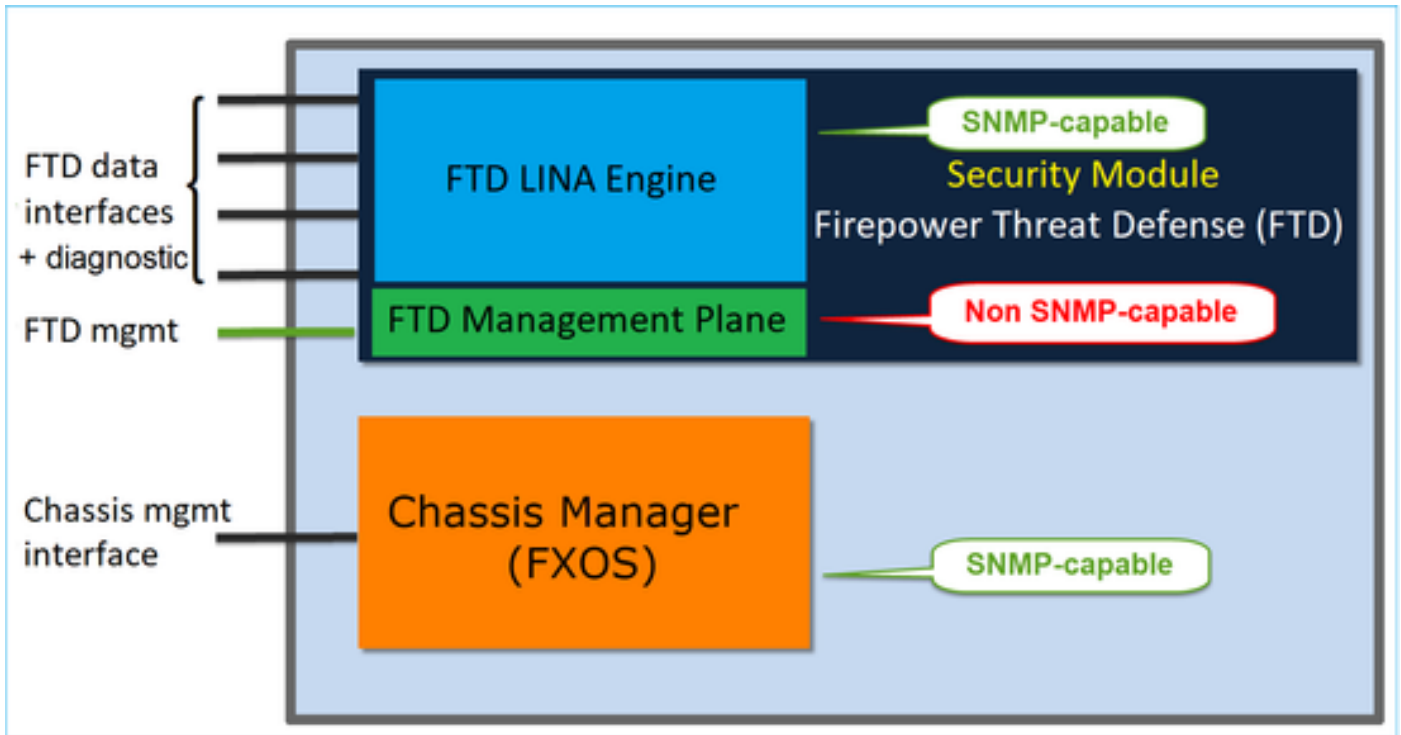
- Firepower Extensible Operating System (FX-OS) 可控制機箱硬體。
- Firepower Threat Defense (FTD) 可在模組內執行。

FTD是一個整合的軟體，其中包括2個主引擎、Snort引擎和LINA引擎。FTD的目前SNMP引擎衍生自傳統ASA，且可看到LINA相關功能。

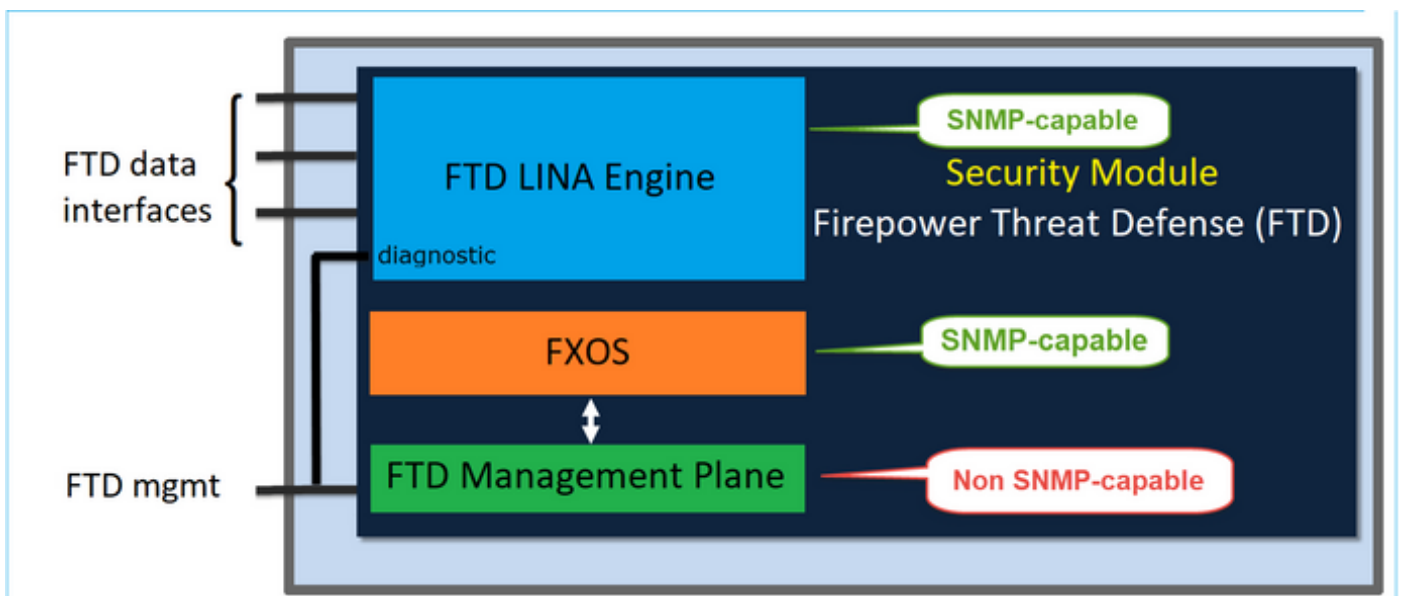
FX-OS和FTD具有獨立的控制平面，並且出於監控目的，它們具有不同的SNMP引擎。每個SNMP引擎都提供不同的資訊，並且可能希望同時監控這兩種資訊，以獲得更全面的裝置狀態檢視。

從硬體角度來看，Firepower NGFW裝置當前有兩個主要架構：Firepower 2100系列和Firepower 4100/9300系列。

Firepower 4100/9300 裝置具有專用的裝置管理介面，而且此介面為傳送到 FXOS 子系統之 SNMP 流量的來源和目的地。另一方面，FTD 應用程式則將 LINA 介面 ( 資料和/或診斷。在 6.6 之後的 FTD 版本中，也可以使用 FTD 管理介面 ) 運用在 SNMP。



Firepower 2100 設備的 SNMP 引擎使用 FTD 管理介面和 IP。設備本身會橋接在此介面上接收到的 SNMP 流量並將其轉送至 FXOS 軟體。

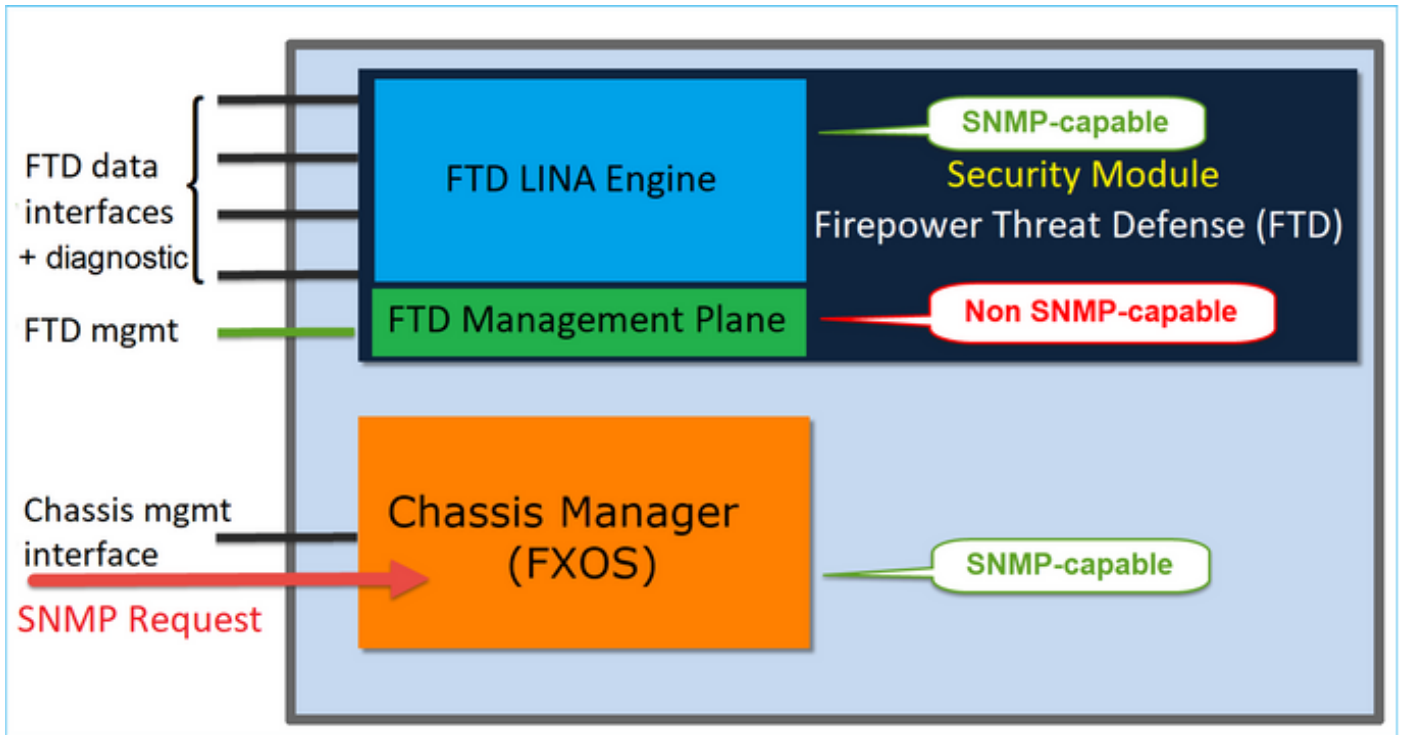


在使用軟體版本 6.6 以的 FTD 上，已導入下列變更。

- 管理介面的 SNMP。
- 在 FPR1000 或 FPR2100 系列平台上，軟體會透過此單一管理介面整合 LINA SNMP 和 FXOS SNMP。此外，軟體也會在「平台設定」>「SNMP」下提供 FMC 的單一組態點。

## 設定

FPR4100/FPR9300 的機箱 (FXOS) SNMP



透過 GUI 設定 FXOS SNMPv1/v2c


步驟 1. 打開 Firepower 機箱管理器 (FCM) UI，然後導航到平台設定 > SNMP 頁籤。勾選「SNMP」的「啟用」核取方塊，指定要用於 SNMP 要求的「社群」字串，然後選擇「儲存」。

The screenshot shows the **Platform Settings** page for SNMP configuration. The left sidebar lists various settings, with **SNMP** selected. The main content area shows the following configuration options:

- Admin State:**  **Enable** (1)
- Port:** 161
- Community/Username:** [.....] **Set: No** (2)
- System Administrator Name:** [ ]
- Location:** [ ]

Below these fields are sections for **SNMP Traps** and **SNMP Users**, each with an **Add** button (4).

At the bottom of the page, there are **Save** and **Cancel** buttons (3).

 註：如果已設定Community/Username欄位，則空白欄位右側的文本為Set：Yes。如果Community/Username欄位尚未填加值，則空白欄位右側的文本為Set：No

步驟 2. 配置SNMP陷阱目標伺服器。

## Add SNMP Trap

Host Name:\*


Community/Username:\*

Port:\*

Version:  V1  V2  V3

Type:  Traps  Informs

V3 Privilege:  Auth  NoAuth  Priv

 注意：查詢和陷阱主機的社群值是獨立的，可以不同

主機可定義為 IP 位址或依名稱定義。選取「確定」，系統便會自動儲存 SNMP 設陷伺服器的組態。您不需要選取 SNMP 主頁面中的儲存按鈕。在刪除主機時也是如此。

透過命令列介面 (CLI) 設定 FXOS SNMPv1/v2c

```
<#root>
```

```
ksec-fpr9k-1-A#
```

```
scope monitoring
```

```
ksec-fpr9k-1-A /monitoring #
```

```
enable snmp
ksec-fpr9k-1-A /monitoring* #
set snmp community
Enter a snmp community:
ksec-fpr9k-1-A /monitoring* #
  enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v2c
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype traps
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set port 162
ksec-fpr9k-1-A /monitoring/snmp-trap* #
exit
ksec-fpr9k-1-A /monitoring* #
  commit-buffer
```

## 透過 GUI 設定 FXOS SNMPv3

步驟 1. 打開FCM並導航到Platform Settings > SNMP頁籤。

步驟 2. 對於SNMP v3，不需要在上部分設定任何社群字串。建立的每個使用者都可以順利執行對FXOS SNMP 引擎的查詢。第一個步驟是在平台中啟用SNMP。完成後，即可建立使用者和目的地設陷主機。系統會自動儲存SNMP使用者和SNMP設陷主機。

Admin State:  Enable **1**

Port: 161

Community/Username:  Set: No

System Administrator Name:

Location:

SNMP Traps

**4**

Name	Port	Version	V3 Privilege	Type
------	------	---------	--------------	------

SNMP Users

**3**

Name	Auth Type	AES-128
------	-----------	---------

**2**

步驟 3.如圖所示，增加SNMP使用者。驗證類型一律為 SHA，但您可以使用 AES 或 DES 進行加密：

**Add SNMP User** ? X

Name:\*

Auth Type: SHA

Use AES-128:

Password:

Confirm Password:

Privacy Password:

Confirm Privacy Password:

步驟 4.增加SNMP陷阱主機，如圖所示：



### Add SNMP Trap

Host Name:\* 192.168.10.100

Community/Username:\* ●●●●●●

Port:\* 162

Version:  V1  V2  V3

Type:  Traps  Informs

V3 Privilege:  Auth  NoAuth  Priv

OK Cancel

#### 透過 CLI 設定 FXOS SNMPv3

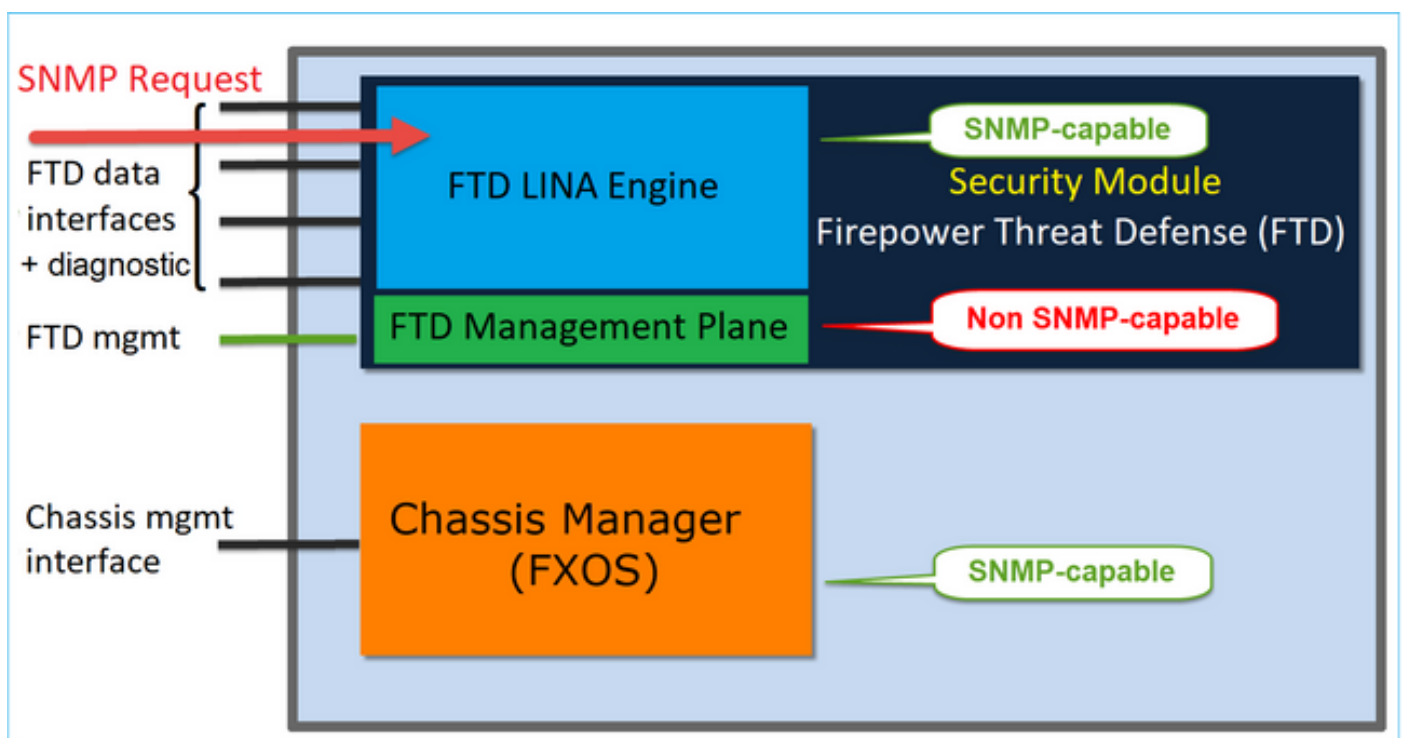
```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring #
create snmp-user user1
Password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set auth sha
ksec-fpr9k-1-A /monitoring/snmp-user* #
set priv-password
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
```

```

set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter snmp-trap 10.48.26.190
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v3
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype traps
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set port 162
ksec-fpr9k-1-A /monitoring/snmp-trap* #
exit
ksec-fpr9k-1-A /monitoring* #
commit-buffer

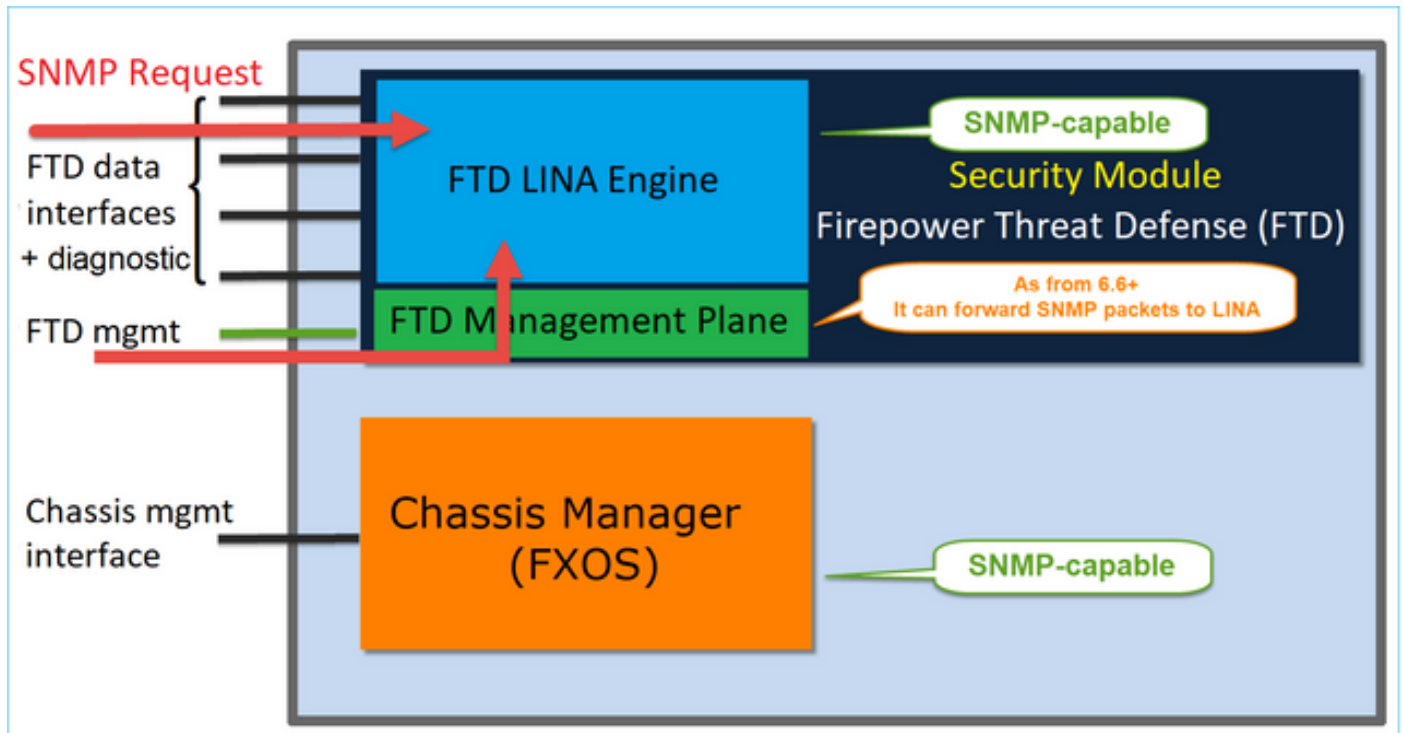
```

## FPR4100/FPR9300 的 FTD (LINA) SNMP



## 6.6 以上版本的變更

- 在 6.6 之後的版本中，您也可以選擇使用 FTD 管理介面進行輪詢和設陷。



從 6.6 開始，所有 FTD 平台均支援 SNMP 單一 IP 管理功能：

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- 執行 FTD 的 ASA5500
- FTDv

### 設定 LINA SNMPv2c

步驟 1. 在 FMC UI 上，導航到裝置 > 平台設定 > SNMP。選中 Enable SNMP Servers 選項並配置 SNMPv2 設定，如下所示：

步驟 2. 在主機頁籤上，選擇增加按鈕並指定 SNMP 伺服器設定：

### Edit SNMP Management Hosts

IP Address\*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port  (1 - 65535)

**Available Zones**

- INSIDE\_FTD4110
- OUTSIDE1\_FTD4110
- OUTSIDE2\_FTD4110
- NET1\_4100-3
- NET2\_4100-3
- NET3\_4100-3

**Selected Zones/Interfaces**

- OUTSIDE3

您也可以將診斷介面指定為 SNMP 訊息的來源。此診斷介面為資料介面，只允許輸入機箱和輸出機箱的流量（僅供管理）。

## Add SNMP Management Hosts



IP Address\*

SNMP-SERVER



SNMP Version

2c

Username



Community String

Confirm

Poll

Trap

Trap Port

162

(1 - 65535)

Reachable By:

Device Management Interface *(Applicable from v6.6.0 and above)*

Security Zones or Named Interface

Available Zones



Search

2100\_inside  
2100\_outside  
cluster\_dmz  
cluster\_inside  
cluster\_outside

Add

Selected Zones/Interfaces

diagnostic



Interface Name

Add

Cancel

OK

此圖為 6.6 版本中的畫面並使用「淺色佈景主題」。

此外，在 6.6 之後的 FTD 版本中，您也可以選擇管理介面：

## Add SNMP Management Hosts

IP Address\*

SNMP-SERVER



SNMP Version

2c

Username

Community String

Confirm

Poll

Trap

Trap Port

162

(1 - 65535)

Reachable By:

Device Management Interface *(Applicable from v6.6.0 and above)*

Security Zones or Named Interface

Available Zones

Search

2100\_inside  
2100\_outside  
cluster\_dmz  
cluster\_inside  
cluster\_outside

Add

Selected Zones/Interfaces

diagnostic

Interface Name

Add

Cancel

OK

如果選取新的管理介面，即可透過新的管理介面使用 LINA SNMP。

結果：

Interface	Network	SNMP Version	Poll/Trap	Port	Username
OUTSIDE3	SNMP-SERVER	2c	Poll		

### 設定 LINA SNMPv3

步驟 1. 在FMC UI上，導航到裝置>平台設定> SNMP。選中啟用SNMP伺服器選項並配置SNMPv3使用者和主機：

**Add Username**

Security Level: Priv

Username\*: cisco

Encryption Password Type: Clear Text

Auth Algorithm Type: SHA

Authentication Password\*: .....

Confirm\*: .....

Encryption Type: AES128

Encryption Password\*: .....

Confirm\*: .....

