

Configurazione di SNMP su appliance Firepower NGFW

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Chassis \(FXOS\) SNMP sulle appliance FPR4100/FPR9300](#)

[Configurazione di FXOS SNMPv1/v2c dalla GUI](#)

[Configurazione di FXOS SNMPv1/v2c dall'interfaccia a riga di comando \(CLI\)](#)

[Configurazione di FXOS SNMPv3 dalla GUI](#)

[Configurazione di FXOS SNMPv3 dalla CLI](#)

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

[Configurazione di LINA SNMPv2c](#)

[Configurazione di LINA SNMPv3](#)

[Unificazione SNMP blade MIO \(FXOS 2.12.1, FTD 7.2, ASA 9.18.1\)](#)

[SNMP sulle appliance FPR2100](#)

[Chassis \(FXOS\) SNMP sulle appliance FPR2100](#)

[Configurazione di FXOS SNMPv1/v2c](#)

[Configurazione di FXOS SNMPv3](#)

[FTD \(LINA\) SNMP sulle appliance FPR2100](#)

[Verifica](#)

[Verifica di FXOS SNMP sulle appliance FPR4100/FPR9300](#)

[Verifiche di FXOS SNMPv2c](#)

[Verifiche di FXOS SNMPv3](#)

[Verifica di FXOS SNMP sulle appliance FPR2100](#)

[Verifiche di FXOS SNMPv2](#)

[Verifiche di FXOS SNMPv3](#)

[Verifica di FTD SNMP](#)

[Autorizzazione del traffico SNMP diretto a FXOS sulle appliance FPR4100/FPR9300](#)

[Configurazione dell'elenco degli accessi globale dalla GUI](#)

[Configurazione dell'elenco degli accessi globale dalla CLI](#)

[Verifica](#)

[Uso di OID Object Navigator](#)

[Risoluzione dei problemi](#)

[Impossibile eseguire il polling di FTD LINA SNMP](#)

[Impossibile eseguire il polling di FXOS SNMP](#)

[Quali sono i valori SNMP OID da usare?](#)

[Impossibile richiamare le trap SNMP](#)

[Impossibile monitorare FMC con il protocollo SNMP](#)

[Configurazione del protocollo SNMP su Firepower Device Manager \(FDM\)](#)

[Appunti per la risoluzione dei problemi del protocollo SNMP](#)

[Ricerca delle anomalie SNMP](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare e risolvere i problemi relativi al protocollo SNMP (Simple Network Management Protocol) su accessori FTD Next-Generation Firewall (NGFW).

Prerequisiti

Requisiti

Il documento richiede una conoscenza base del protocollo SNMP.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le appliance NGFW Firepower possono essere suddivise in 2 categorie principali:

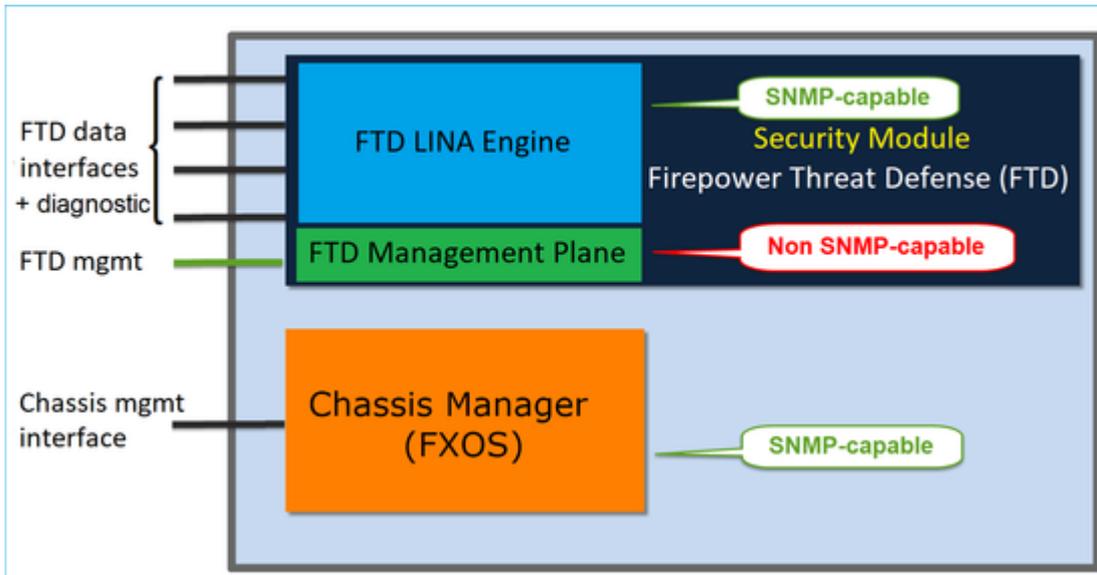
- Firepower Extensible Operative System (FXOS) per il controllo dell'hardware dello chassis.
- Firepower Threat Defense (FTD) che viene eseguito nel modulo.