OK Cancel



Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS **Platform Settings** FlexConfig Certificates

### mzafeiro\_FTD4110-HA

Enter Description

- ARP Inspection
- Banner
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Port  (1 - 65535)

**Hosts** Users SNMP Traps

Interface	Network	SNMP Version	Poll/Trap	Port	Username
OUTSIDE3	SNMP-SERVER	3	Poll		cisco

步驟 2.同時配置主機以接收陷阱：

### Edit SNMP Management Hosts

IP Address\*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port  (1 - 65535)

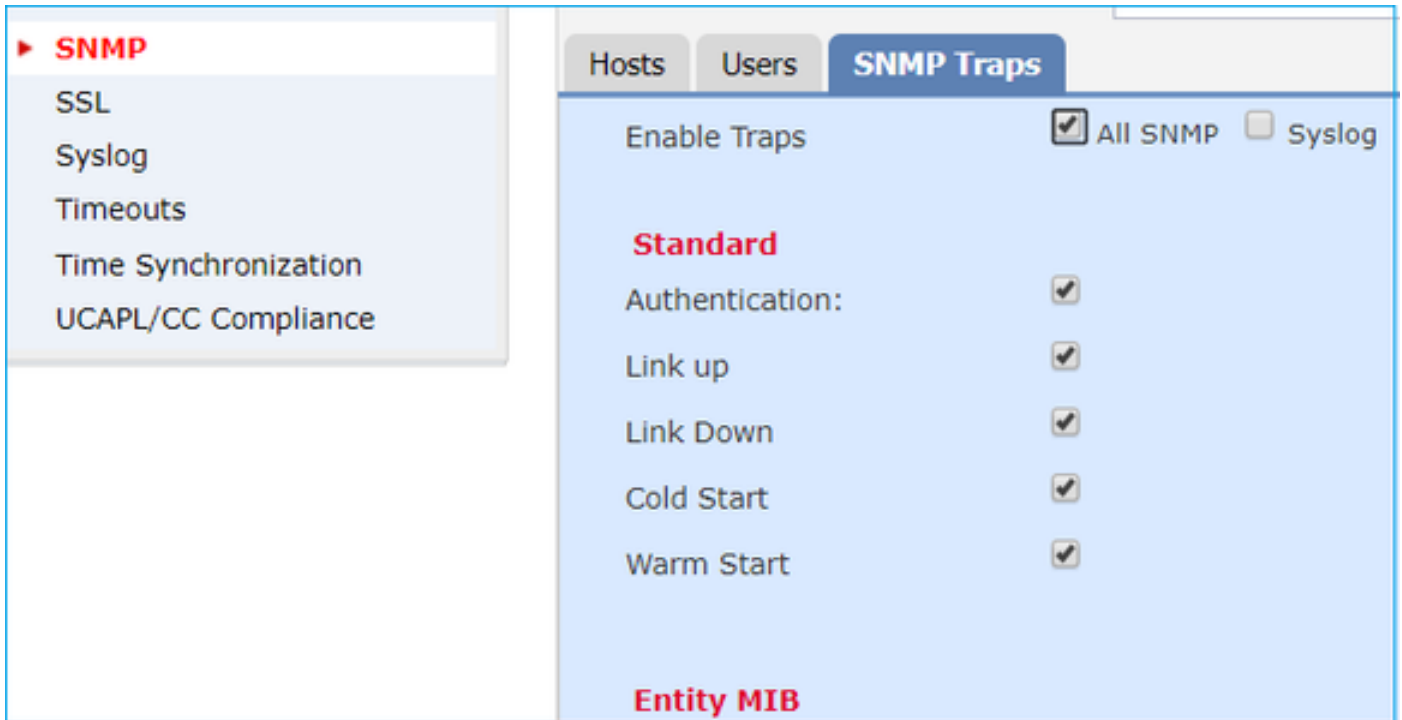
**Available Zones**

INSIDE\_FTD4110

**Selected Zones/Interfaces**

OUTSIDE3

步驟 3.可以在SNMP陷阱部分下選擇要接收的陷阱：



MIO刀片SNMP統一(FXOS 2.12.1、FTD 7.2、ASA 9.18.1)

7.2之前的行為

- 在9300和4100平台上，無法在FTD/ASA應用程式上設定的SNMP上使用機箱資訊的SNMP MIB。它需要在MIO上透過機箱管理器單獨配置並單獨訪問。MIO是管理和I/O (Supervisor)模組。
- 需要配置兩個獨立的SNMP策略，一個在刀片/應用上，另一個在MIO上，以進行SNMP監控。
- 使用單獨的埠，一個用於刀片，一個用於MIO，用於同一裝置的SNMP監控。
- 當您嘗試透過SNMP設定和監控9300和4100裝置時，這可能會造成複雜性。

其在新版本 ( FXOS 2.12.1、FTD 7.2、ASA 9.18.1及更高版本 ) 上的運作方式

- 使用MIO刀片SNMP統一，使用者可以透過應用(ASA/FTD)介面輪詢LINA和MIO MIB。
- 可透過新的MIO CLI和FCM ( 機箱管理器 ) 使用者介面啟用或停用此功能。
- 預設狀態為停用。這意味著MIO SNMP代理作為獨立例項運行。需要使用MIO介面輪詢機箱/DME MIB。啟用該功能後，應用程式介面可用於輪詢相同的MIB。
- 該配置位於機箱管理器UI的Platform-settings > SNMP > Admin Instance下，使用者可以在其中指定FTD例項，以便整理/收集機箱MIB以將其提供給NMS
- 支援ASA/FTD本地和MI應用。
- 此功能僅適用於基於MIO的平台 ( FPR9300和FPR4100 )。

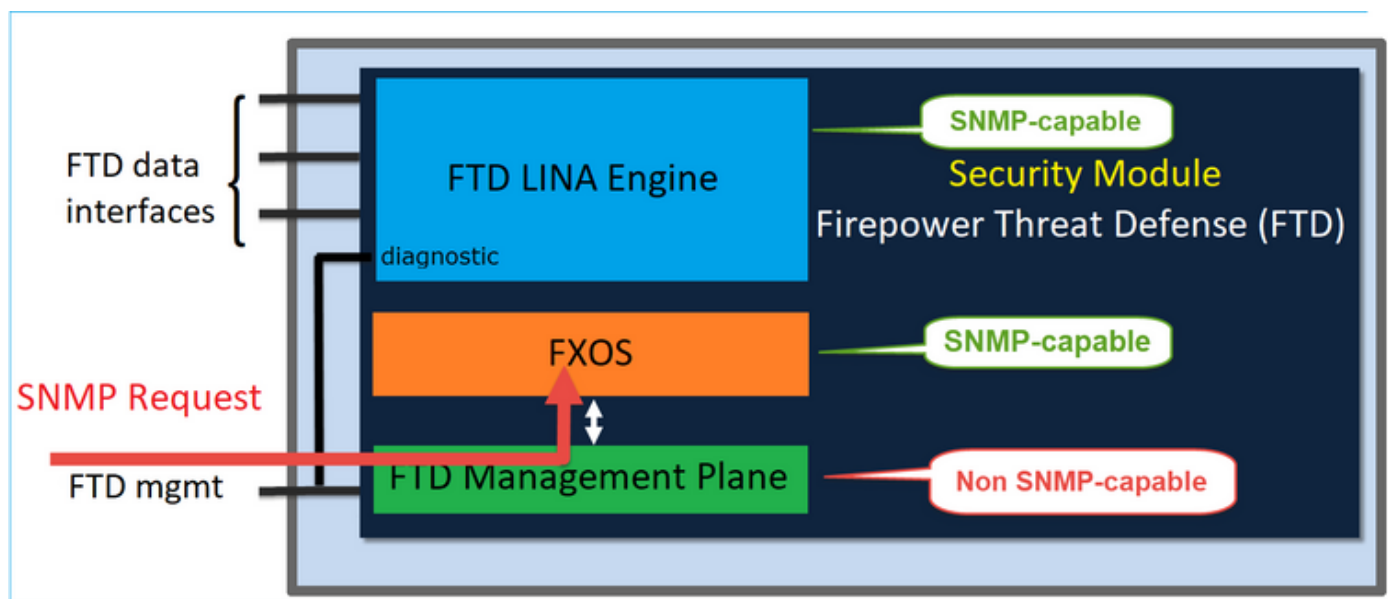
先決條件，支援的平台

- 支援的最低管理員版本：FCM 2.12.1
- 受管裝置：FPR9300/FP4100系列
- 需要支援的最低受管裝置版本：FXOS 2.12.1、FTD 7.2或ASA 9.18.1

FPR2100 中的 SNMP

FPR2100 系統上沒有 FCM。您只能透過 FMC 來設定 SNMP。

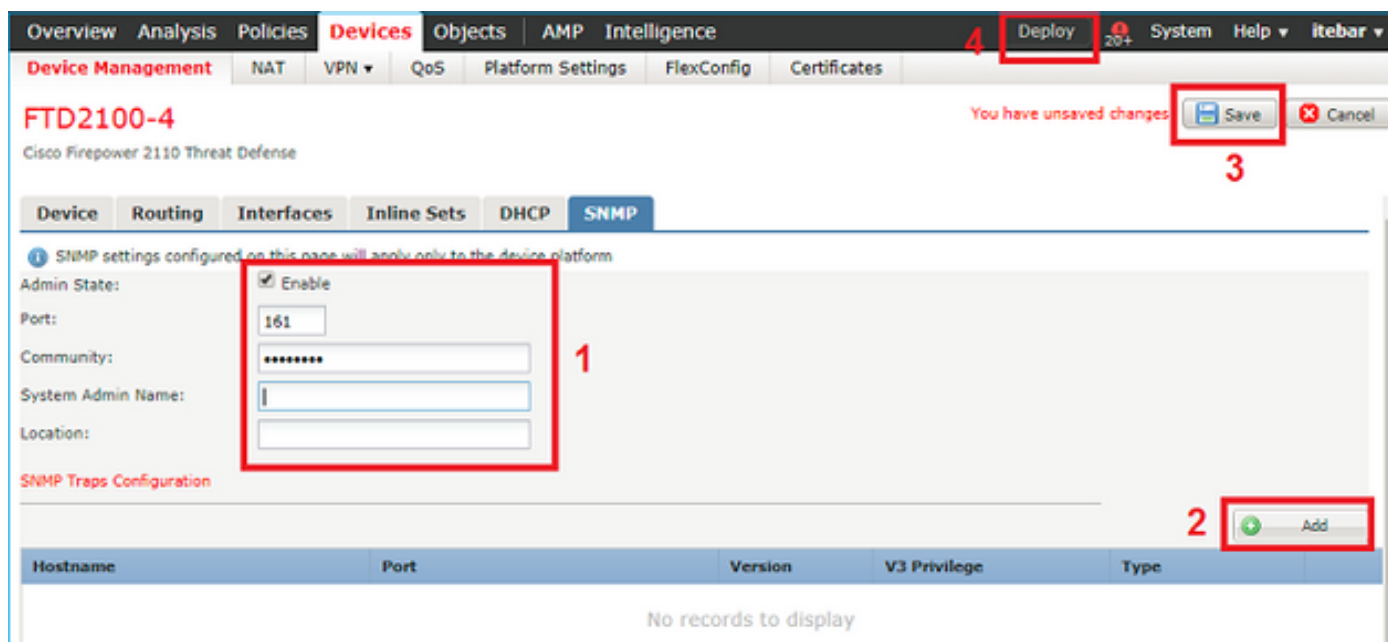
## FPR2100 的機箱 (FXOS) SNMP




從 FTD 6.6 以上開始，您也可以選擇使用 SNMP 的 FTD 管理介面。在此案例中，FXOS 和 LINA SNMP 資訊是透過 FTD 管理介面傳輸。

## 設定 FXOS SNMPv1/v2c

打開FMC UI，導航到裝置>裝置管理。選擇裝置並選擇SNMP：



### SNMP Trap Configuration

Hostname:\* 10.48.26.190 

Community String:\* .....

Port:\* 162 (1 - 65535)

SNMP Version: V2

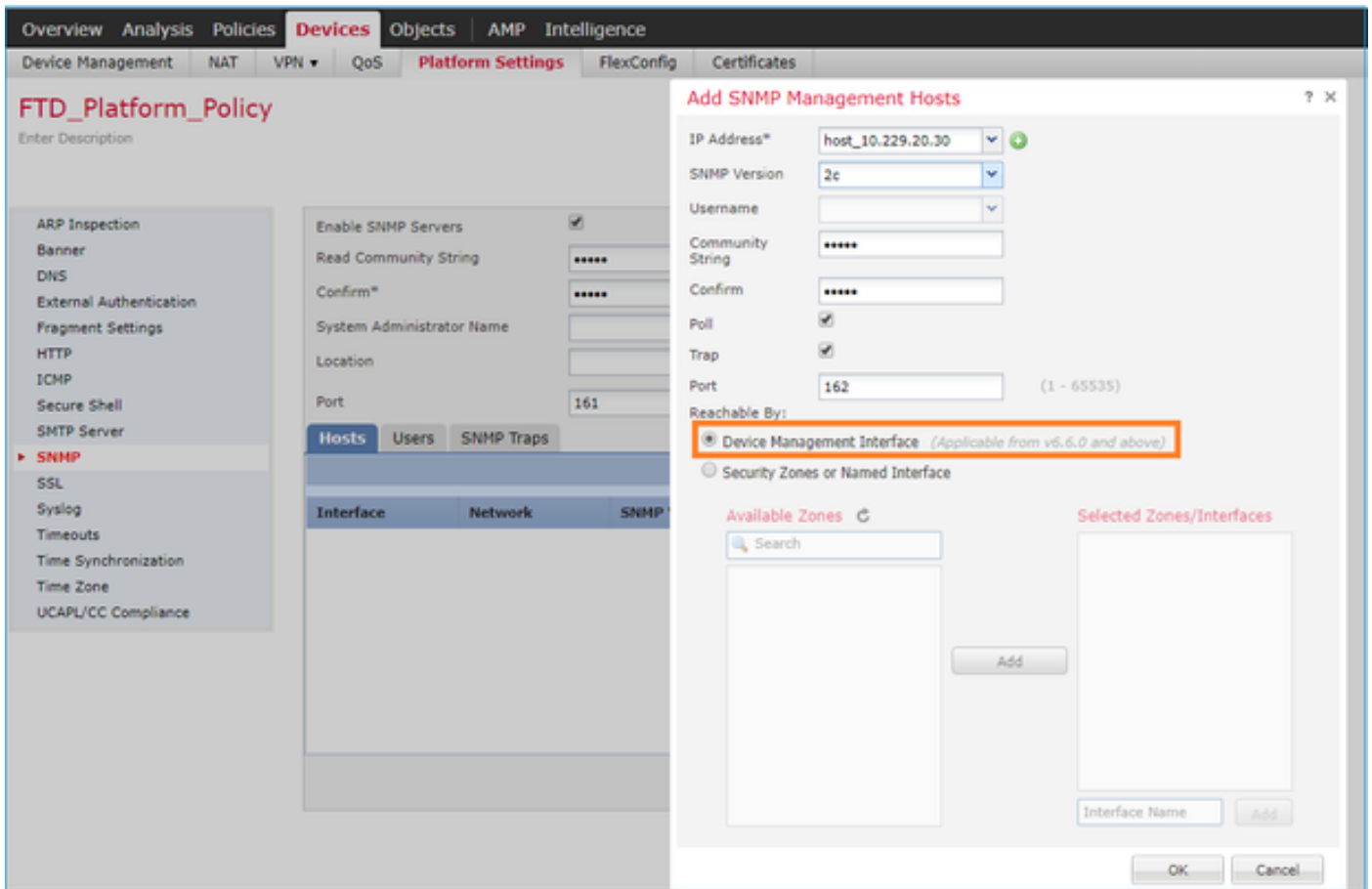
Type: TRAPS

Privilege: NO\_AUTH

OK Cancel

FTD 6.6 以上的變更

您可以指定 FTD 管理介面：



由於也可以針對 SNMP 設定管理介面，因此頁面會顯示以下警告訊息：

如果透過 Devices > Platform Settings (Threat Defense) > SNMP > Hosts 使用裝置管理介面配置了 SNMP 設定，則會停用此頁上的裝置平台 SNMP 配置。

### 設定 FXOS SNMPv3

打開 FMC UI，導航至選擇裝置 > 裝置管理。選擇裝置並選擇 SNMP。

Overview Analysis Policies **Devices** Objects AMP Intelligence 5 Deploy 20+ System Help ▾ itebar ▾

**Device Management** NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

**FTD2100-4** You have unsaved changes Save Cancel

Cisco Firepower 2110 Threat Defense 4

Device Routing Interfaces Inline Sets DHCP **SNMP**

SNMP settings configured on this page will apply only to the device platform

Admin State:  Enable 1

Port: 161

Community:

System Admin Name:

Location:

SNMP Traps Configuration 3 + Add

Hostname	Port	Version	V3 Privilege	Type
No records to display				

SNMP Users Configuration 2 + Add

Name	Auth Type	AES-128
No records to display		

## SNMP User Configuration ? X

Username: \*

Auth Algorithm Type:  ▾

Use AES:

Password\*:

Confirm:

Privacy Password\*:

Confirm:

### SNMP Trap Configuration

Hostname:\*  +

Community String:\*

Port:\*  (1 - 65535)

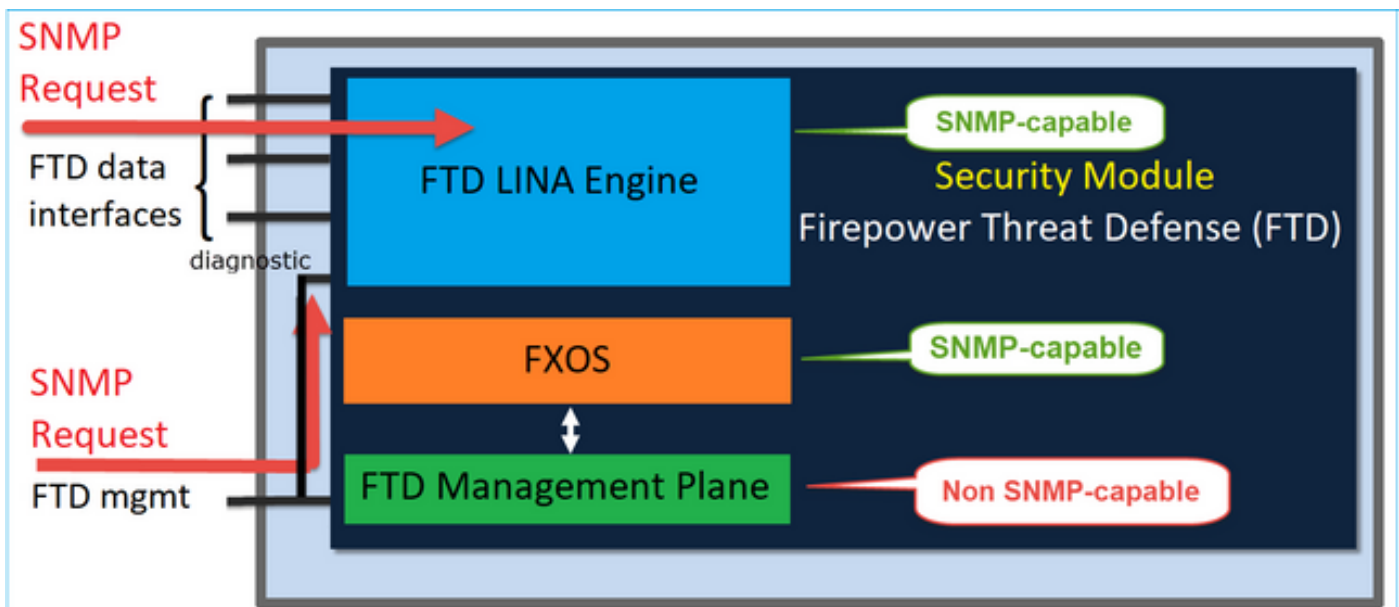
SNMP Version:

Type:

Privilege:

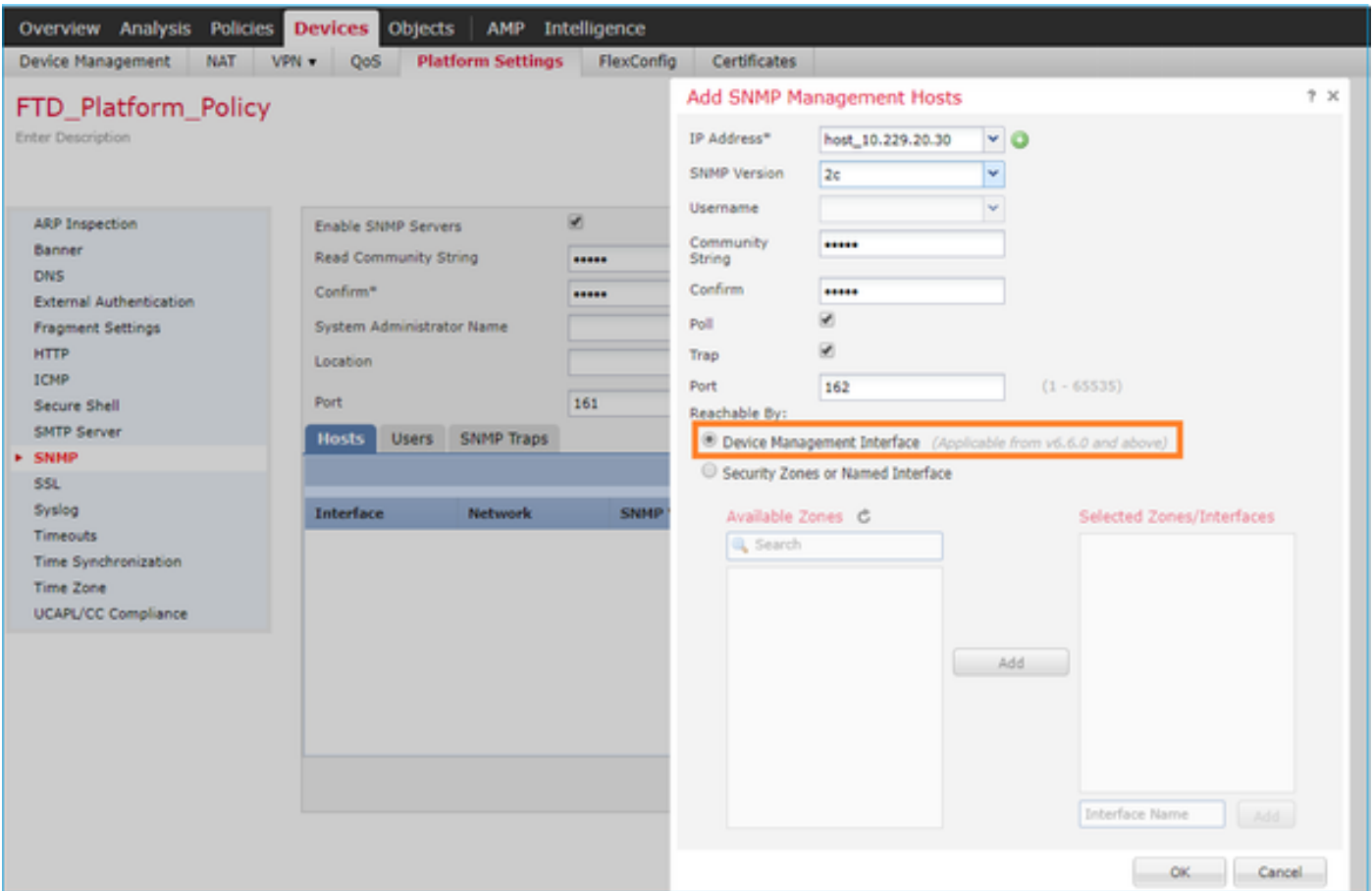
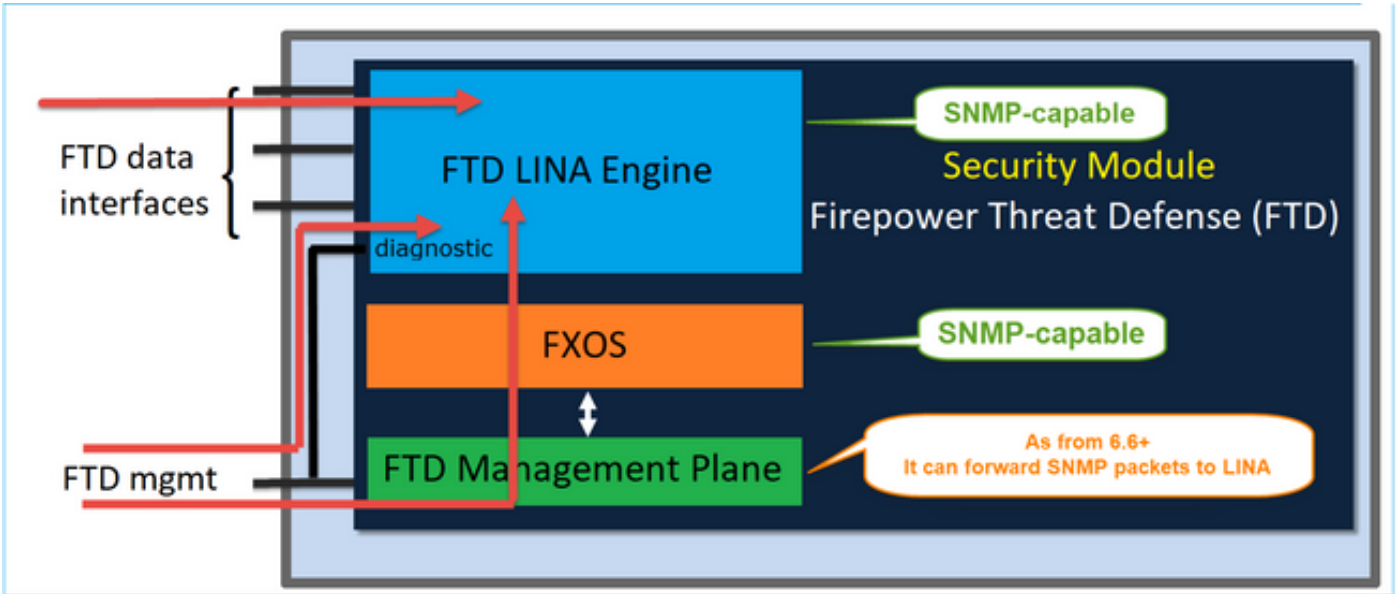
### FPR2100 的 FTD (LINA) SNMP

- 如果是 6.6 之前的版本，則 FTD FP1xxx/FP21xx 設備的 LINA FTD SNMP 組態與 Firepower 4100 或 9300 設備的 FTD 相同。



FTD 6.6 以上版本

- 在 6.6 之後的版本中，您也可以選擇使用 FTD 管理介面進行 LINA 輪詢和設陷。



如果選取新的管理介面：

- 將可透過管理介面使用 LINA SNMP。
- 在「裝置」>「裝置管理」下，「SNMP」標籤將會停用，因為不再需要此標籤。系統會顯示通知橫幅。只有在 2100/1100 平台上才會顯示 SNMP 裝置標籤。此頁面不存在於 FPR9300/FPR4100 和 FTD55xx 平台上。

設定完成後，合併的 LINA SNMP + FXOS ( 在 FP1xxx/FP2xxx 上 ) SNMP 輪詢/設陷資訊會位於



FTD 管理介面上方。

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

**FTD2100-6**  
Cisco Firepower 2140 Threat Defense

Device Routing Interfaces Inline Sets DHCP **SNMP**

⚠ Device platform SNMP setting configuration on this page is deprecated and the same will be configurable through **Devices > Platform Settings (Threat Defense) > SNMP > Hosts** with Device Management Interface.

SNMP settings configured on this page will apply only to the device platform

Admin State:  Enable

Port:

Community:

System Admin Name:

Location:

SNMP Traps Configuration

Hostname	Port	Version	V3 Privilege	Type
No records to display				

從 6.6 開始，所有 FTD 平台均支援 SNMP 單一 IP 管理功能：

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- 執行 FTD 的 ASA5500
- FTDv

如需詳細資料，請查看「設定 Threat Defense 的 SNMP」

## 驗證

驗證 FPR4100/FPR9300 的 FXOS SNMP

FXOS SNMPv2c 驗證

CLI 組態驗證：

```
<#root>
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

```
Sys Contact:
```

```
Sys Location:
```

```
ksec-fpr9k-1-A /monitoring # show snmp-trap
```

```
SNMP Trap:
  SNMP Trap          Port      Community  Version V3 Privilege Notification Type
  -----
  192.168.10.100    162      V2c        Noauth    Traps
```

從 FXOS 模式 :

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show run snmp
```

```
!Command: show running-config snmp
!Time: Mon Oct 16 15:41:09 2017
```

```
version 5.0(3)N2(4.21)
snmp-server host 192.168.10.100 traps version 2c cisco456
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
... All traps will appear as enable ...
snmp-server enable traps flexlink ifStatusChange
snmp-server context mgmt vrf management
snmp-server community cisco123 group network-operator
```

其他驗證 :

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp host
```

```
-----
Host          Port Version  Level  Type  SecName
-----
192.168.10.100  162  v2c      noauth trap  cisco456
-----
```

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp
```

```
Community      Group / Access  context  acl_filter
-----
cisco123      network-operator
```

```
...
```

測試 SNMP 要求.

從有效主機執行SNMP請求。

確認產生設陷.

您可以在啟用 Ethalyzer 的情況下，藉由翻動介面來確認 SNMP 設陷是否已產生並傳送至定義的設陷主機：

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
ethalyzer local interface mgmt capture-filter "udp port 162"
```

```
Capturing on eth0
```

```
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
```

```
2017-11-17 09:01:35.954624 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```

```
2017-11-17 09:01:36.054511 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```



警告：介面抖動可能導致流量中斷。請僅在實驗室環境或維護時段執行此測試

---

## FXOS SNMPv3 驗證

步驟 1. 打開FCM UI Platform Settings > SNMP > User，顯示是否配置了任何密碼和隱私密碼：

## Edit user1

?
X

Name:\*

Auth Type: SHA

Use AES-128:

Password:  Set:Yes

Confirm Password:

Privacy Password:  Set:Yes

Confirm Privacy Password:

---

OK
Cancel

步驟 2.在CLI中，可以在作用域monitoring下驗證SNMP配置：

```
<#root>
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp
```

```
Name: snmp
  Admin State: Enabled
  Port: 161
  Is Community Set: No
  Sys Contact:
  Sys Location:
```

```
ksec-fpr9k-1-A /monitoring # show snmp-user
```

```
SNMPv3 User:
  Name                Authentication type
  -----
  user1                Sha
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp-user detail
```

```
SNMPv3 User:
```

```
Name: user1
Authentication type: Sha
Password: ****
Privacy password: ****
Use AES-128: Yes
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp-trap
```

```
SNMP Trap:
```

SNMP Trap	Port	Community	Version	V3 Privilege	Notification Type
192.168.10.100	162		V3	Priv	Traps

步驟 3.在FXOS模式下，您可以展開SNMP配置和詳細資訊：

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show running-config snmp all
```

```
...
snmp-server user user1 network-operator auth sha 0x022957ee4690a01f910f1103433e4b7b07d4b5fc priv aes-128
snmp-server host 192.168.10.100 traps version 3 priv user1
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp user
```

```
SNMP USERS
```

User	Auth	Priv(enforce)	Groups
user1	sha	aes-128(yes)	network-operator

```
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
```

User	Auth	Priv

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp host
```

Host	Port	Version	Level	Type	SecName
10.48.26.190	162	v3	priv	trap	user1

測試 SNMP 要求.

您可以驗證配置，並從任何具有SNMP功能的裝置發出SNMP請求。

若要檢查 SNMP 要求的處理狀態，您可以使用 SNMP 偵錯：


```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
debug snmp pkt-dump
```

```
ksec-fpr9k-1-A(fxos)# 2017 Oct 16 17:11:54.681396 snmpd: 1281064976.000000:iso.10.10.1.1.10.10.10.10.1 :  
2017 Oct 16 17:11:54.681833 snmpd:  SNMPPKTSTRT: 3.000000 161 1281064976.000000 1647446526.000000 0.000000  
2017 Oct 16 17:11:54.683952 snmpd: 1281064976.000000:iso.10.10.1.2.10.10.10.10.2.83886080 = STRING: "mg  
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.000000
```

---

 注意：調試可能會影響裝置效能。

---

## 驗證 FPR2100 的 FXOS SNMP

### FXOS SNMPv2 驗證

透過 CLI 檢查組態：

```
<#root>
```

```
FP2110-4 /monitoring #
```

```
show snmp
```

```
Name: snmp  
Admin State: Enabled  
Port: 161  
Is Community Set: Yes  
Sys Contact:  
Sys Location:
```

```
FP2110-4 /monitoring #
```

```
show snmp-trap
```

```
SNMP Trap:  
SNMP Trap          Port      Version V3 Privilege Notification Type  
-----  
10.48.26.190      162      V2c      Noauth      Traps
```

確認 SNMP 行為。

您可以驗證您是否能夠輪詢FXOS並從主機或任何具有SNMP功能的裝置傳送SNMP請求。

使用 capture-traffic 命令以查看 SNMP 要求和回應：

<#root>

>

capture-traffic

Please choose domain to capture traffic from:

0 - management0

Selection?

0

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options:

udp port 161

HS\_PACKET\_BUFFER\_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes

13:50:50.521383 IP 10.48.26.190.42224 > FP2110-4.snmp: C=cisco123 GetNextRequest(29) interfaces.ifTab

13:50:50.521533 IP FP2110-4.snmp > 10.48.26.190.42224: C=cisco123 GetResponse(32) interfaces.ifTable.

^C

Caught interrupt signal

Exiting.

2 packets captured

2 packets received by filter

0 packets dropped by kernel

## FXOS SNMPv3 驗證

透過 CLI 檢查組態：

<#root>

FP2110-4 /monitoring #

show snmp

Name: snmp

Admin State: Enabled

Port: 161

Is Community Set: No

Sys Contact:

Sys Location:

FP2110-4 /monitoring #

show snmp-user detail

SNMPv3 User:

Name: user1

Authentication type: Sha

Password: \*\*\*\*

Privacy password: \*\*\*\*

```
Use AES-128: Yes
FP2110-4 /monitoring #
```

```
show snmp-trap detail
```

```
SNMP Trap:
SNMP Trap: 10.48.26.190
Port: 163
Version: V3
V3 Privilege: Priv
Notification Type: Traps
```

確認 SNMP 行為。

傳送SNMP請求以驗證您能夠輪詢FXOS。

此外，您還可以擷取要求：

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management0
```

```
Selection?
```

```
0
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options:
```

```
udp port 161
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
14:07:24.016590 IP 10.48.26.190.38790 > FP2110-4.snmp: F=r U= E= C= [|snmp]
```

```
14:07:24.016851 IP FP2110-4.snmp > 10.48.26.190.38790: F= [|snmp][|snmp]
```

```
14:07:24.076768 IP 10.48.26.190.38790 > FP2110-4.snmp: F=apr [|snmp][|snmp]
```

```
14:07:24.077035 IP FP2110-4.snmp > 10.48.26.190.38790: F=ap [|snmp][|snmp]
```

```
^C4 packets captured
```

```
Caught interrupt signal
```

```
Exiting.
```

```
4 packets received by filter
```

```
0 packets dropped by kernel
```



## 驗證 FTD SNMP

若要驗證 FTD LINA SNMP 組態：

```
<#root>
```

```
Firepower-module1#
```

```
show run snmp-server
```

```
snmp-server host OUTSIDE3 10.62.148.75 community ***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
```

在 6.6 之後的 FTD 版本中，您可以設定並使用 SNMP 的 FTD 管理介面：

```
<#root>
```

```
firepower#
```

```
show running-config snmp-server
```

```
snmp-server group Priv v3 priv
snmp-server group NoAuth v3 noauth
snmp-server user uspriv1 Priv v3 engineID
80000009fe99968c5f532fc1f1b0dbdc6d170bc82776f8b470 encrypted auth sha256
6d:cf:98:6d:4d:f8:bf:ee:ad:01:83:00:b9:e4:06:05:82:be:30:88:86:19:3c:96:42:3b
:98:a5:35:1b:da:db priv aes 128
6d:cf:98:6d:4d:f8:bf:ee:ad:01:83:00:b9:e4:06:05
snmp-server user usnoauth NoAuth v3 engineID
80000009fe99968c5f532fc1f1b0dbdc6d170bc82776f8b470
snmp-server host ngfw-management 10.225.126.168 community ***** version 2c
snmp-server host ngfw-management 10.225.126.167 community *****
snmp-server host ngfw-management 10.225.126.186 version 3 uspriv1
no snmp-server location
no snmp-server contact
```

其他驗證：

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

```
host ip = 10.62.148.75, interface = OUTSIDE3 poll community ***** version 2c
```

從 SNMP 伺服器 CLI 執行 snmpwalk：

```
<#root>
```

```
root@host:/Volume/home/admin#
```

```
snmpwalk -v2c -c cisco -OS 10.62.148.48
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 10.2.3.1 (Build 43), ASA Versi
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2313
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8350600) 23:11:46.00
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: Firepower-module1
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 4
IF-MIB::ifNumber.0 = INTEGER: 10
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifIndex.11 = INTEGER: 11
...
```

驗證 SNMP 流量統計資料。

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server statistics
```

```
1899 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  1899 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  1899 Get-next PDUs
  0 Get-bulk PDUs
  0 Set-request PDUs (Not supported)
1904 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  1899 Response PDUs
  5 Trap PDUs
```

## 允許 SNMP 流量進入 FPR4100/FPR9300 的 FXOS

FPR4100/9300 的 FXOS 組態可以限制每個來源 IP 位址的 SNMP 存取。「存取清單」組態區段會定義可透過 SSH、HTTPS 或 SNMP 連線到裝置的網路/主機。您必須確保允許來自 SNMP 伺服器的 SNMP 查詢。

## 透過 GUI 設定全域存取清單

The screenshot shows the 'Platform Settings' page in a network management GUI. The left sidebar contains a menu with 'Access List' selected. The main content area is divided into two sections: 'Ipv4 Access List' and 'Ipv6 Access List'. Each section has an 'Add' button and a table of entries. In the IPv4 section, the entry for '0.0.0.0' with a prefix length of '0' and protocol 'snmp' is highlighted with a red rectangle. The IPv6 section shows similar entries for '::' with protocol 'snmp'.

IP Address	Prefix Length	Protocol	
0.0.0.0	0	https	
0.0.0.0	0	snmp	
0.0.0.0	0	ssh	

IP Address	Prefix Length	Protocol	
::	0	https	
::	0	snmp	
::	0	ssh	

## 透過 CLI 設定全域存取清單

```
<#root>  
ksec-fpr9k-1-A#  
scope system  
ksec-fpr9k-1-A /system #  
  scope services  
ksec-fpr9k-1-A /system/services #  
enter ip-block 0.0.0.0 0 snmp  
ksec-fpr9k-1-A /system/services/ip-block* #  
commit-buffer
```

## 驗證

```
<#root>
```

```
ksec-fpr9k-1-A /system/services #
```

```
show ip-block
```

Permitted IP Block:

IP Address	Prefix Length	Protocol
0.0.0.0	0	https
0.0.0.0	0	snmp
0.0.0.0	0	ssh

## 使用 OID 物件導覽器

[Cisco SNMP Object Navigator](#) 是一種線上工具，您可以在當中轉譯不同的 OID 並取得簡短說明。

Tools & Resources

# SNMP Object Navigator

HOME | SUPPORT | TOOLS & RESOURCES

TRANSLATE/BROWSE | SEARCH | DOWNLOAD MIBS | MIB SUPPORT - SW

Translate | Browse The Object Tree

Translate OID into object name or object name into OID to receive object details

Enter OID or object name:  examples -  
OID: 1.3.6.1.4.1.9.9.27  
Object Name: ifIndex

Translate

Object Information

Specific Object Information

Object	cpmCPUTotalTable
OID	1.3.6.1.4.1.9.9.109.1.1.1
Type	SEQUENCE
Permission	not-accessible
Status	current
MIB	<a href="#">CISCO-PROCESS-MIB</a> ; - <a href="#">View Supporting Images</a>
Description	A table of overall CPU statistics.

從 FTD LINA CLI 使用命令 `show snmp-server oid` 以擷取可以輪詢的 LINA OID 完整清單。

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
firepower#
```

```
show snmp-server oid
```

```

-----
[0]      10.10.1.10.10.10.1.1.      sysDescr
[1]      10.10.1.10.10.10.1.2.      sysObjectID
[2]      10.10.1.10.10.10.1.3.      sysUpTime
[3]      10.10.1.1.10.1.1.4.         sysContact
[4]      10.10.1.1.10.1.1.5.         sysName
[5]      10.10.1.1.10.1.1.6.         sysLocation
[6]      10.10.1.1.10.1.1.7.         sysServices
[7]      10.10.1.1.10.1.1.8.         sysORLastChange
...
[1081]   10.3.1.1.10.0.10.1.10.1.9.  vacmAccessStatus
[1082]   10.3.1.1.10.0.10.1.10.1.    vacmViewSpinLock
[1083]   10.3.1.1.10.0.10.1.10.2.1.3. vacmViewTreeFamilyMask
[1084]   10.3.1.1.10.0.10.1.10.2.1.4. vacmViewTreeFamilyType
[1085]   10.3.1.1.10.0.10.1.10.2.1.5. vacmViewTreeFamilyStorageType
[1086]   10.3.1.1.10.0.10.1.10.2.1.6. vacmViewTreeFamilyStatus
-----
firepower#

```

 注意：命令是隱藏的。

## 疑難排解

以下是 Cisco TAC 發現最常見的 SNMP 案例產生因素：

1. 無法輪詢 FTD LINA SNMP
2. 無法輪詢 FXOS SNMP
3. 要使用什麼 SNMP OID 值？
4. 無法取得 SNMP 設陷
5. 無法透過 SNMP 監控 FMC
6. 無法設定 SNMP
7. Firepower Device Manager (FDM) 的 SNMP 組態

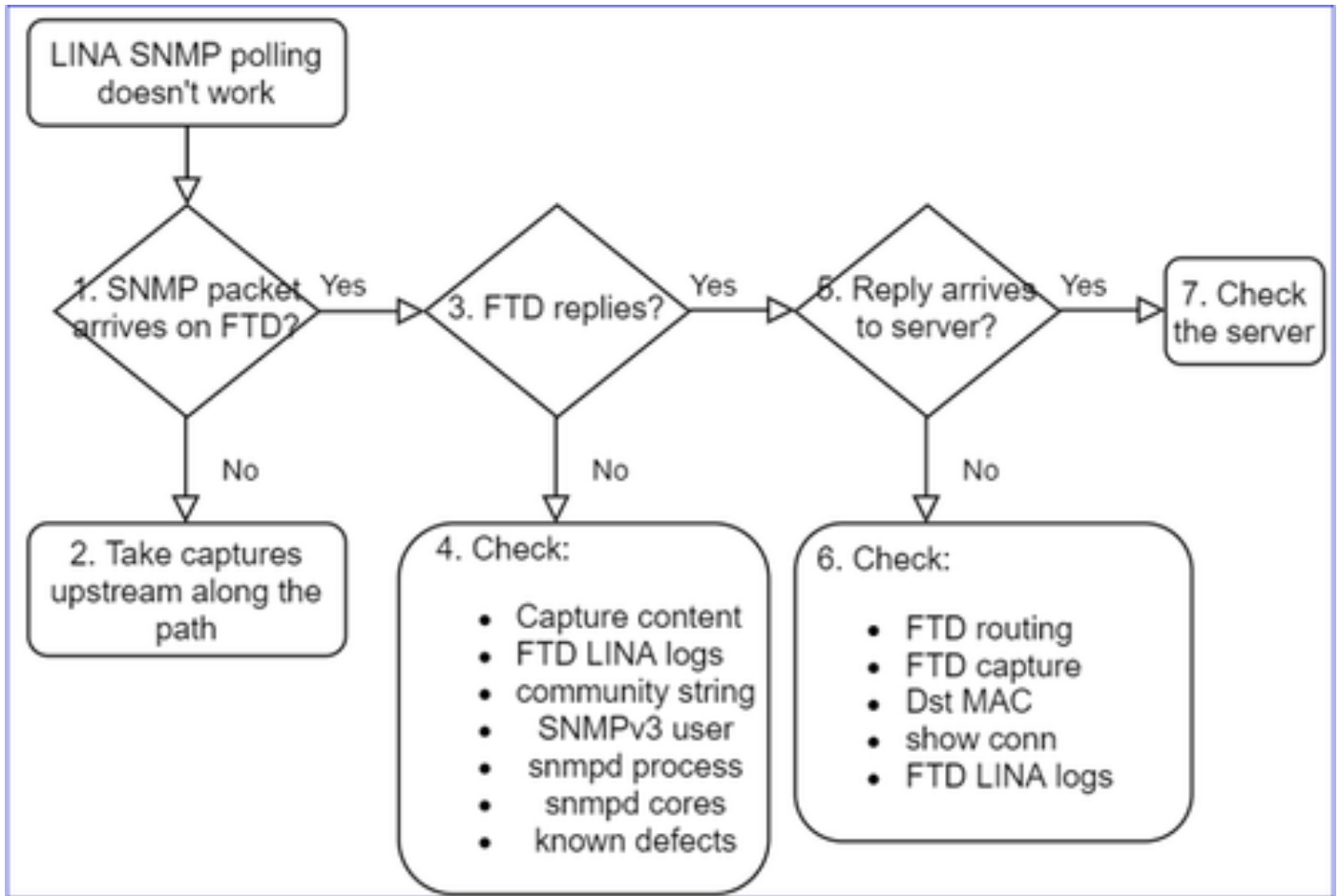
### 無法輪詢 FTD LINA SNMP

問題說明 ( 來自 Cisco TAC 真實案例的範例 )：

- 「無法透過 SNMP 擷取資料。」
- 「無法透過 SNMPv2 輪詢裝置。」
- 「SNMP 無法運作。我們想要使用 SNMP 監控防火牆，但設定完畢後，我們就遇到了問題。」
- 「我們有兩個監控系統無法透過 SNMP v2c 或 3 監控 FTD。」
- 「SNMP 測試無法在防火牆上運作。」

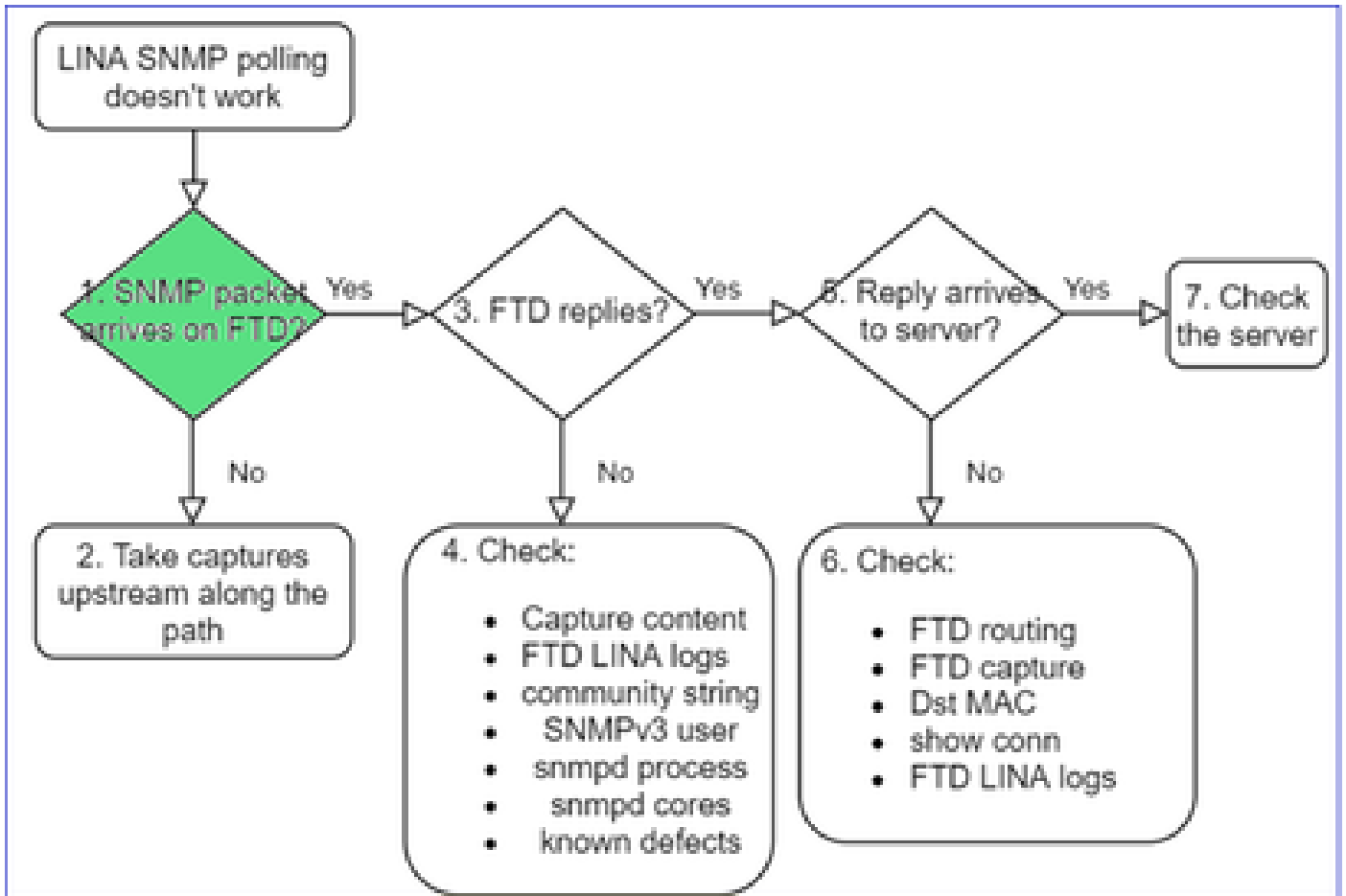
### 故障排除建議

建議使用以下程式來解決 LINA SNMP 輪詢問題的流程圖：



## 深入探討

### 1. SNMP封包是否到達FTD



- 啟用擷取以驗證 SNMP 封包是否到達。

FTD管理介面上的SNMP ( 6.6版後版本 ) 使用管理關鍵字 :

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

```
snmp-server host management 192.168.2.100 community ***** version 2c
```

FTD 資料介面的 SNMP 使用介面的名稱 :

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

```
snmp-server host net201 192.168.2.100 community ***** version 2c
```

FTD 管理介面的擷取：

```
<#root>
>
capture-traffic

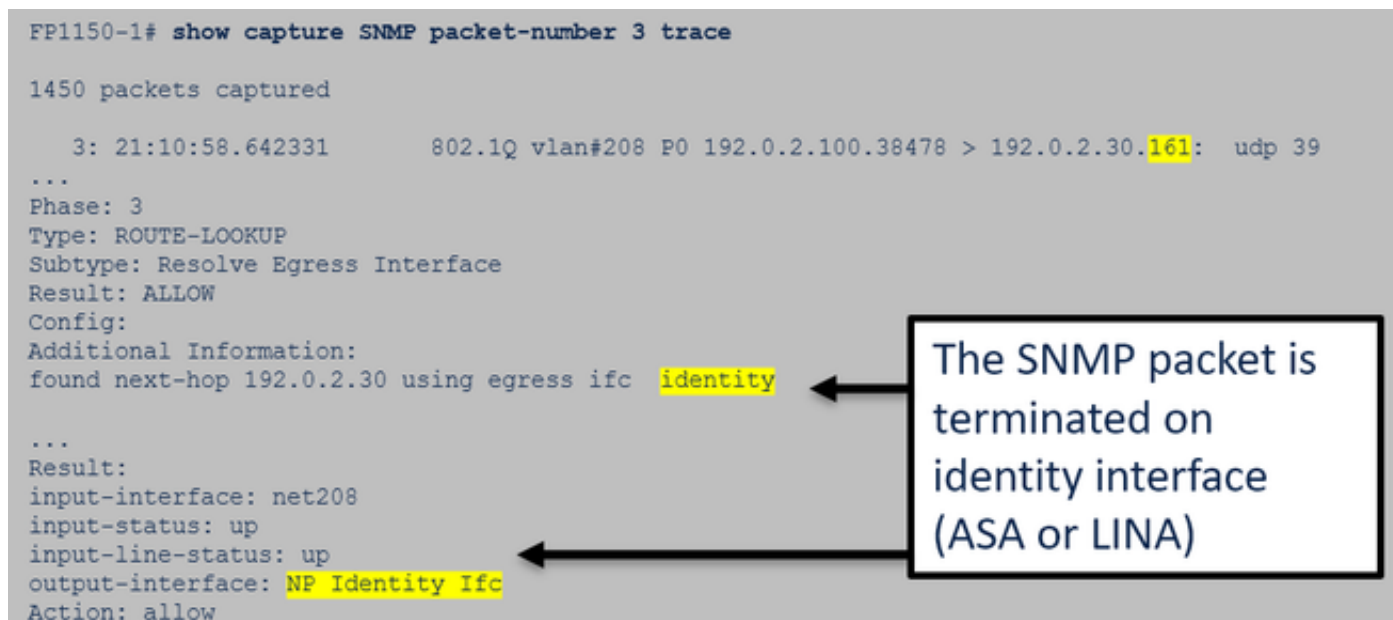
Please choose domain to capture traffic from:
 0 - management1
 1 - management0
 2 - Global
Selection?
1
```

FTD 資料介面的擷取：

```
<#root>
firepower#
capture SNMP interface net201 trace match udp any any eq 161
```

FTD資料介面封包追蹤 ( 6.6/9.14.1之前的版本 )：

```
FP1150-1# show capture SNMP packet-number 3 trace
1450 packets captured
 3: 21:10:58.642331      802.1Q vlan#208 P0 192.0.2.100.38478 > 192.0.2.30.161:  udp 39
...
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.0.2.30 using egress ifc identity
...
Result:
input-interface: net208
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
```



The SNMP packet is terminated on identity interface (ASA or LINA)

FTD資料介面封包追蹤 ( 6.6/9.14.1以後 )：



```

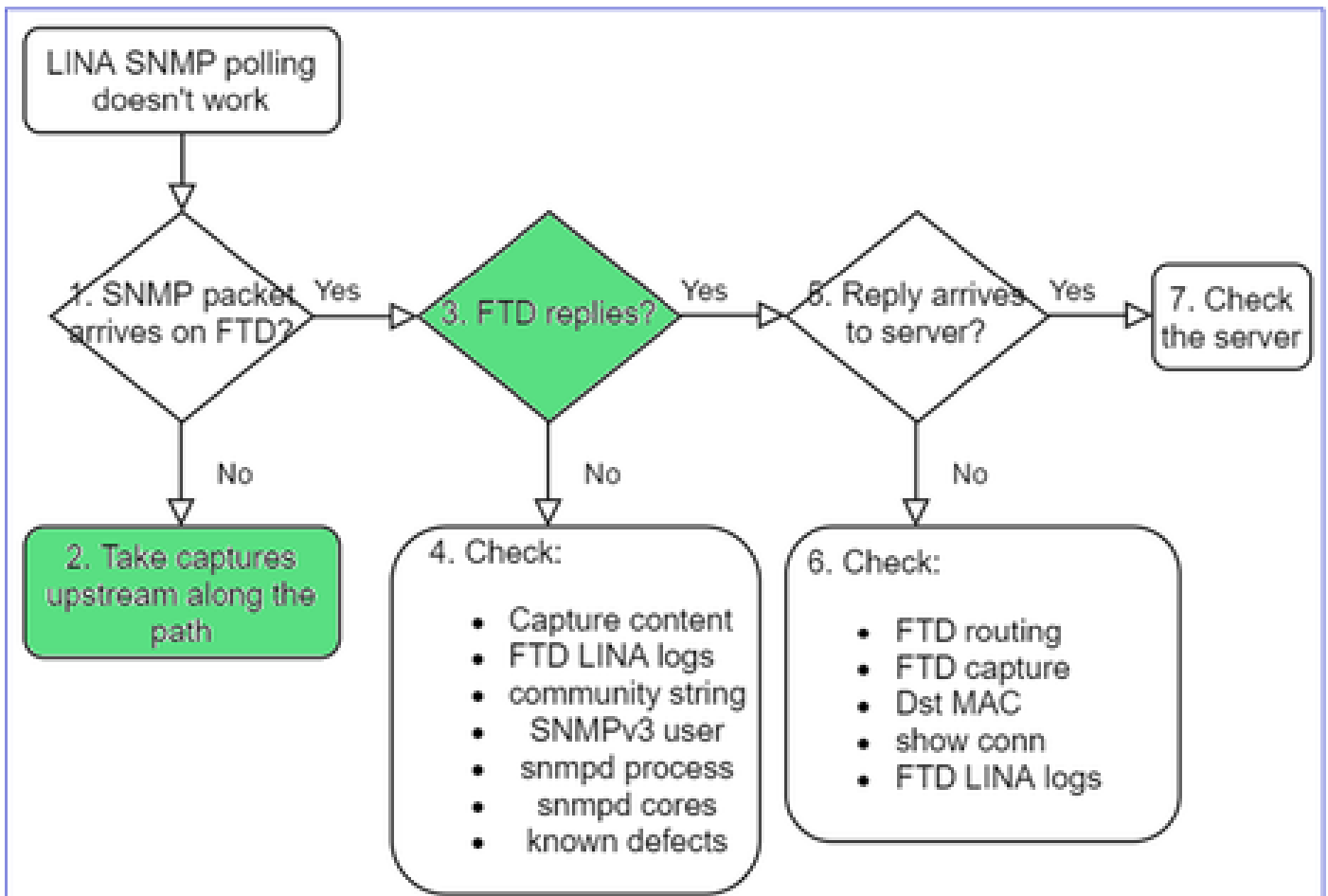
firepower# show capture SNMP packet-number 1 trace
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.21.100.58255 > 192.168.21.50.161:  udp 39
...
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 9
Config:
nat (nlp_int_tap,net201) source static nlp_server__snmp_192.168.21.100_intf4 interface destination static
0_192.168.21.100_4 0_192.168.21.100_4
Additional Information:
NAT divert to egress interface nlp_int_tap(vrfid:0)
Untranslate 192.168.21.50/161 to 169.254.1.2/161

```

NAT diverts the packet to Snort engine  
(NLP – Non-Lina Process tap interface)

2. 如果您在FTD輸入擷取中看不到SNMP封包：

- 沿著路徑往上游進行擷取.
- 確保 SNMP 伺服器使用正確的 FTD IP.
- 從因應 FTD 介面的交換器連接埠開始並往上游移動.



3. 是否看到FTD SNMP回覆？

若要驗證 FTD 是否回覆，請檢查：

1. FTD 輸出擷取 ( LINA 或管理介面 )

檢查是否有來源連接埠為 161 的 SNMP 封包：

```
<#root>
```

```
firepower#
```

```
show capture SNMP
```

```
75 packets captured
```

```
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161:  udp 39
2: 22:43:39.568329      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161:  udp 39
3: 22:43:39.569611      802.1Q vlan#201 P0 192.168.2.50.161 > 192.168.2.100.58255:  udp 119
```

在6.6/9.14.1之後的版本中，您還有另一個捕獲點：NLP分路器介面上的捕獲。NATed IP來自162.254.x.x範圍：

```
<#root>
```

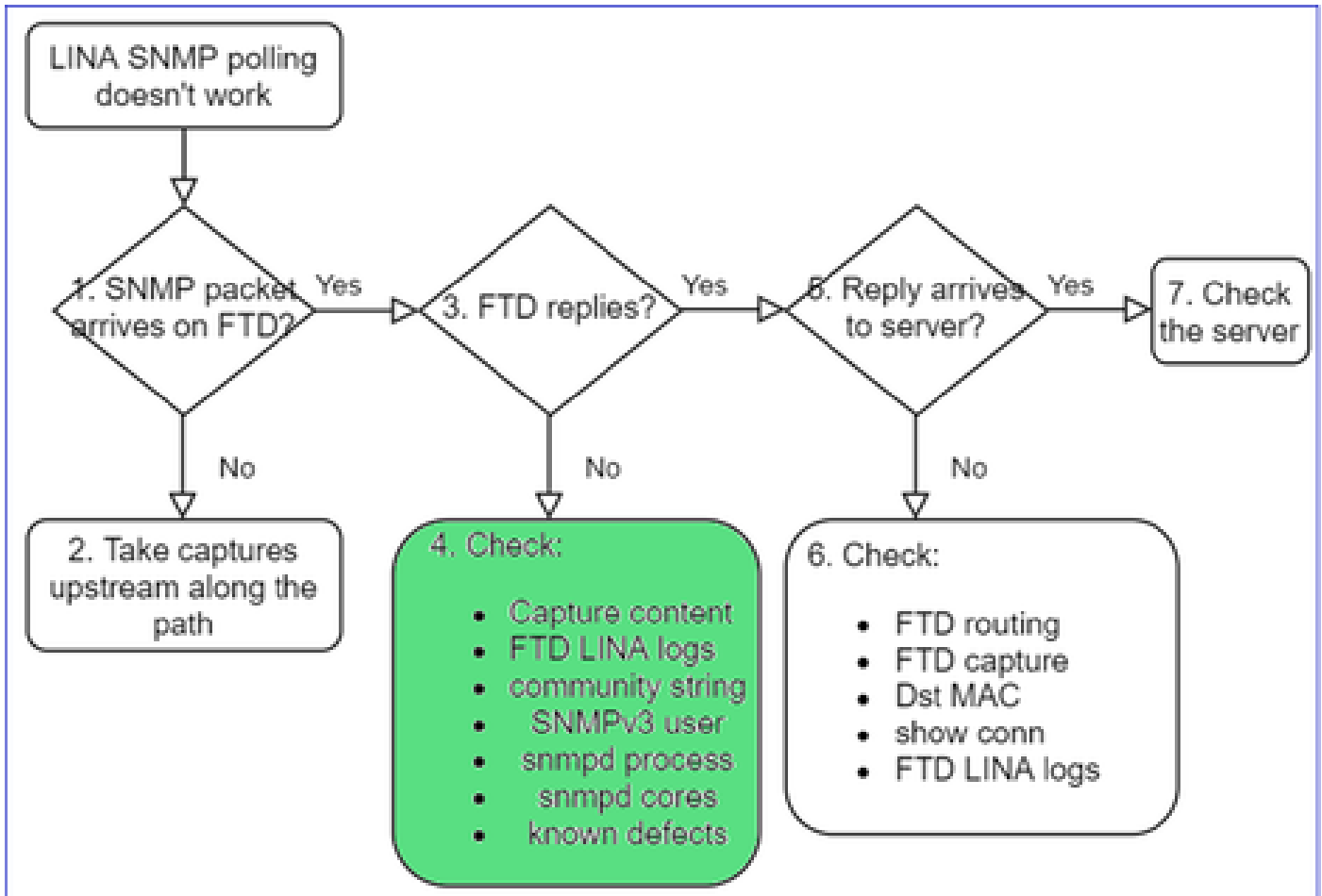
```
admin@firepower:~$
```

```
sudo tcpdump -i tap_nlp
```

```
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
16:46:28.372018 IP 192.168.2.100.49008 > 169.254.1.2.snmp: C="Cisc0123" GetNextRequest(28) E:cisco.9.
16:46:28.372498 IP 192.168.1.2.snmp > 192.168.2.100.49008: C="Cisc0123" GetResponse(35) E:cisco.9.109
```

#### 4. 額外支票



a.對於Firepower 4100/9300裝置，請檢查[FXOS相容性表](#)。

**Firepower 4100/9300 Compatibility with ASA and Threat Defense**

The following table lists compatibility between the ASA or threat defense applications with the Firepower 4100/9300. The FXOS versions with (EoL) appended have reached their end of life (EoL), or end of support.

- Note** The bold versions listed below are specially-qualified companion releases. You should use these software combinations whenever possible because Cisco performs enhanced testing for these combinations.
- Note** Firepower 1000/2100 appliances utilize FXOS only as an underlying operating system that is included in the ASA and threat defense unified image bundles.
- Note** FXOS 2.12/ASA 9.18/Threat Defense 7.2 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

Table 2. ASA or Threat Defense, and Firepower 4100/9300 Compatibility

FXOS Version	Model	ASA Version	Threat Defense Version		
<b>2.13(0.198)+</b> <b>Note</b> FXOS 2.13(0.198)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.3.0</b> (recommended) 7.2.0 7.1.0 7.0.0 6.7.0 6.6.x		
	Firepower 4145 Firepower 4125 Firepower 4115	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.3.0</b> (recommended) 7.2.0 7.1.0 7.0.0 6.7.0 6.6.x		
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)	7.0.0 6.7.0 6.5.0 6.4.0		
	<b>2.12(0.31)+</b> <b>Note</b> FXOS 2.12(0.31)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x	
		Firepower 4145 Firepower 4125 Firepower 4115	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x	
		Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.14(x) 9.13(1) 9.12(x)	6.6.x 6.5.0 6.4.0	
		Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x) 9.12(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x 6.5.0 6.4.0 6.3.0	
		Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.10(x) 9.9(x) 9.8(x)	6.4.0 6.3.0	
		<b>2.11(1.154)+</b> <b>Note</b> FXOS 2.11(1.154)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use	Firepower 4112	<b>9.17(x)</b> (recommended) 9.16(x) 9.15(1) 9.14(x)	<b>7.1.0</b> (recommended) 7.0.0 6.7.0 6.6.x

## b. 檢查FTD LINA snmp-server統計資料：

```
<#root>
firepower#
clear snmp-server statistics

firepower#
show snmp-server statistics

379 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  351 Number of requested variables    <- SNMP requests in
...
360 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  351 Response PDUs                    <- SNMP replies out
  9 Trap PDUs
```

## c. FTD LINA連線表

此檢查對FTD輸入介面上的擷取中看不到封包十分有用。請注意，此驗證僅對資料介面上的SNMP有效。如果SNMP在管理介面（6.6/9.14.1之後）上，則不會建立任何conn。

```
<#root>
firepower#
show conn all protocol udp port 161

13 in use, 16 most used
...
UDP nlp_int_tap 192.168.1.2:161 net201 192.168.2.100:55048, idle 0:00:21, bytes 70277, flags -c
```

## d. FTD LINA系統日誌

此驗證也僅適用於資料介面的SNMP！如果SNMP位於管理介面上，則不會建立記錄。

```
<#root>
firepower#
```

```
show log | i 302015.*161
```

```
Jul 13 2021 21:24:45: %FTD-6-302015: Built inbound UDP connection 5292 for net201:192.0.2.100/42909 (19
```

### e. 檢查FTD是否由於主機來源IP錯誤而捨棄SNMP封包

```
firepower# show capture SNMP packet-number 1 trace
1: 22:33:00.183248      802.1Q vlan#201 P0 192.168.21.100.43860 > 192.168.21.50.161: udp 39
Phase: 1
Type: CAPTURE
...
Phase: 6
Type: ACCESS-LIST
Result: DROP
...
Result:
input-interface: net201(vrfid:0)
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
flow (NA)/NA

firepower# show run snmp-server
snmp-server host net201 192.168.22.100 community **** version 2c

firepower# show asp table classify interface net201 domain permit match port=161
Input Table
in id=0x14f65b193b30, priority=501, domain=permit, deny=false
hits=8, user_data=0x0, cs_id=0x0, use_real_addr, flags=0x0, protocol=17
src ip/id=192.168.22.100, mask=255.255.255.255, port=0, tag=any
dst ip/id=192.168.21.50, mask=255.255.255.255, port=161, tag=any, dscp=0x0, nsg_id=none
input_ifc=net201(vrfid:0), output_ifc=any
```

### f. 不正確的憑證 ( SNMP社群 )

在擷取內容中，您可以看到社群值 ( SNMP v1 和 2c ) :

```
snmp
Delta      Source      Destination      Protocol      Length
0.000000  192.168.21.100  192.168.21.50    SNMP

> Frame 3: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: VMware_85:3e:d2 (00:50:56:85:3e:d2), Dst: a2:b8:dc:
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 201
> Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50
> User Datagram Protocol, Src Port: 45230, Dst Port: 161
Simple Network Management Protocol
  version: v2c (1)
  community: cisco123
  data: get-next-request (1)
```

### g. 配置不正確 ( 例如，SNMP版本或社群字串 )

有幾種方法可以驗證裝置 SNMP 組態和社群字串 :

```
<#root>
```

```
firepower#
```

```
more system:running-config | i community
```

```
snmp-server host net201 192.168.2.100 community CISC0123 version 2c
```

其他方法：

```
<#root>
firepower#
debug menu netsnmp 4
```

#### h. FTD LINA/ASA ASP捨棄

若要驗證 FTD 是否捨棄 SNMP 封包，這是相當實用的檢查。首先，請清除計數器（清除 asp 捨棄），然後測試：

```
<#root>
firepower#
clear asp drop

firepower#
show asp drop
```

```
Frame drop:
  No valid adjacency (no-adjacency)                6
  No route to host (no-route)                       204
  Flow is denied by configured rule (acl-drop)      502
  FP L2 rule drop (l2_acl)                          1
```

```
Last clearing: 19:25:03 UTC Aug 6 2021 by enable_15
```

```
Flow drop:
Last clearing: 19:25:03 UTC Aug 6 2021 by enable_15
```

#### i. ASP捕獲

ASP 擷取可讓您檢視捨棄的封包（例如：ACL 或相鄰）：

```
<#root>
firepower#
capture ASP type asp-drop all
```

測試並檢查擷取內容：

```
<#root>
```

```
firepower#  
show capture  
  
capture ASP type asp-drop all [Capturing - 196278 bytes]
```

## j. SNMP核心 ( 回溯 ) - 驗證方式1

當您懷疑發生系統穩定性問題時，此檢查相當實用：

```
<#root>  
firepower#  
show disk0: | i core  
  
13 52286547 Jun 11 2021 12:25:16 coredumpfsys/core.snmpd.6208.1626214134.gz
```

## SNMP 核心 ( 回溯 ) - 驗證方法 2

```
<#root>  
admin@firepower:~$  
ls -l /var/data/cores  
  
-rw-r--r-- 1 root root 685287 Jul 14 00:08 core.snmpd.6208.1626214134.gz
```

如果您看到 SNMP 核心檔案，請收集下列項目並聯絡 Cisco TAC：

- FTD TS 檔案 ( 或 ASA show tech )
- snmpd 核心檔案

SNMP 偵錯 ( 這些為隱藏命令，且僅適用於較新的版本 )：

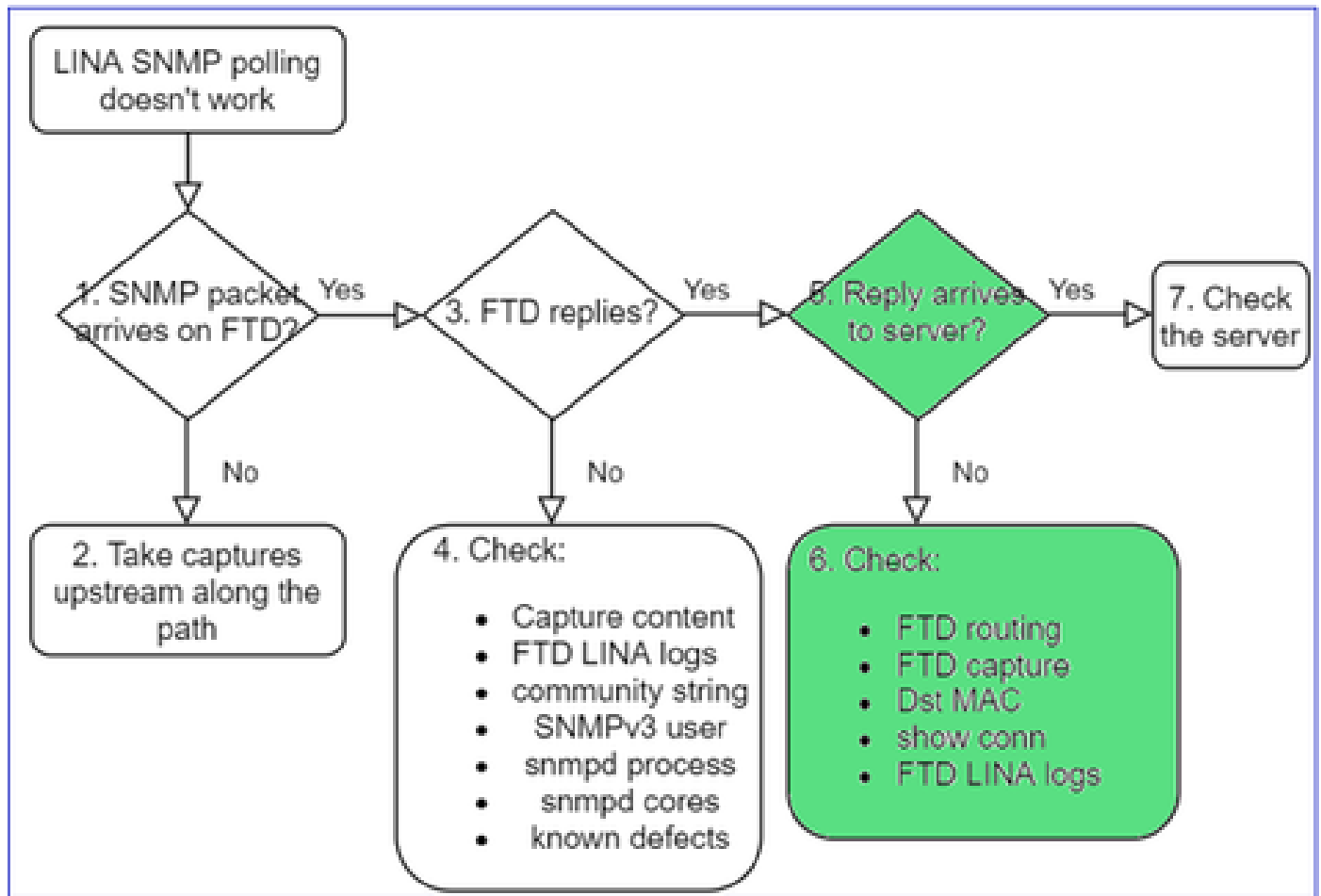
```
<#root>  
firepower#  
debug snmp trace [255]  
  
firepower#  
debug snmp verbose [255]  
  
firepower#
```

```
debug snmp error [255]
```

```
firepower#
```

```
debug snmp packet [255]
```

防火牆 SNMP 回覆是否送達伺服器？



如果 FTD 已回覆，但該回覆未送達伺服器，請檢查：

a.FTD製程

適用於 FTD 管理介面路由：

```
<#root>
```

```
>
```

```
show network
```

適用於 FTD LINA 資料介面路由：

```
<#root>
```



```
firepower#
```

```
show route
```

## b. 目的MAC驗證

FTD 管理目的地 MAC 驗證：

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management1
```

```
1 - management0
```

```
2 - Global
```

```
Selection?
```

```
1
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options:
```

```
-n -e udp port 161
```

```
01:00:59.553385 a2:b8:dc:00:00:02 > 5c:fc:66:36:50:ce, ethertype IPv4 (0x0800), length 161: 10.62.148.1
```

FTD LINA 資料介面目的地 MAC 驗證：

```
<#root>
```

```
firepower#
```

```
show capture SNMP detail
```

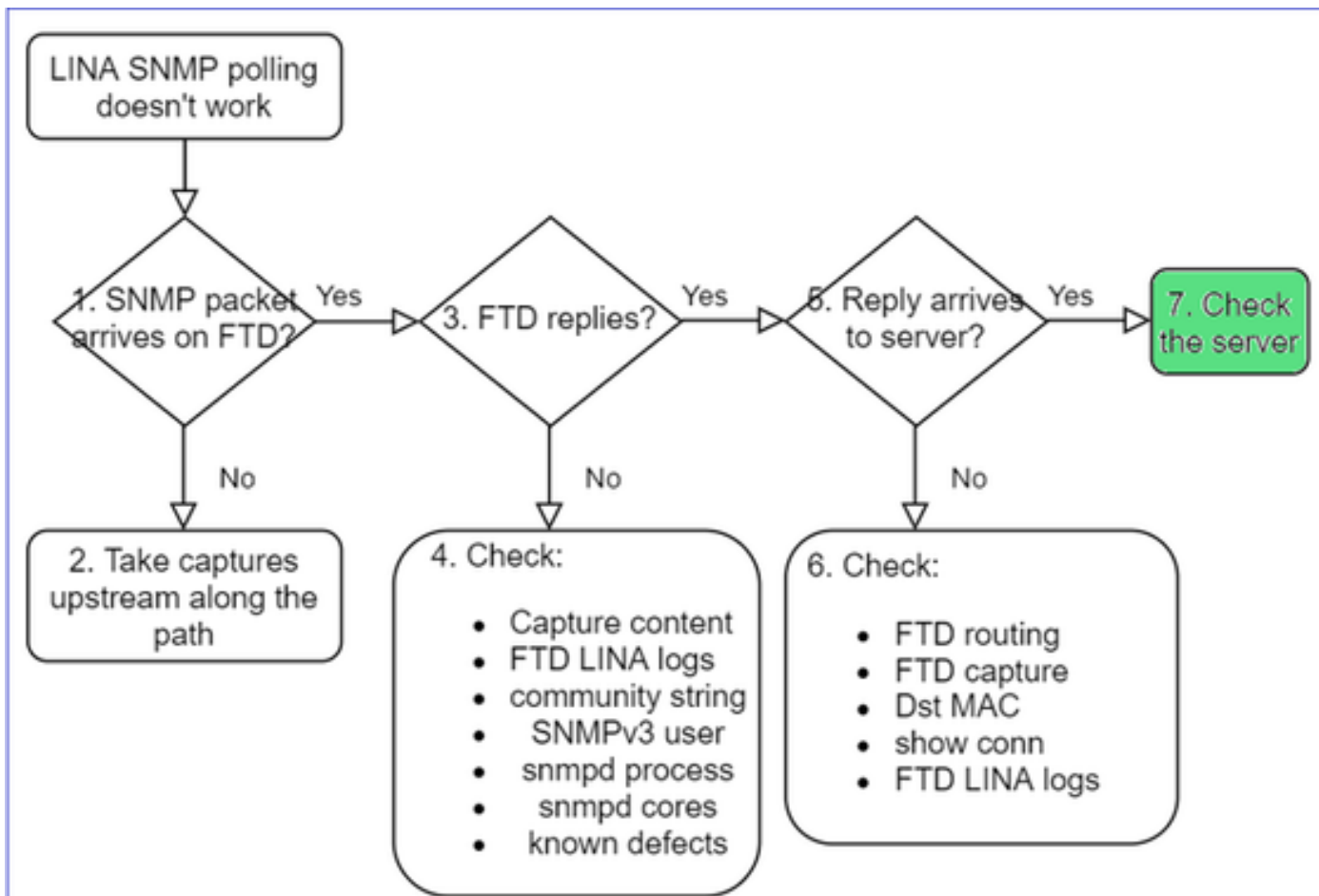
```
...
```

```
6: 01:03:01.391886 a2b8.dc00.0003 0050.5685.3ed2 0x8100 Length: 165
```

```
802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.40687: [udp sum ok] udp 119 (DF) (ttl 64,
```

c. 沿著路徑檢查可能捨棄/封鎖 SNMP 封包的裝置。

檢查 SNMP 伺服器



a. 檢查捕獲內容以驗證設定。

b. 檢查伺服器配置。

c. 嘗試修改SNMP社群名稱（例如，沒有特殊字元）。

只要符合2個條件，您就可以使用終端主機甚至FMC來測試輪詢：

1. SNMP 連線已就緒。
2. 來源 IP 可以輪詢裝置。

<#root>

```
admin@FS2600-2:~$
```

```
snmpwalk -c cisco -v2c 192.0.2.197
```

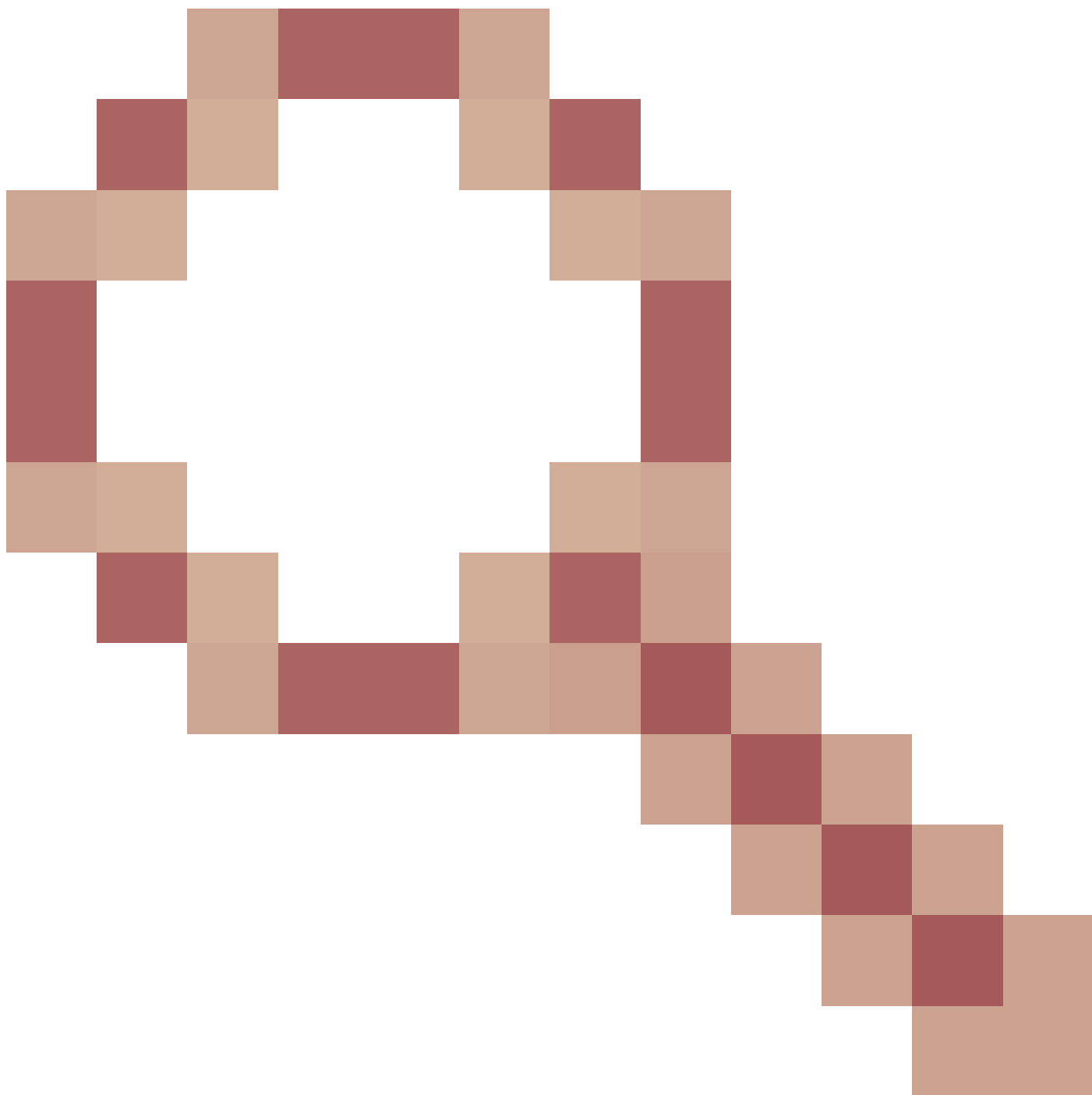
```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9.
```

### SNMPv3輪詢注意事項

- 許可證：SNMPv3需要強加密許可證。請確認您已在智慧型授權入口網站上啟用匯出控制功能
- 若要疑難排解，您可以嘗試使用新的使用者/認證
- 如果使用加密，則可以解密SNMPv3流量並檢查負載，如中所述

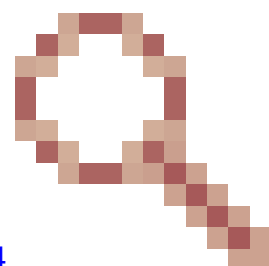
: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>


- 請考慮使用 AES128 進行加密，以免軟體受到下列瑕疵的影響：
- 思科漏洞ID [CSCvy27283](#)



使用隱私演算法AES192/AES256時，ASA/FTD SNMPv3輪詢可能會失敗

對具有身份驗證sha和優先順序aes 192的使用者而言，思科漏洞ID [CSCvx45604](#)  
Snmpv3 walk失敗



 注意：如果SNMPv3由於演算法不匹配而失敗，則show輸出和日誌不會顯示任何明顯內容

```
firepower# show snmp-server statistics
6 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 1500)
 0 No such name errors
 0 Bad values errors
 0 General errors
 0 Response PDUs
 0 Trap PDUs
```

Input packets increase, but no replies!

First recommended action:  
Verify your configuration 'show run snmp-server'

## SNMPv3 輪詢考量事項 – 案例研究

### 1. SNMPv3 snmpwalk – 作用中情況

<#root>

admin@FS2600-2:~\$

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x AES -X Cisco123 192.168.21.50
```

SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9  
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2315

在擷取 (snmpwalk) 中，您可以看到每個封包的回覆：

```
firepower# show capture SNMP
...
14: 23:44:44.156714      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 64
15: 23:44:44.157325      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 132
16: 23:44:44.160819      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 157
17: 23:44:44.162039      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 238
18: 23:44:44.162375      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
19: 23:44:44.197850      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 168
20: 23:44:44.198262      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
21: 23:44:44.237826      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 162
22: 23:44:44.238268      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
23: 23:44:44.277909      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 159
24: 23:44:44.278260      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
25: 23:44:44.317869      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 168
```

擷取檔案未顯示任何異常狀況：

```

Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  <v> msgAuthoritativeEngineID: 80000009feca41e36a96147f184553b777
    1... .. = Engine ID Conformance: RFC3411 (SNMPv3)
    Engine Enterprise ID: ciscoSystems (9)
    Engine ID Format: Reserved/Enterprise-specific (254)
    Engine ID Data: ca41e36a96147f184553b777a7127ccb3710888f
  msgAuthoritativeEngineBoots: 6
  msgAuthoritativeEngineTime: 5089
  msgUserName: Cisco123
  <v> msgAuthenticationParameters: 79ee0d463313558f4529954f
    <v> [Authentication: OK]
      <v> [Expert Info (Chat/Checksum): SNMP Authentication OK]
        [SNMP Authentication OK]
        [Severity level: Chat]
        [Group: Checksum]
      msgPrivacyParameters: 714e78d6bc292c88

```

## 2. SNMPv3 snmpwalk – 加密失敗

提示#1：存在超時：

```
<#root>
```

```
admin@FS2600-2:~$
```

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x DES -X Cisco123 192.168.21.50
```

```
Timeout: No Response from 192.168.2.1
```

提示#2：請求很多，1個回覆：

```

firepower# show capture SNMP
7 packets captured
  1: 23:25:06.248446      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161:  udp 64
  2: 23:25:06.248613      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161:  udp 64
  3: 23:25:06.249224      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.55137:  udp 132
  4: 23:25:06.252992      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161:  udp 163
  5: 23:25:07.254183      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161:  udp 163
  6: 23:25:08.255388      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161:  udp 163
  7: 23:25:09.256624      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161:  udp 163

```

提示#3：Wireshark解密失敗：

```
> User Datagram Protocol, Src Port: 35446, Dst Port: 161
  Simple Network Management Protocol
    msgVersion: snmpv3 (3)
    > msgGlobalData
    > msgAuthoritativeEngineID: 80000009feca41e36a96147f184553b777a7127ccb3710888f
    msgAuthoritativeEngineBoots: 6
    msgAuthoritativeEngineTime: 4359
    msgUserName: Cisco123
    > msgAuthenticationParameters: 1bc9daaa366647cbbb70c5d5
    msgPrivacyParameters: 0000000197eaef1a
  > msgData: encryptedPDU (1)
    > encryptedPDU: 452ee7ef0b13594f8b0f6031213217477ecb2422d353581311cade539a27951af821524c...
      > Decrypted data not formatted as expected, wrong key?
        > [Expert Info (Warning/Malformed): Decrypted data not formatted as expected, wrong key?]
          [Decrypted data not formatted as expected, wrong key?]
          [Severity level: Warning]
          [Group: Malformed]
```

提示#4。檢查ma\_ctx2000.log檔案中是否存在「剖析ScopedPDU時出錯」消息：

```
<#root>
```

```
> expert
admin@firepower:~$
```

```
tail -f /mnt/disk0/log/ma_ctx2000.log
```

```
security service 3 error parsing ScopedPDU
security service 3 error parsing ScopedPDU
security service 3 error parsing ScopedPDU
```

分析ScopedPDU時出錯，強烈提示存在加密錯誤。ma\_ctx2000.log檔案僅顯示SNMPv3的事件！

### 3. SNMPv3 snmpwalk – 驗證失敗

提示#1：身份驗證失敗

```
<#root>
```

```
admin@FS2600-2:~$
```

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a MD5 -A Cisco123 -x AES -X Cisco123 192.168.21.50
```

```
snmpwalk: Authentication failure (incorrect password, community or key)
```

提示#2：有許多請求和許多回覆

```
firepower# show capture SNMP
4 packets captured
1: 23:25:28.468847      802.1Q vlan#201 PO 192.168.21.100.34348 > 192.168.21.50.161: udp 64
2: 23:25:28.469412      802.1Q vlan#201 PO 192.168.21.50.161 > 192.168.21.100.34348: udp 132
3: 23:25:28.474386      802.1Q vlan#201 PO 192.168.21.100.34348 > 192.168.21.50.161: udp 157
4: 23:25:28.475561      802.1Q vlan#201 PO 192.168.21.50.161 > 192.168.21.100.34348: udp 137
```

提示#3：Wireshark格式錯誤的資料包

```
> Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50
> User Datagram Protocol, Src Port: 47752, Dst Port: 161
> Simple Network Management Protocol
✖ [Malformed Packet: SNMP]
  ✖ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

提示#4。檢查ma\_ctx2000.log檔案是否存在「身份驗證失敗」消息：

```
<#root>
```

```
>
```

```
expert
```

```
admin@firepower:~$
```

```
tail -f /mnt/disk0/log/ma_ctx2000.log
```

```
Authentication failed for Cisco123
Authentication failed for Cisco123
```

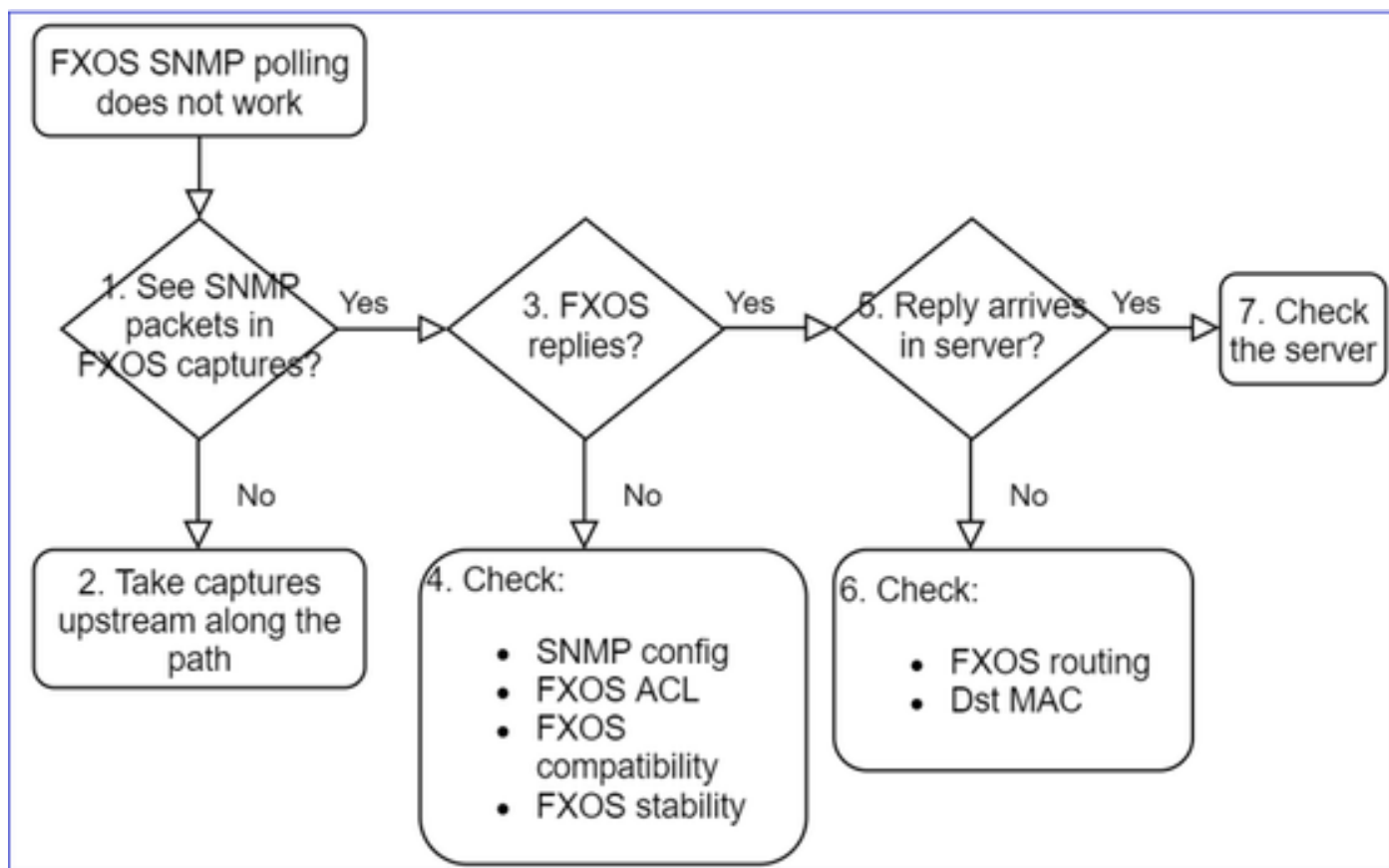
## 無法輪詢 FXOS SNMP

問題說明 ( 來自 Cisco TAC 真實案例的範例 )：

- 「SNMP 提供的 FXOS 版本錯誤。當透過 SNMP 針對 FXOS 版本進行輪詢時，輸出內容難以理解。」
- 「無法設定 FXOS FTD4115 的 snmp 社群。」
- 「在待命防火牆上將 FXOS 從 2.8 升級至 2.9 後，當嘗試透過 SNMP 接收任何資訊時，我們遇到了逾時狀況。」
- 「snmpwalk 在 FXOS 9300 設備上失敗，但適用於使用相同版本的 FXOS 4140 設備。問題並非出在連線能力和社群。」
- 「我們想要在 FPR4K FXOS 上新增 25 個 SNMP 伺服器，但無法這麼做。」

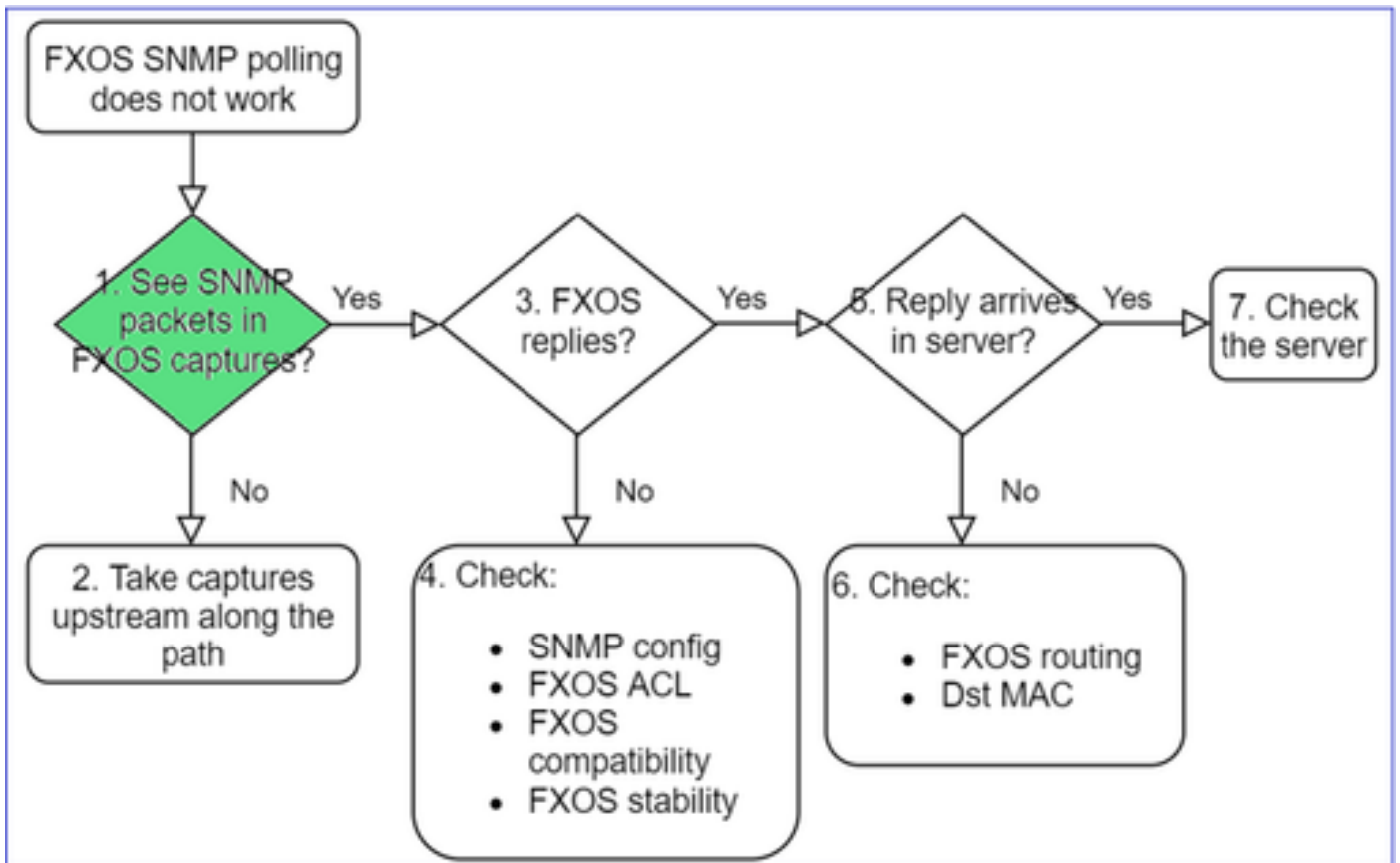
## 建議的疑難排解

以下是對FXOS SNMP輪詢問題進行故障排除的流程圖：



1. 是否在FXOS捕獲中看到SNMP資料包？





#### FPR1xxx/21xx

- FPR1xxx/21xx上沒有機箱管理器（裝置模式）。
- 您可以從管理介面輪詢 FXOS 軟體。

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management0
```

```
1 - Global
```

```
Selection?
```

```
0
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options:
```

```
-n host 192.0.2.100 and udp port 161
```

#### 41xx/9300

- 在 Firepower 41xx/93xx 上，使用 Ethalyzer CLI 工具進行機箱擷取：

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
firepower(fxos)#
```

```
ethalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace
```

```
firepower(fxos)#
```

```
exit
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

```
dir
```

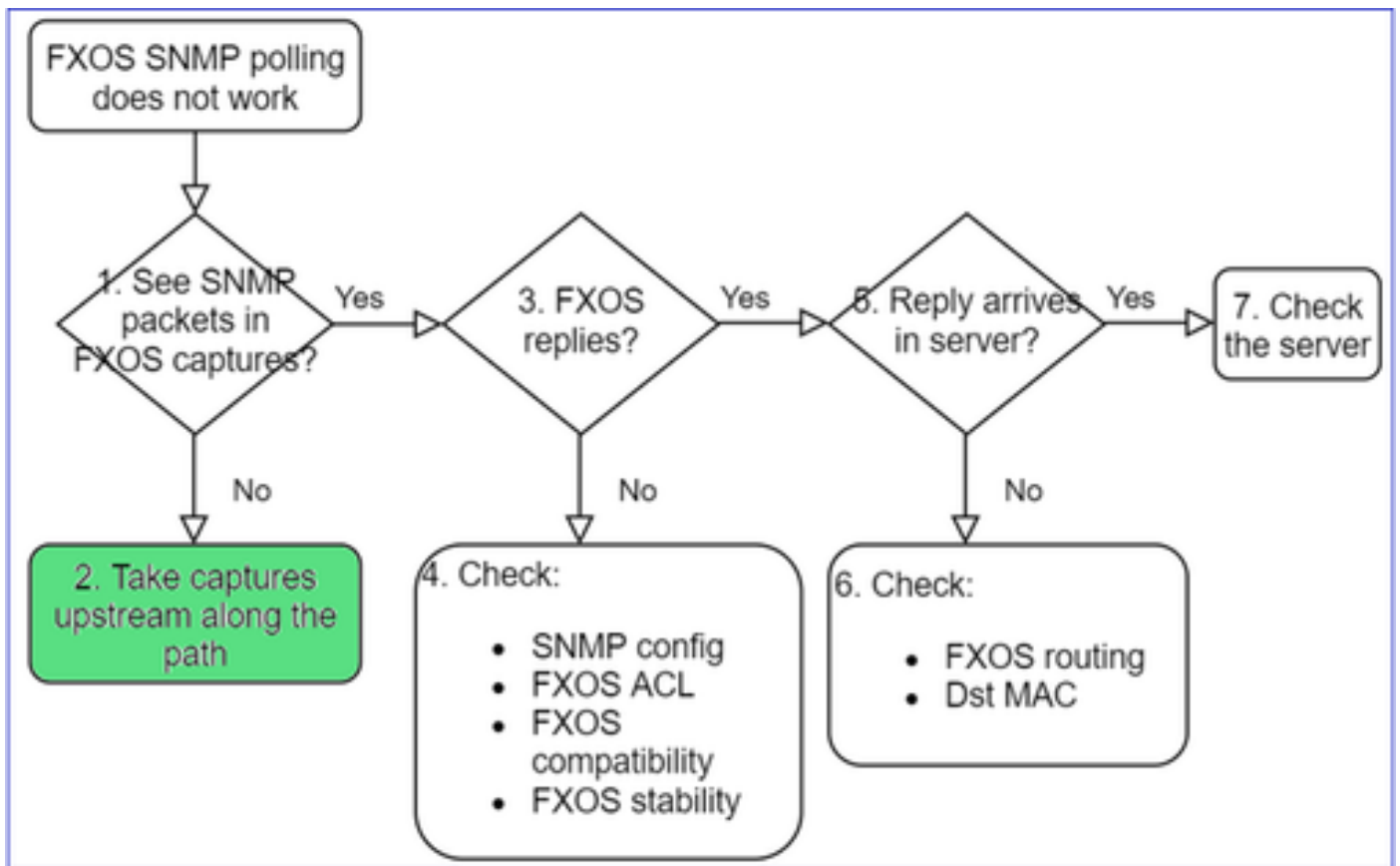
```
1
```

```
11152 Jul 26 09:42:12 2021 SNMP.pcap
```

```
firepower(local-mgmt)#
```

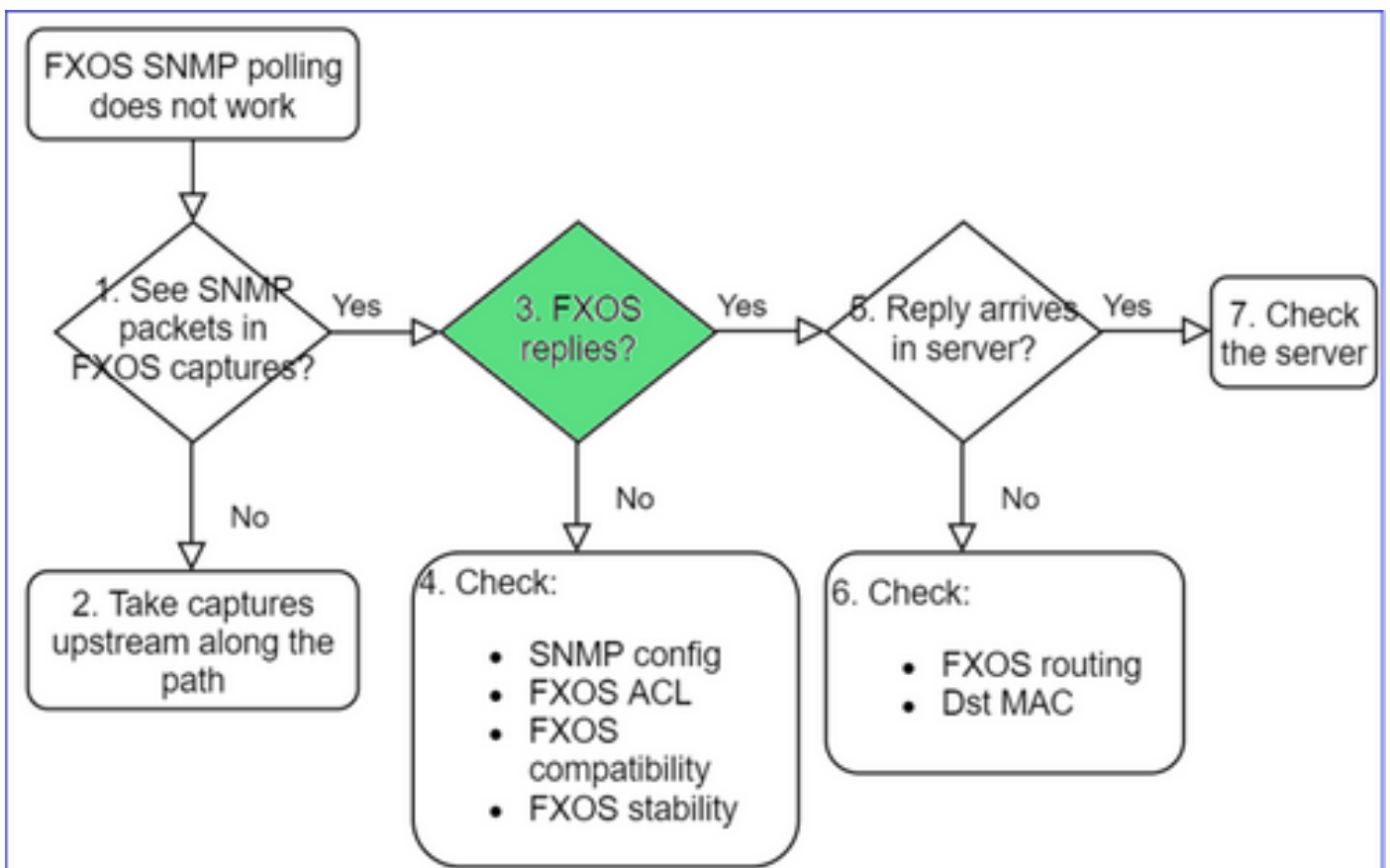
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

## 2. FXOS捕獲中沒有資料包？



- 沿著路徑往上游進行擷取

### 3. FXOS回覆？



- 作用中情況：

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS\_PACKET\_BUFFER\_SIZE is set to 4.

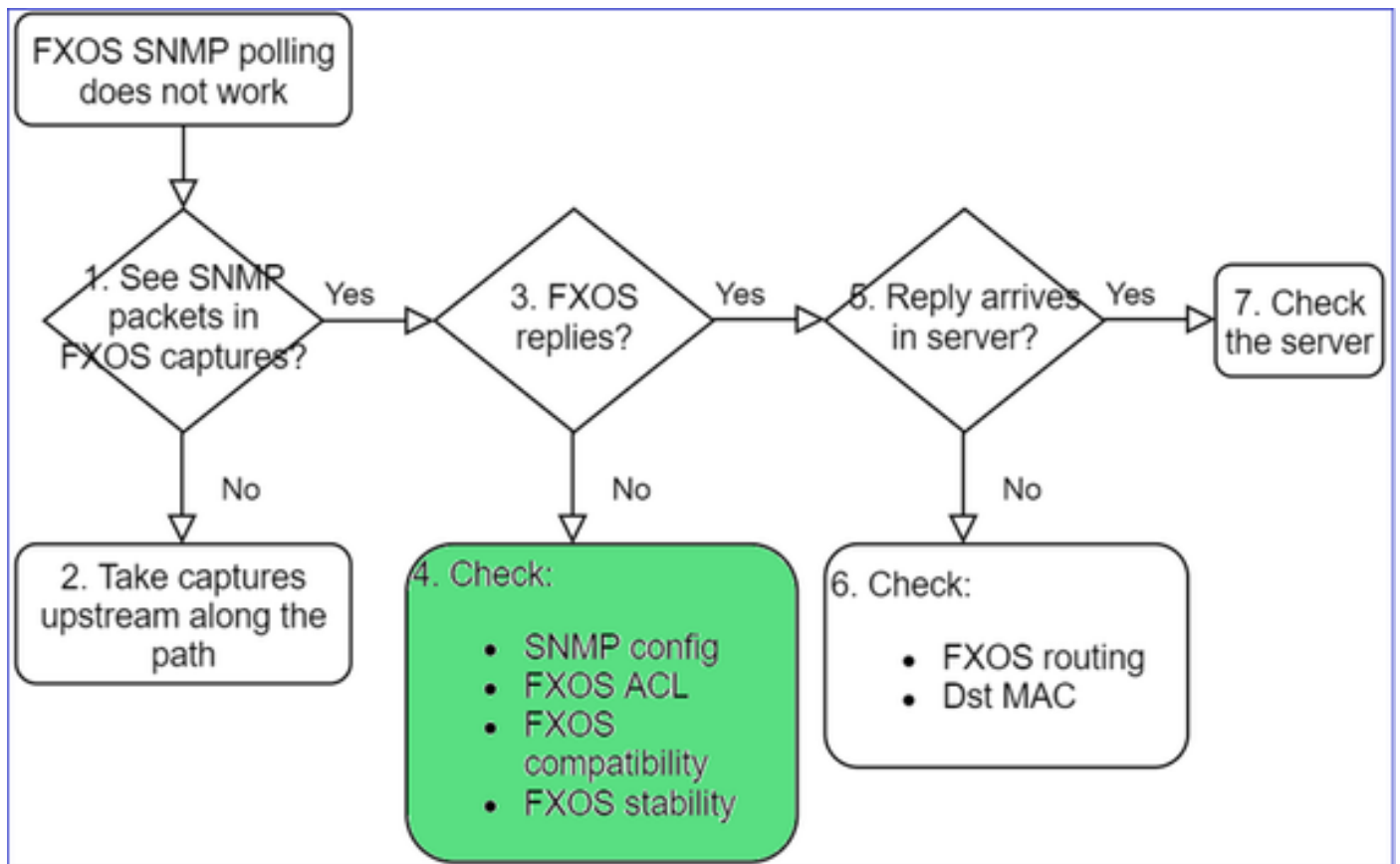
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

Listening on management0, link-type EN10MB (Ethernet), capture size 262144 bytes

08:17:25.952457 IP 192.168.2.23.36501 > 192.168.2.28.161: C="Cisco123" GetNextRequest(25) .10.3.1.1.2

08:17:25.952651 IP 192.168.2.28.161 > 192.168.2.23.36501: C="Cisco123" GetResponse(97) .1.10.1.1.1.1.

#### 4. FXOS 未回覆



#### 其他檢查

- 驗證 SNMP 組態 ( 透過 UI 或 CLI )：

<#root>

```
firepower#
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

- 請留意特殊字元 ( 例如 : 「\$」 ) :

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

```
FP4145-1(fxos)#
```

```
show running-config snmp all
```

```
FP4145-1(fxos)#
```

```
show snmp community
```

Community	Group / Access	context	acl_filter
-----	-----	-----	-----
Cisco123	network-operator		

- 若為 SNMP v3 , 請使用 show snmp-user [detail]
- 驗證 FXOS 相容性

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id\\_59069](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id_59069)

#### 4. 若FXOS未回覆

驗證 FXOS SNMP 計數器 :

```

FP4145-1# connect fxos
FP4145-1 (fxos)# show snmp
...
2243 SNMP packets input
  0 Bad SNMP versions
  28 Unknown community name
  0 Illegal operation for community name
supplied
  28 Encoding errors
  2214 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  2214 Get-next PDUs
  0 Set-request PDUs
3483 SNMP packets output
  0 Too big errors
  1296 Out Traps PDU

```

- 驗證 FXOS 存取控制清單 (ACL)。這僅適用於 FPR41xx/9300 平台。

如果流量被FXOS ACL阻塞，您會看到請求，但不會看到任何回覆：

<#root>

firepower(fxos)#

ethalyzer local interface mgmt capture-filter

"udp port 161" limit-captured-frames 50 write workspace:///SNMP.pcap

Capturing on 'eth0'

```

1 2021-07-26 11:56:53.376536964 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1
2 2021-07-26 11:56:54.377572596 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.10.1.10.1.1
3 2021-07-26 11:56:55.378602241 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1

```

您可以從使用者介面 (UI) 驗證 FXOS ACL：

您也可以從 CLI 驗證 FXOS ACL：

```
<#root>
```

```
firepower#
```

```
scope system
```

```
firepower /system #
```

```
scope services
```

```
firepower /system/services #
```

```
show ip-block detail
```

```
Permitted IP Block:
```

```
IP Address: 0.0.0.0
```

```
Prefix Length: 0
```

```
Protocol: snmp
```

- 偵錯 SNMP ( 僅限封包 ) 。 僅適用於 FPR41xx/9300 :

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

```
FP4145-1(fxos)#
```

```
terminal monitor
```

```
FP4145-1(fxos)#
```

```
debug snmp pkt-dump
```

```
2021 Aug 4 09:51:24.963619 snmpd: SNMPPKTSTRT: 1.000000 161 495192988.000000 0.000000 0.000000 0.000000
```

- Debug SNMP (all) -此調試輸出非常詳細。

```
<#root>
```

```
FP4145-1(fxos)#
```

```
debug snmp all
```

```
2021 Aug 4 09:52:19.909032 snmpd: SDWRAP message Successfully processed
```

```
2021 Aug 4 09:52:21.741747 snmpd: Sending it to SDB-Dispatch
```

```
2021 Aug 4 09:52:21.741756 snmpd: Sdb-dispatch did not process
```

- 驗證是否有任何與 SNMP 相關的 FXOS 故障：

```
<#root>
```

```
FXOS#
```

```
show fault
```

```
Severity Code Last Transition Time ID Description
```

```
-----  
Warning F78672 2020-04-01T21:48:55.182 1451792 [FSM:STAGE:REMOTE-ERROR]: Result: resource-unavailable C
```

- 驗證是否有任何 snmpd 核心：

在 FPR41xx/FPR9300 上：

```
<#root>
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

```
dir cores
```

```
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz
```

```
1 1984340 Apr 01 16:53:09 2021 core.snmpd.10018.1585759989.gz
```

在 FPR1xxx/21xx 上：

```
<#root>
```

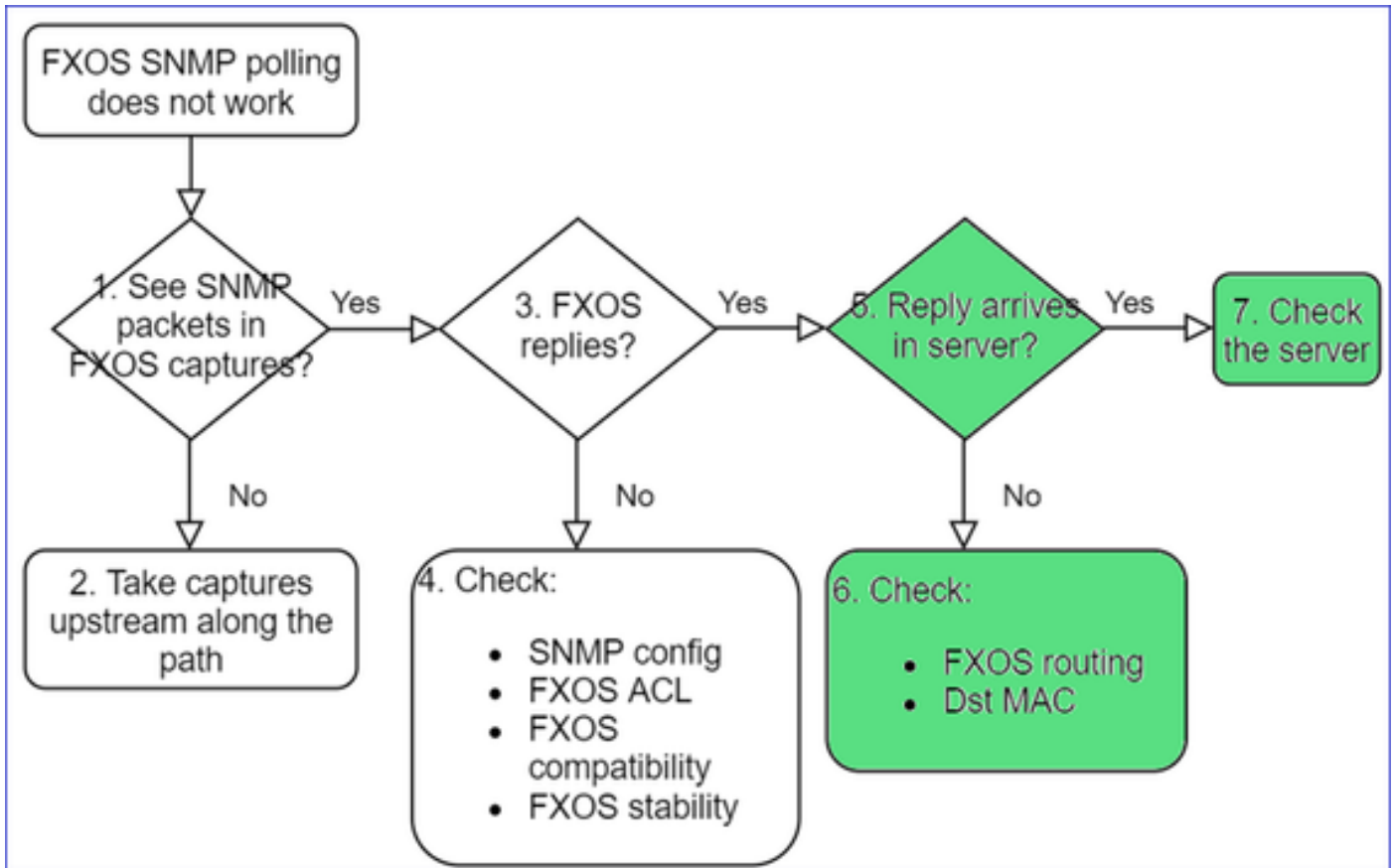
```
firepower(local-mgmt)#
```

```
dir cores_fxos
```

如果您看到任何 snmpd 核心，請收集這些核心以及 FXOS 疑難排解套件，然後聯絡 Cisco TAC。

5. SNMP回覆是否到達SNMP伺服器？





- 檢查 FXOS 路由

此輸出來自 FPR41xx/9300 :

```
<#root>
```

```
firepower#
```

```
show fabric-interconnect
```

```
Fabric Interconnect:
```

ID	OOB IP Addr	OOB Gateway	OOB Netmask	OOB IPv6 Address	OOB IPv6 Gateway	Prefix	Operational
A	192.168.2.37	192.168.2.1	10.255.255.128 ::	::		64	Operable

- 進行擷取並匯出 pcap，然後檢查回覆的目的地 MAC
- 最後，檢查 SNMP 伺服器 ( 擷取、組態、應用程式等 )

要使用什麼 SNMP OID 值 ?

問題說明 ( 來自 Cisco TAC 真實案例的範例 ) :

- 「我們想要監控 Cisco Firepower 設備。請為每個核心 CPU、記憶體、磁碟提供 SNMP OID。」
- 「是否有任何 OID 可以用來監控 ASA 5555 裝置的電源供應器狀態？」

- 「我們想要擷取 FPR 2K 和 FPR 4K 的機箱 SNMP OID。」
- 「我們想要輪詢 ASA ARP 快取。」
- 「我們需要知道 BGP 對等關閉的 SNMP OID。」

如何找到 SNMP OID 值

這些文件提供有關 Firepower 裝置上 SNMP OID 的資訊：

- Cisco Firepower Threat Defense (FTD) SNMP 監控白皮書：

<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/white-paper-c11-741739.html>

- Cisco Firepower 4100/9300 FXOS MIB 參考指南：

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b\\_FXOS\\_4100\\_9300\\_MIBRef.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b_FXOS_4100_9300_MIBRef.html)

- 如何搜尋 FXOS 平台的特定 OID：

<https://www.cisco.com/c/en/us/support/docs/security/firepower-9000-series/214337-how-to-look-for-an-specific-oid-on-fxos.html>

- 從 CLI (ASA/LINA) 檢查 SNMP OID

```
<#root>
```

```
firepower#
```

```
show snmp-server ?
```

```
engineID    Show snmp engineID
group        Show snmp groups
host         Show snmp host's
statistics  Show snmp-server statistics
user         Show snmp users
```

```
firepower#
```

```
show snmp-server oid
```

```
<- hidden option!
[1] .1.10.1.1.10.1.2.1  IF-MIB::ifNumber
[2] .1.10.1.1.1.10.2.2.1.1  IF-MIB::ifIndex
[3] .1.10.1.1.1.10.2.2.1.2  IF-MIB::ifDescr
[4] .1.10.1.1.1.10.2.2.1.3  IF-MIB::ifType
```

- 如需 OID 的詳細資訊，請查看 SNMP Object Navigator

<https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en>

- 在 FXOS (41xx/9300) 上，透過 FXOS CLI 執行下列 2 個命令：

```

<#root>

FP4145-1#

connect fxos

FP4145-1(fxos)#

show snmp internal oids supported create

FP4145-1(fxos)#

show snmp internal oids supported

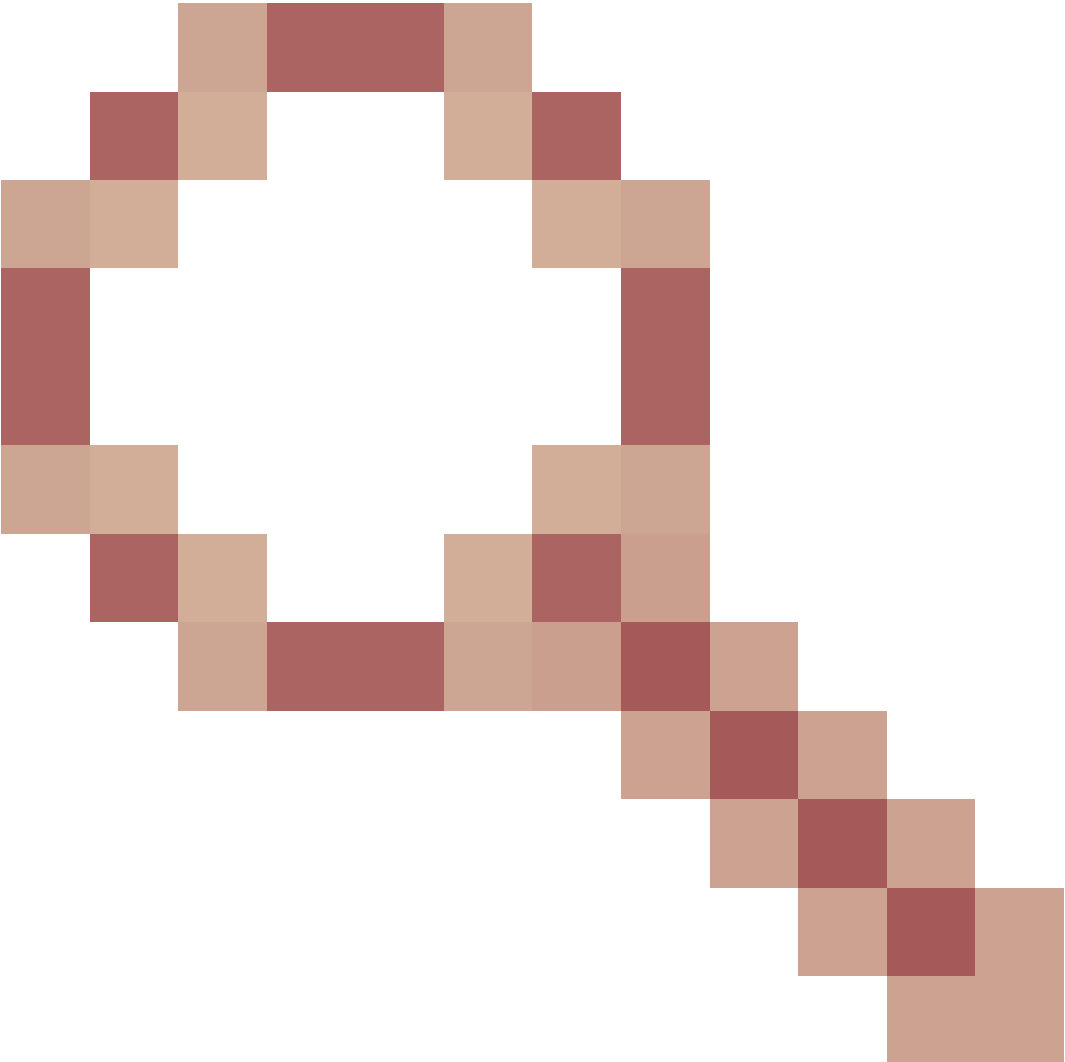
- SNMP All supported MIB OIDs -0x11a72920
Subtrees for Context:
ccitt
1
1.0.88010.1.1.1.1.1.1.1 ieee8021paeMIB
1.0.88010.1.1.1.1.1.1.2
...

```

## 常見 OID 快速參考

需求	OID
CPU (LINA)	1.3.6.1.4.1.9.9.109.1.1.1
CPU (Snort)	1.3.6.1.4.1.9.9.109.1.1.1 (FP >= 6.7)
記憶體 (LINA)	1.3.6.1.4.1.9.9.221.1.1
記憶體 (Linux/FMC)	1.3.6.1.1.4.1.2021.4
HA 資訊	1.3.6.1.4.1.9.9.491.1.4.2
叢集資訊	1.3.6.1.4.1.9.9.491.1.8.1
VPN 資訊	RA-VPN會話數 : 1.3.6.1.4.1.9.9.392.1.3.1 (7.x) RA-VPN使用者數 : 1.3.6.1.4.1.9.9.392.1.3.3 (7.x) RA-VPN峰值會話 : 1.3.6.1.4.1.9.9.392.1.3.41 (7.x) S2S VPN會話數 : 1.3.6.1.4.1.9.9.392.1.3.29

	<p>S2S VPN峰值會話數 : 1.3.6.1.4.1.9.9.392.1.3.31</p> <p>- 提示 : firepower# show snmp-server oid   我喜歡</p>
<p>BGP 狀態</p>	 <p>增強型思科漏洞ID <a href="#">CSCux13512</a> : 增加用於SNMP輸詢的BGP MIB</p>
<p>FPR1K/2K ASA/ASA v 智慧型 授權</p>	 <p>增強型思科漏洞ID <a href="#">CSCvv83590</a> : FPR1k/2k上的ASA v/ASA : 需要SNMP OID以跟蹤智慧許可的狀態</p>
<p>FXOS 層級連接埠 通道的 LINA SNMP OID</p>	<p>增強型思科漏洞ID <a href="#">CSCvu91544</a></p>

	
	: 支援Lina SNMP OID，用於FXOS級埠通道介面統計資訊

FMC 7.3新增 ( 適用於FMC 1600/2600/4600及更新版本 )

需求	OID
風扇狀態陷阱	陷阱OID : 1.3.6.1.4.1.9.9.117.2.0.6 值OID : 1.3.6.1.4.1.9.9.117.1.4.1.1.1。 <index> 0 -風扇未運行 1 -風扇正在運行
CPU/PSU溫度陷阱	陷阱OID : 1.3.6.1.4.1.9.9.91.2.0.1 閾值OID : 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1 值OID : 1.3.6.1.4.1.9.9.91.1.1.1.4.<index>

PSU狀態陷阱	陷阱OID : 1.3.6.1.4.1.9.9.117.2.0.2 OperStatus OID : 1.3.6.1.4.1.9.9.117.1.1.2.1.2.<index> 管理狀態OID : 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<index>  0 -未檢測到電源供應器  1 -檢測到電源供應器存在 , 正常
---------	--

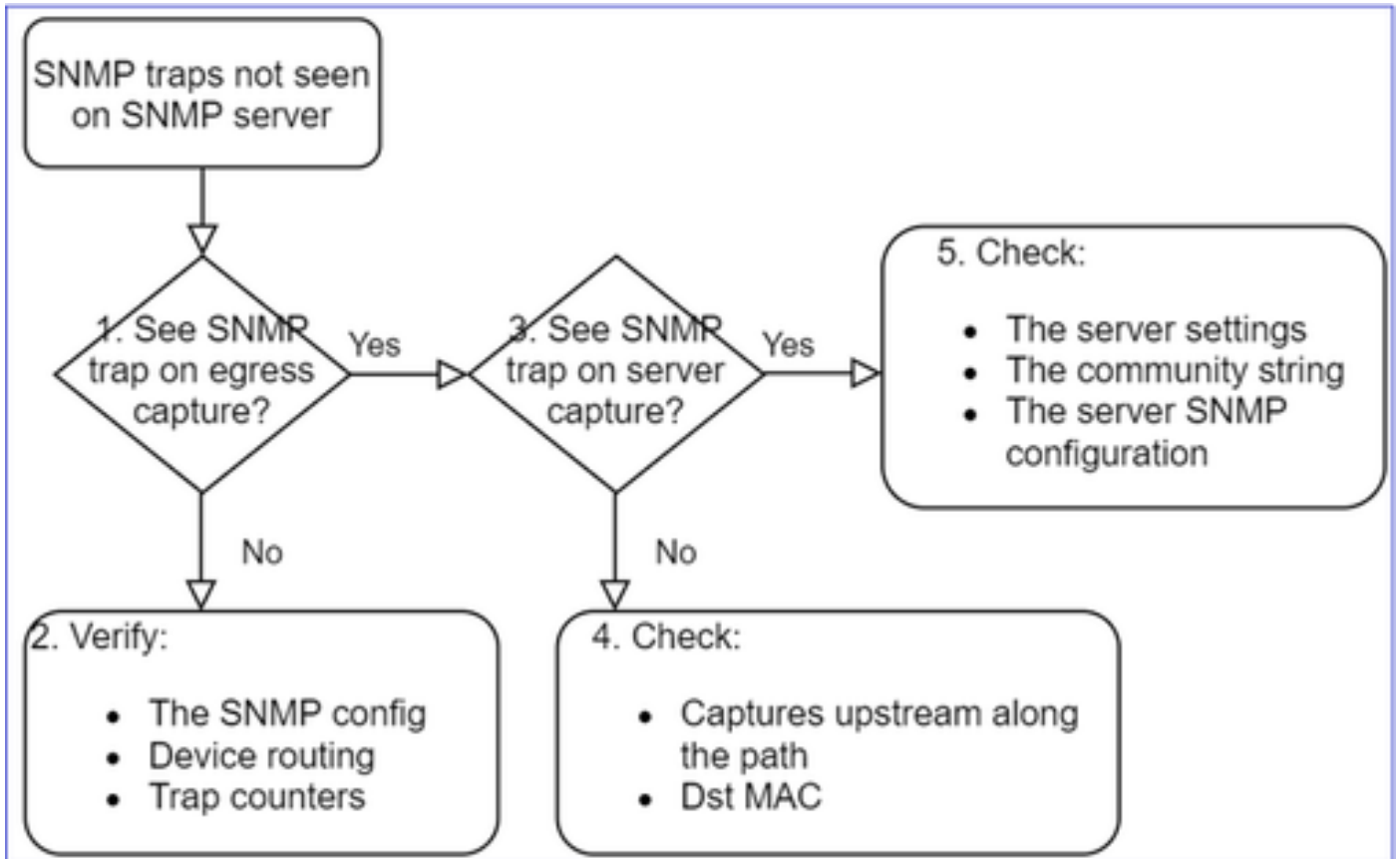
## 無法取得 SNMP 設陷

問題說明 ( 來自 Cisco TAC 真實案例的範例 ) :

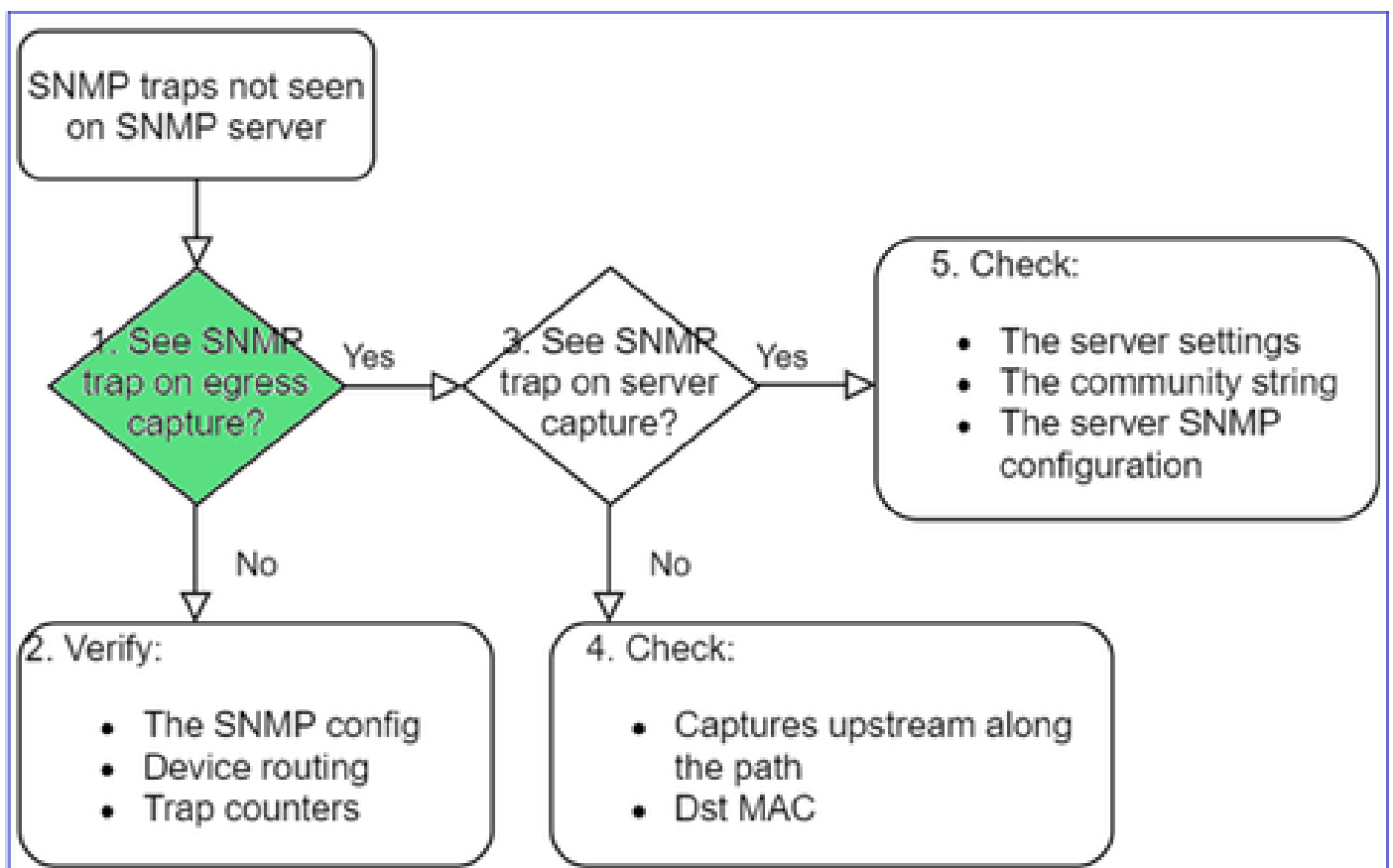
- 「FTD 的 SNMPv3 不會傳送任何設陷到 SNMP 伺服器。」
- 「FMC 和 FTD 不會傳送 SNMP 設陷訊息。」
- 「我們已針對 FXOS 在 FTD 4100 上設定 SNMP , 並嘗試使用 SNMPv3 和 SNMPv2 , 但兩者都無法傳送設陷。」
- 「Firepower SNMP 不會傳送設陷到監控工具。」
- 「Firewall FTD 不會傳送 SNMP 設陷到 NMS。」
- 「SNMP 伺服器設陷無法運作。」
- 「我們已針對 FXOS 在 FTD 4100 上設定 SNMP , 並嘗試使用 SNMPv3 和 SNMPv2 , 但兩者都無法傳送設陷。」

## 建議的疑難排解

以下是對Firepower SNMP陷阱問題進行故障排除的流程圖 :



1. 您是否看到出口捕獲上的SNMP陷阱？



在管理介面上擷取 LINA/ASA 設限：

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management0
```

```
1 - Global
```

```
Selection?
```

```
0
```

```
Options:
```

```
-n host 192.168.2.100 and udp port 162
```

在資料介面上擷取 LINA/ASA 設限：

```
<#root>
```

```
firepower#
```

```
capture SNMP interface net208 match udp any any eq 162
```

擷取 FXOS 設限 ( 41xx/9300 )：

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
firepower(fxos)#
```

```
ethalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 500 write workspace
```

```
1 2021-08-02 11:22:23.661436002 10.62.184.9 → 10.62.184.23 SNMP 160 snmpV2-trap 10.3.1.1.2.1.1.3.0 10.3.1.1.1.2.1.1.3.0
```

```
firepower(fxos)#
```

```
exit
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

```
dir
```

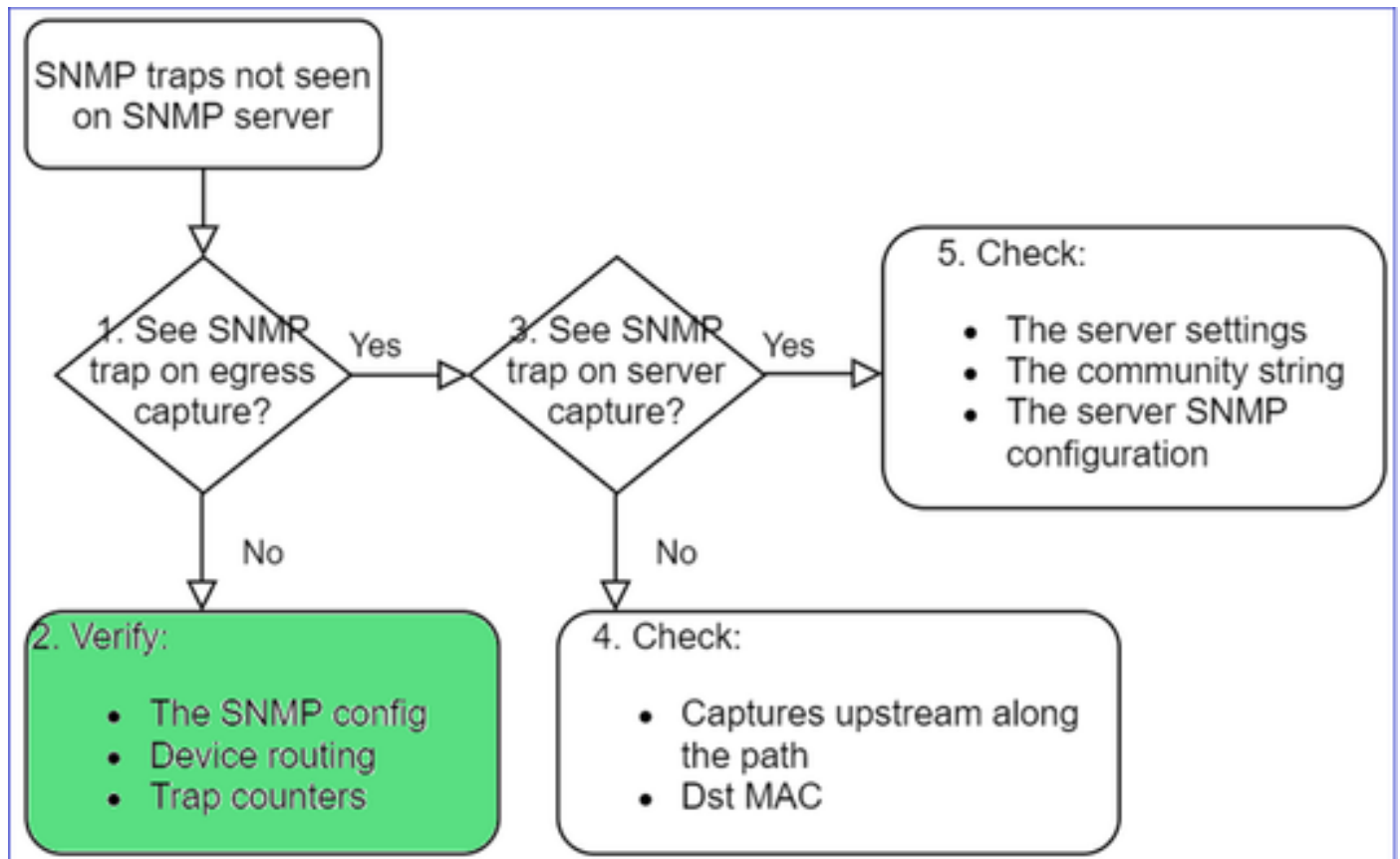
```
1 11134 Aug 2 11:25:15 2021 SNMP.pcap
```

```
firepower(local-mgmt)#
```



copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap

## 2. 如果在輸出介面上未看到封包



<#root>

firepower#

```
show run all snmp-server
```

```
snmp-server host ngfw-management 10.62.184.23 version 3 Cisco123 udp-port 162
snmp-server host net208 192.168.208.100 community ***** version 2c udp-port 162
snmp-server enable traps failover-state
```

FXOS SNMP 設陷組態：

<#root>

FP4145-1#

```
scope monitoring
```

FP4145-1 /monitoring #

```
show snmp-trap
```

SNMP Trap:

SNMP Trap	Port	Community	Version	V3 Privilege	Notification Type
192.168.2.100	162	****	V2c	Noauth	Traps

注意：在1xxx/21xx上，您只能在Devices > Device Management > SNMP config！的情況下看到這些設定。

- 設陷的 LINA/ASA 路由（透過管理介面）：

```
<#root>
```

```
>
```

```
show network
```

- 設陷的 LINA/ASA 路由（透過資料介面）：

```
<#root>
```

```
firepower#
```

```
show route
```

- FXOS 路由（41xx/9300）：

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- 設陷計數器（LINA/ASA）：

```
<#root>
```

```
firepower#
```

```
show snmp-server statistics | i Trap
```

```
20 Trap PDUs
```

FXOS 則如下：

```
<#root>
```

```
FP4145-1#
```

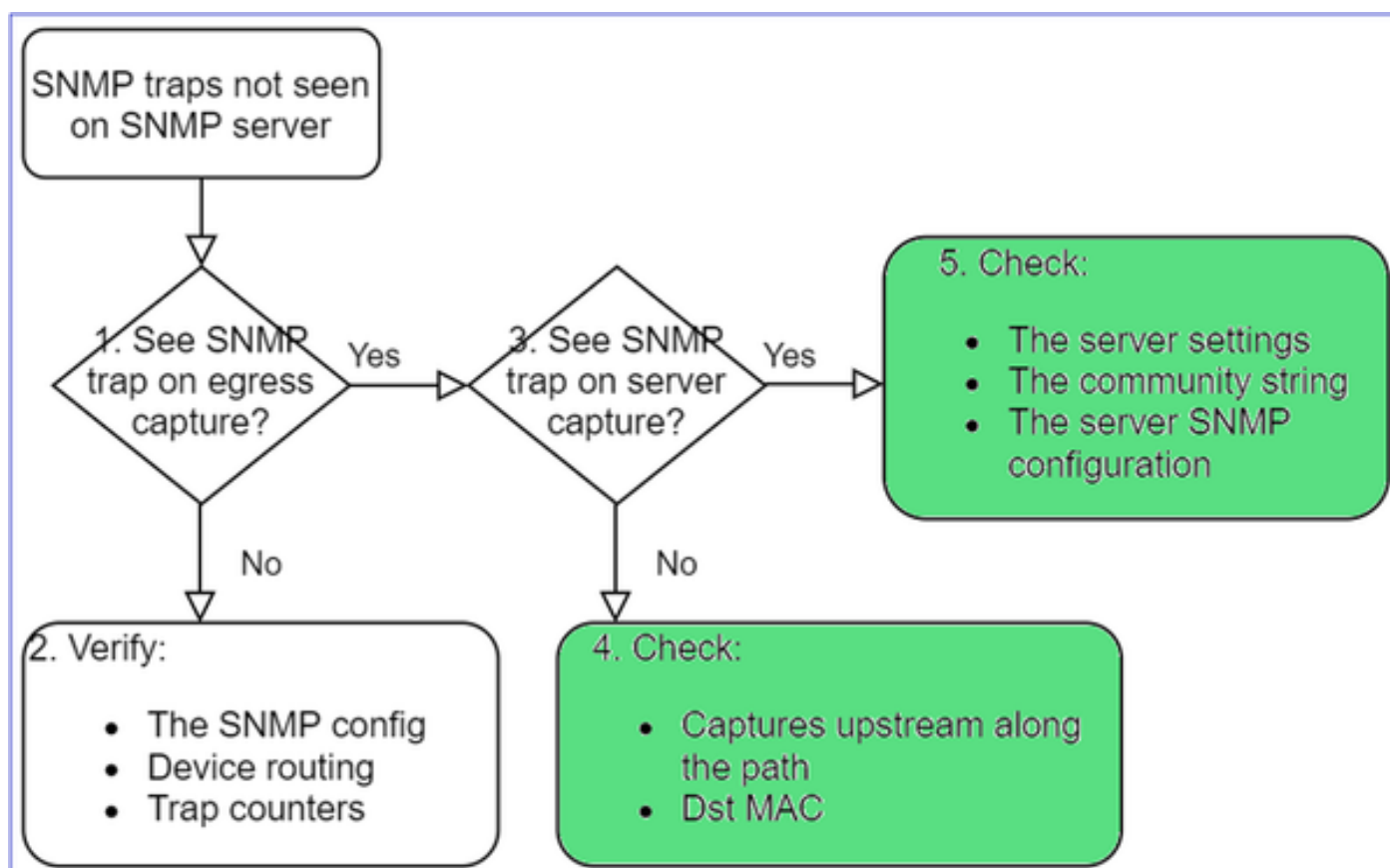
```
connect fxos
```

```
FP4145-1(fxos)#
```

```
show snmp | grep Trap
```

```
1296 Out Traps PDU
```

### 其他檢查



- 在目的地 SNMP 伺服器上進行擷取。

要檢查的其他項目：

- 沿著路徑的擷取。
- SNMP 設陷封包的目的地 MAC 位址。
- SNMP 伺服器設定和狀態（例如，防火牆、打開埠等）。
- SNMP 社群字串。
- SNMP 伺服器組態。

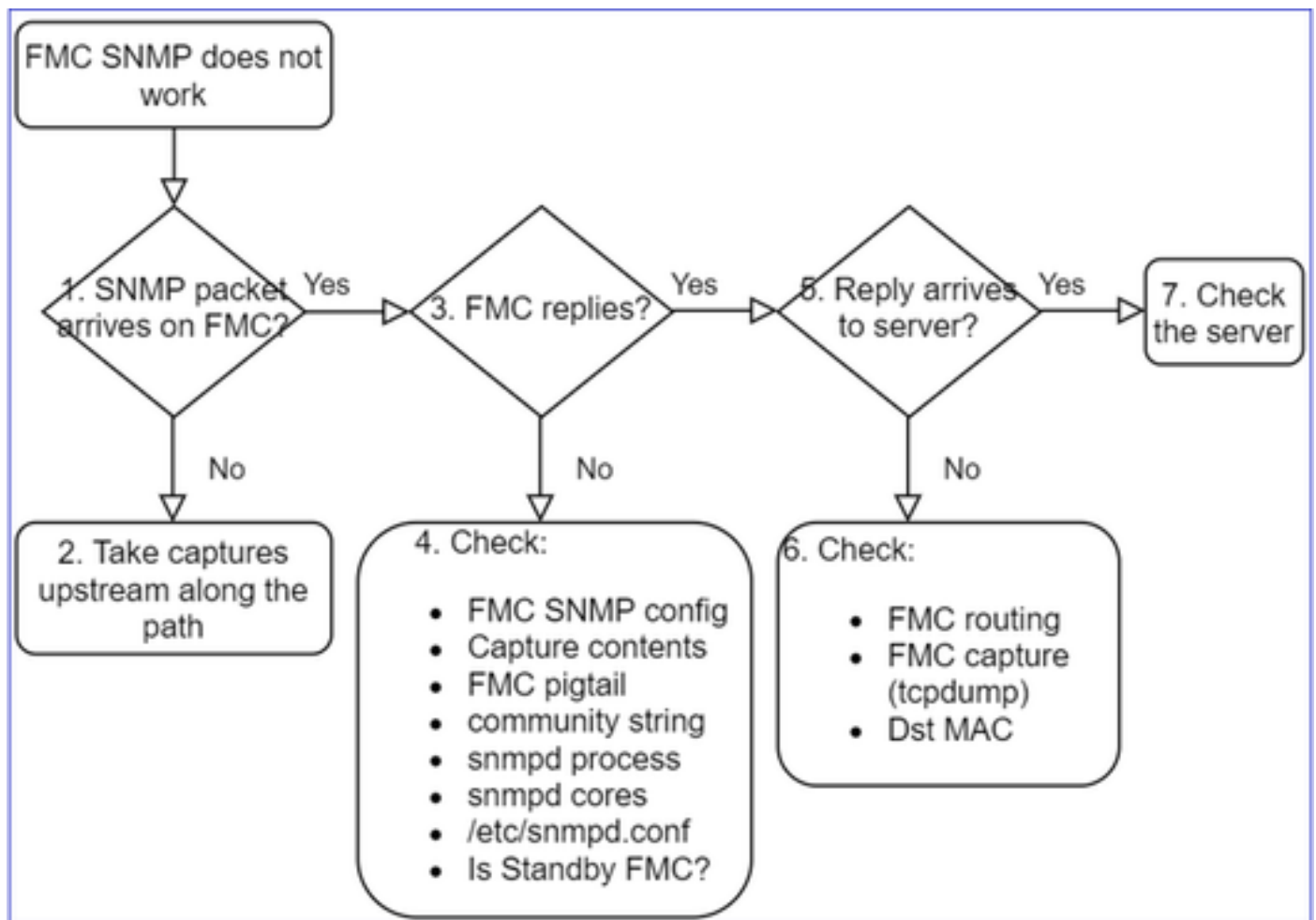
## 無法透過 SNMP 監控 FMC

問題說明 ( 來自 Cisco TAC 真實案例的範例 ) :

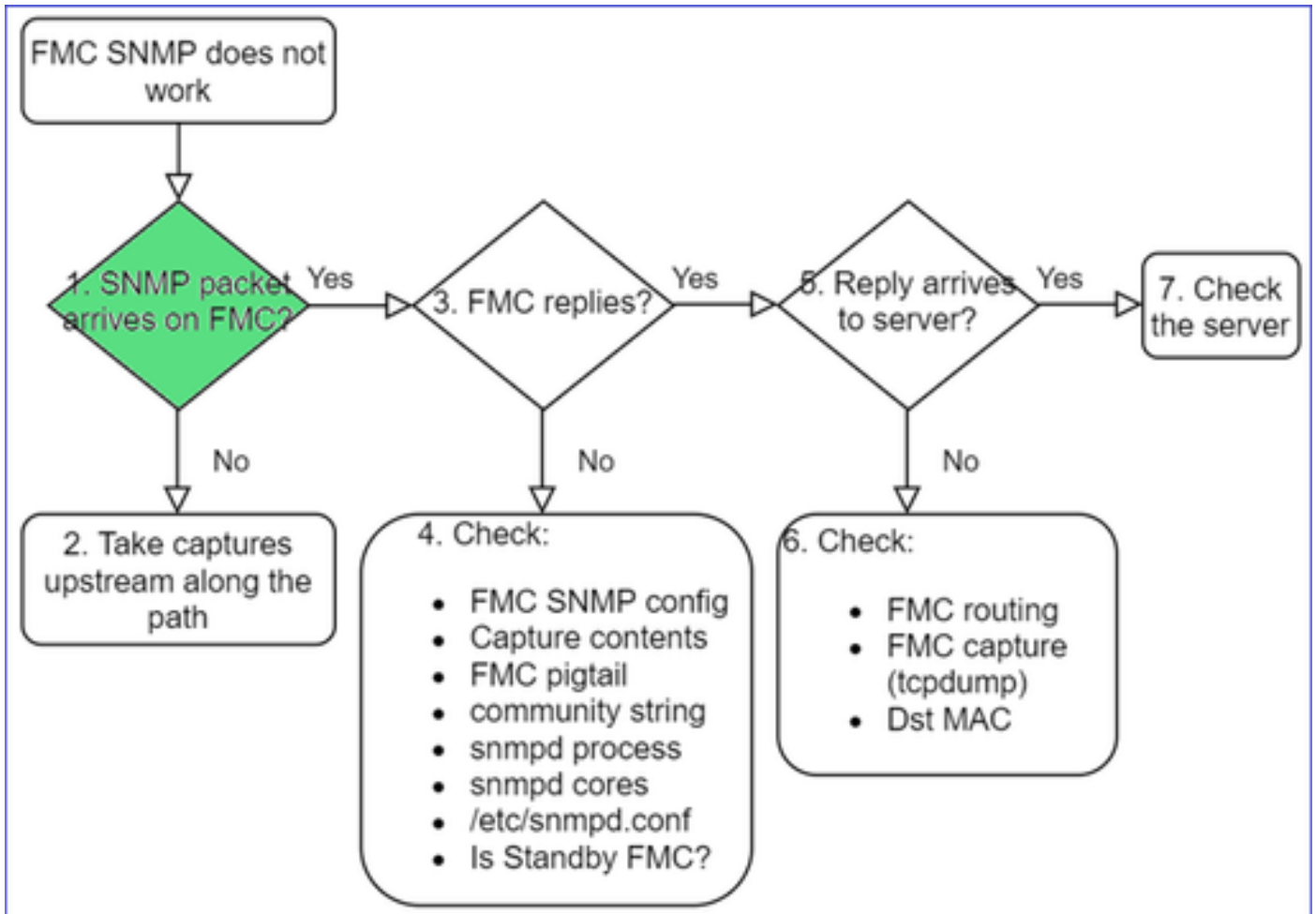
- 「SNMP 在待命 FMC 上無法運作。」
- 「需要監控 FMC 記憶體。」
- 「在待命 192.168.4.0.8 FMC 上，SNMP 是否應可正常運作？」
- 「我們必須配置FMC以監控其資源，如CPU、記憶體等。」

如何疑難排解

以下是對FMC SNMP問題進行故障排除的流程圖：



1. SNMP 封包已傳送至 FMC ?



- FMC 管理介面的擷取：

<#root>

```
admin@FS2600-2:~$
```

```
sudo tcpdump -i eth0 udp port 161 -n
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
10:58:45.961836 IP 192.168.2.10.57076 > 192.168.2.23.161: C="Cisco123" GetNextRequest(28) .10.3.1.1.4.
```



提示：將捕獲儲存在FMC /var/common/目錄下，然後從FMC UI下載

<#root>

```
admin@FS2600-2:~$
```

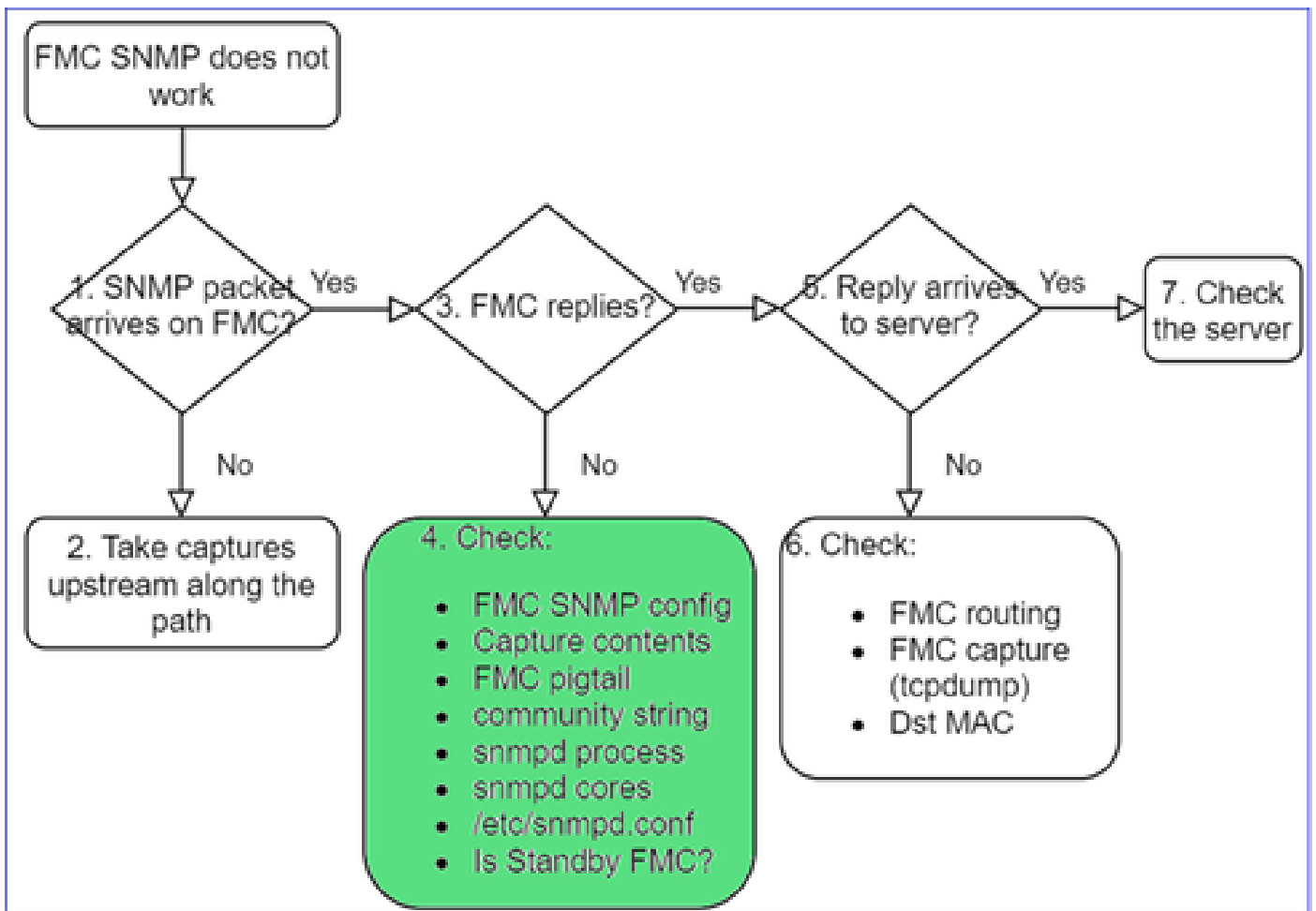
```
sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

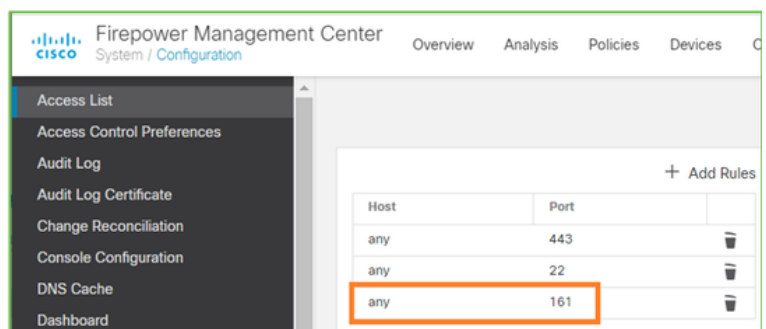
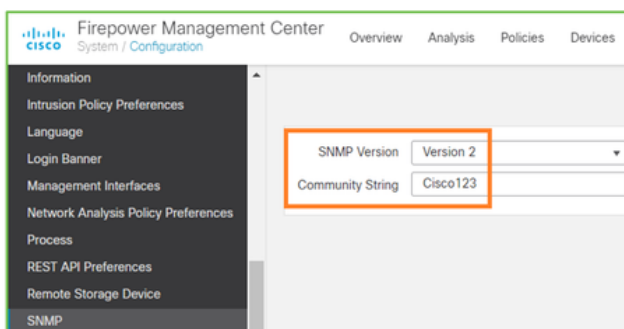
^C46 packets captured  
46 packets received by filter

FMC 是否回覆？



如果 FMC 未回覆，請檢查：

- FMC SNMP 組態 (「系統」>「組態」)
  1. SNMP 區段
  2. 存取清單區段



如果 FMC 未回覆，請檢查：

- 擷取 (pcap) 內容

- 社群字串 ( 這可以在擷取中看到 )
- FMC 接續用引線輸出 ( 尋找錯誤、失敗、追蹤 ) 和 /var/log/snmpd.log 的內容
- snmpd 程序

<#root>

```
admin@FS2600-2:~$
```

```
sudo pmtool status | grep snmpd
```

```
snmpd (normal) - Running 12948
Command: /usr/sbin/snmpd -c /etc/snmpd.conf -Ls daemon -f -p /var/run/snmpd.pid
PID File: /var/run/snmpd.pid
Enable File: /etc/snmpd.conf
```

- snmpd 核心

<#root>

```
admin@FS2600-2:~$
```

```
ls -al /var/common | grep snmpd
```

```
-rw----- 1 root root          5840896 Aug  3 11:28 core_1627990129_FS2600-2_snmpd_3.12948
```

- /etc/snmpd.conf 中的後端組態檔案：

<#root>

```
admin@FS2600-2:~$
```

```
sudo cat /etc/snmpd.conf
```

```
# additional user/custom config can be defined in *.conf files in this folder
includeDir /etc/snmp/config.d
engineIDType 3
agentaddress udp:161,udp6:161
rocommunity Cisco123
rocommunity6 Cisco123
```

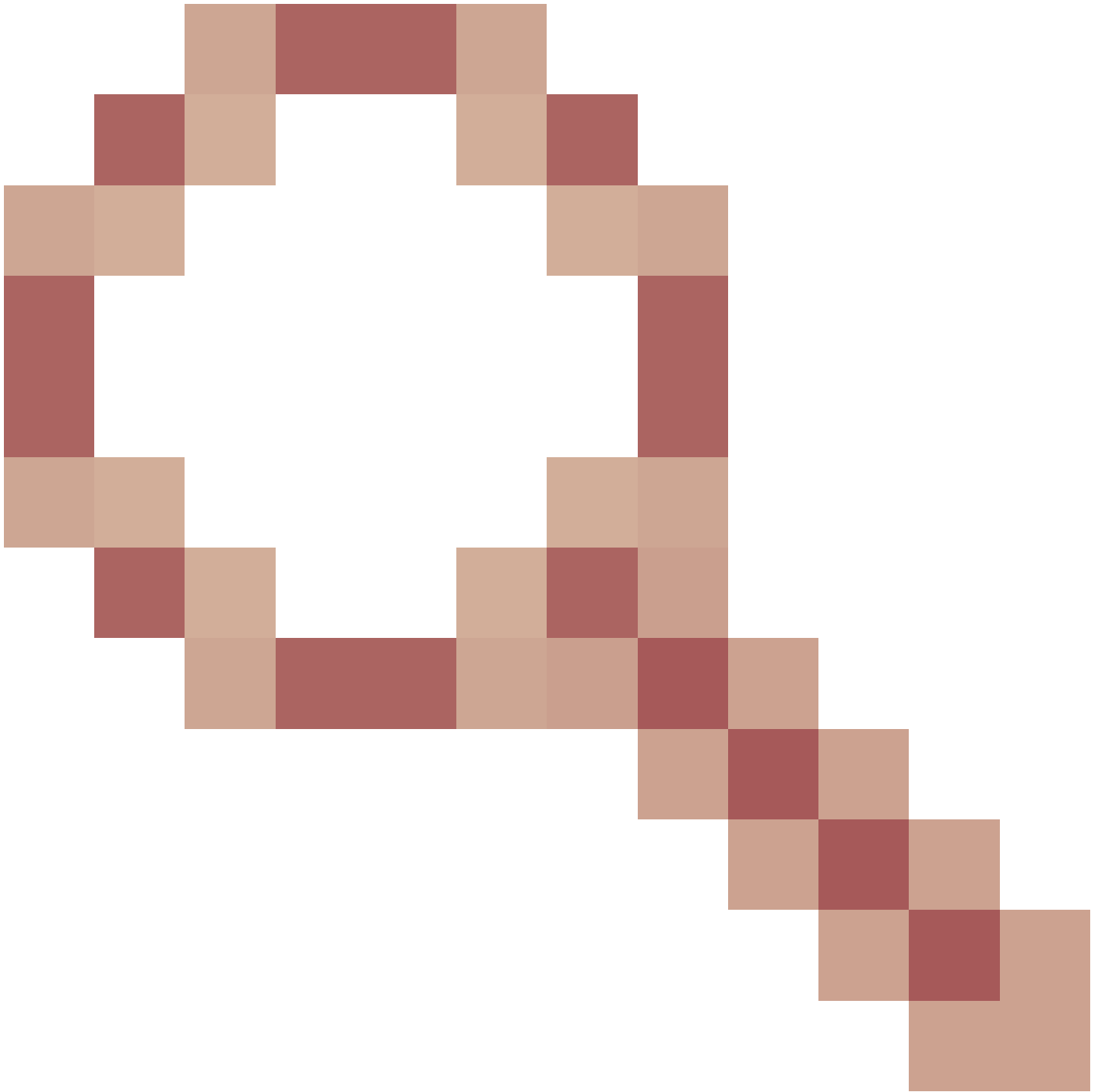
---

 注意：如果已停用SNMP，則snmpd.conf檔案不存在

---

- 是否為待命 FMC？

在 6.4.0-9 之前和 6.6.0 之前的版本中，待命 FMC 不會傳送 SNMP 資料 ( snmpd 處於「等待」狀態 )。這是預期行為。檢查增強功能思科漏洞ID [CSCvs32303](#)



## 無法設定 SNMP

問題說明 ( 來自 Cisco TAC 真實案例的範例 ) :

- 「我們想要為 Cisco Firepower Management Center 和 Firepower 4115 Threat Defense 設定 SNMP。」
- 「FTD上有SNMP設定的支援」。
- 「我們想要在 FTD 設備上啟用 SNMP 監控。」
- 「我們嘗試在 FXOS 中設定 SNMP 服務，但系統最後不讓我們執行 commit-buffer。它顯示「錯誤：不允許變更。請使用『連線ftd』進行變更。」
- 「我們想要在 FTD 設備上啟用 SNMP 監控。」
- 「無法在 FTD 上設定 SNMP 和探索監控中裝置。」



## 如何處理 SNMP 組態問題

首要任務：說明檔案！

- 閱讀目前的文件！
- FMC 組態指南：

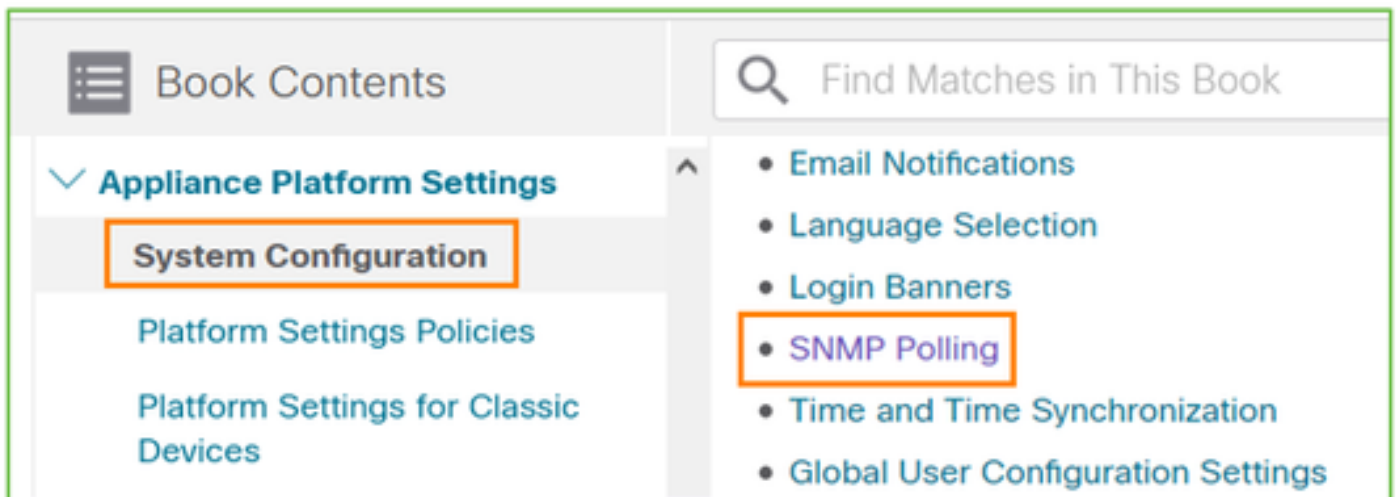
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- FXOS 組態指南：

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b\\_GUI\\_FXOS\\_ConfigGuide\\_2101/platform\\_settings.html#topic\\_6C6725BBF4BC4333BA207BE9DB](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB)

請注意各種 SNMP 文件！

FMC SNMP：



FXOS SNMP：

# Cisco Firepower 4100/9300 FXOS Firepower

Book Contents

Find Matches in This Book

Book Title Page

Introduction to the Firepower Security Appliance

Getting Started

License Management for the ASA

User Management

Image Management

Security Certifications Compliance

System Administration

**Platform Settings**

Chapter: Platform Settings

> Chapter Contents

- Setting the Date and Time
- Configuring SSH
- Configuring TLS
- Configuring Telnet
- **Configuring SNMP**
- Configuring HTTPS

Firepower 41xx/9300 SNMP 組態 :

✓ Appliance Platform Settings

System Configuration

Platform Settings Policies

Platform Settings for Classic Devices

**Platform Settings for Firepower Threat Defense**

Firepower 1xxx/21xx SNMP 組態 :

## Firepower Threat Defense Interfaces and Device Settings

Interface Overview for Firepower Threat Defense

Regular Firewall Interfaces for Firepower Threat Defense

Inline Sets and Passive Interfaces for Firepower Threat Defense

DHCP and DDNS Services for Threat Defense

SNMP for the Firepower 1000/2100

### Firepower Device Manager (FDM) 的 SNMP 組態

問題說明 ( 來自 Cisco TAC 真實案例的範例 ) :

- 「我們需要具有 FDM 之 Firepower 裝置的 SNMPv3 相關指引。」
- 「SNMP 組態無法透過 FDM 在 FPR 2100 裝置上運作。」
- 「無法讓 SNMP v3 組態在 FDM 上運作。」
- 「FDM 6.7 SNMP 組態協助。」
- 「在 Firepower FDM 中啟用 SNMP v3。」

如何處理 SNMP FDM 組態問題

- 若為 6.7 之前的版本，您可以使用 FlexConfig 來進行 SNMP 組態設定：

<https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-advanced.html>

- 從 Firepower 版本 6.7 開始，已不再使用 FlexConfig 進行 SNMP 組態設定，而是使用 REST API：

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/216551-configure-and-troubleshoot-snmp-on-firep.html>

### SNMP 疑難排解速查表

1xxx/21xx/41xx/9300 (LINA/ASA) – 透過 Cisco TAC 開啟案例之前要收集的項目

指令	說明
firepower# show run snmp-server	驗證 ASA/FTD LINA SNMP 組態.
firepower# show snmp-server statistics	驗證 ASA/FTD LINA 的 SNMP 統計資料。請注意

	SNMP 封包輸入和 SNMP 封包輸出計數器。
> capture-traffic	擷取管理介面的流量。
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	擷取UDP 161的資料介面流量 ( 名稱為if 'net201' ) ( SNMP輪詢 ) 。
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	為UDP 162捕獲資料介面 ( 名稱為if 'net208' ) 上的流量。 ( SNMP陷阱 ) 。
firepower# show capture SNMP-POLL packet-number 1 trace	追蹤到達ASA/FTD LINA資料介面的輸入SNMP封包。
admin@firepower:~\$ sudo tcpdump -i tap_nlp	NLP ( 非 LINA 程序 ) 內部 TAP 介面的擷取。
firepower# show conn all protocol udp port 161	檢查UDP 161上的所有ASA/FTD LINA連線 ( SNMP輪詢 ) 。
firepower# show log   我302015.*161	檢查 SNMP 輪詢的 ASA/FTD LINA 記錄 302015.
firepower# more system:running-config   i社群	檢查 SNMP 社群字串。
firepower# debug menu netsnmp 4	驗證 SNMP 組態和程序 ID.
firepower# show asp table classify interface net201 domain permit match port=161	在名為「net201」的介面上檢查SNMP ACL的命中數。
firepower# show disk0:   i核心	檢查是否有任何 SNMP 核心。
admin@firepower:~\$ ls -l /var/data/cores	檢查是否有任何 SNMP 核心。僅適用於 FTD.
firepower# show route	驗證 ASA/FTD LINA 路由表。
> show network	驗證 FTD 管理層路由表。
admin@firepower:~\$ tail -f	驗證/疑難排解FTD上的SNMPv3。

/mnt/disk0/log/ma_ctx2000.log	
<pre>firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]</pre>	較新版本的隱藏命令。內部偵錯，有助於透過 Cisco TAC 對 SNMP 進行疑難排解。

41xx/9300 (FXOS) – 透過 Cisco TAC 開啟案例之前要收集的項目

指令	說明
<pre>firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture- filter "udp port 161" limit-captured-frames 50 write workspace:///SNMP-POLL.pcap firepower(fxos)# exit firepower# connect local-mgmt firepower(local-mgmt)# dir 1 11152 Jul 26 09:42:12 2021 SNMP.pcap firepower(local-mgmt)# copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap</pre>	SNMP 輪詢 (UDP 161) 的 FXOS 擷取 上傳至遠端 FTP 伺服器 FTP IP : 192.0.2.100 FTP使用者名稱 : ftp
<pre>firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture- filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap</pre>	SNMP 設限 (UDP 162) 的 FXOS 擷取
<pre>firepower# scope system firepower /system # scope services firepower /system/services # show ip-block detail</pre>	檢查 FXOS ACL
<pre>firepower# show fault</pre>	檢查是否發生 FXOS 故障

firepower# show fabric-interconnect	驗證 FXOS 介面組態和預設閘道設定
firepower# connect fxos firepower(fxos)# show running-config snmp all	驗證 FXOS SNMP 組態
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	驗證 FXOS SNMP OID
firepower# connect fxos firepower(fxos)# show snmp	驗證 FXOS SNMP 設定和計數器
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	偵錯 FXOS SNMP (「封包」或「全部」) 使用「terminal no monitor」和「undebg all」即可停止

1xxx/21xx (FXOS) – 透過 Cisco TAC 開啟案例之前要收集的項目

指令	說明
> capture-traffic	擷取管理介面的流量
> show network	驗證 FTD 管理層路由表
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	驗證 FXOS SNMP 組態
firepower# show fault	檢查是否發生 FXOS 故障

firepower# connect local-mgmt	
firepower(local-mgmt)# dir cores_fxos	檢查是否有 FXOS 核心檔案 ( 回溯 )
firepower(local-mgmt)# dir cores	

### FMC – 透過 Cisco TAC 開啟案例之前要收集的項目

指令	說明
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	擷取 SNMP 輪詢管理介面的流量
admin@FS2600-2 : ~\$ sudo tcpdump -i eth0 udp埠 161 -n -w /var/common/FMC_SNMP.pcap	擷取 SNMP 輪詢管理介面的流量，並將其儲存為檔案
admin@FS2600-2:~\$ sudo pmtool status   grep snmpd	檢查 SNMP 程序狀態
admin@FS2600-2:~\$ ls -al /var/common   grep snmpd	檢查是否有 SNMP 核心檔案 ( 回溯 )
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	檢查 SNMP 組態檔案的內容

### snmpwalk 範例

這些命令可以用來進行驗證和疑難排解：

指令	說明
# snmpwalk -c Cisco123 -v2c 192.0.2.1	使用 SNMP v2c 從遠端主機擷取所有 OID。 Cisco123 = 社群字串 192.0.2.1 = 目的地主機
# snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.9.109.1.1.1.3	使用 SNMP v2c 從遠端主機擷取特定 OID。

iso.3.6.1.4.1.9.9.109.1.1.1.1.3.1 = Gauge32 : 0	
# snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.1.4.1.9.9.109.1.1.1.1 -開啟 .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = Gauge32 : 0	以數值格式顯示擷取的 OID
# snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1	使用 SNMP v3 從遠端主機擷取所有 OID。 SNMPv3 使用者 = cisco SNMPv3 驗證 = SHA SNMPv3 授權 = AES
# snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1	使用 SNMP v3 ( MD5 和 AES128 ) 從遠端主機擷取所有 OID。
# snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1	僅限具有驗證的 SNMPv3

## 如何搜尋 SNMP 瑕疵

### 1. 導覽至

<https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV>

### 2. 輸入關鍵字snmp並選擇Select from list。

The screenshot shows the Cisco Bug Search Tool interface. At the top, it says "Tools & Resources" and "Bug Search Tool". Below this, there are several action buttons: "Save Search", "Load Saved Search", "Clear Search", and "Email Current Search". The main search area has a "Search For:" field containing the text "snmp". Below this field are examples: "Examples: CSCtd10124, router crash, etc...". There are two dropdown menus: "Product:" set to "Series/Model" and "Releases:" set to "Affecting or Fixed in these Releases". To the right of the "Product:" dropdown is a button labeled "Select from list". At the bottom of the search area, there are filter options for "Modified Date:", "Status:", "Severity:", "Rating:", "Support Cases:", and "Bug Type:". The "Bug Type:" dropdown is currently set to "Customer Visible".



Save Search Load Saved Search Clear Search Email Current Search

Search For:  Examples: CSCtd10124, router crash, etc...

Product:   Select from list

Releases:

Modified Date: Status: Severity: Rating: Support Cases: Bug Type: Customer Visible

Filter:

Viewing 1 - 25 of 159 results Sort by

**CSCvh32876 - ENH:Device level settings of FP2100 should allow to configure ACL and SNMP location**

**Symptom:** This is a feature request for an option to configure access-list to restrict specific host/network to poll device using SNMP and SNMP location. FP2100 allows you to configure ...

Severity: 6 | Status: Terminated | Updated: Jan 3, 2021 | Cases: 2 | ☆☆☆☆☆ (0)

最常見的產品：

- 思科調適型安全裝置(ASA)軟體
- Cisco Firepower 9300 系列
- Cisco Firepower 管理中心虛擬設備
- 思科 Firepower 新世代防火牆(NGFW)

## 相關資訊

- [設定 Threat Defense 的 SNMP](#)
- [在FXOS \(UI\)上配置SNMP](#)
- [技術支援與文件 - Cisco Systems](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。