FTD è un software unificato composto da due motori principali, il motore Snort e il motore LINA. L'attuale motore SNMP dell'FTD deriva dall'ASA classica e ha visibilità sulle funzionalità relative a LINA.

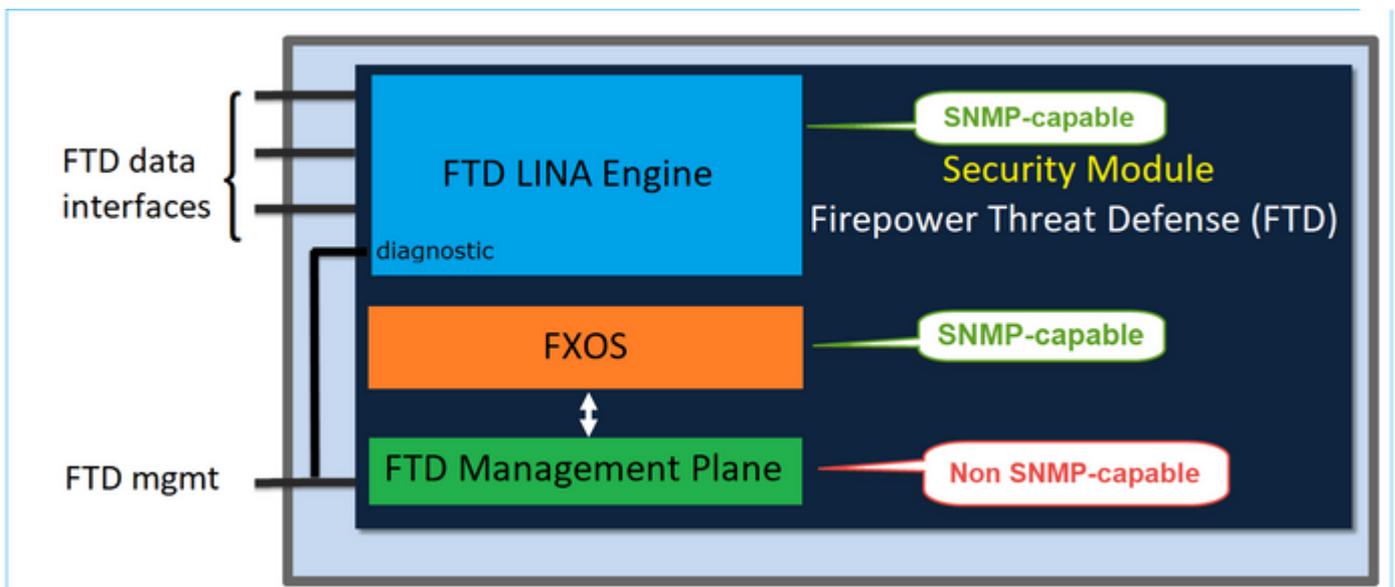
FX-OS e FTD hanno piani di controllo indipendenti e per lo scopo di monitoraggio hanno motori SNMP diversi. Ciascun motore SNMP fornisce informazioni diverse e potrebbe voler monitorare entrambi per una visualizzazione più completa dello stato del dispositivo.

Dal punto di vista hardware, attualmente esistono due architetture principali per gli accessori Firepower NGFW: Firepower serie 2100 e Firepower serie 4100/9300.

I dispositivi Firepower 4100/9300 hanno un'interfaccia dedicata per la gestione dei dispositivi, che rappresenta l'origine e la destinazione del traffico SNMP indirizzato al sottosistema FXOS. L'applicazione FTD invece utilizza un'interfaccia LINA (dati e/o diagnostica; nelle release FTD successive alla 6.6 è possibile usare anche l'interfaccia di gestione FTD) per la configurazione SNMP.



Il motore SNMP delle appliance Firepower 2100 usa l'interfaccia di gestione e l'indirizzo IP dell'FTD. L'appliance trasmette il traffico SNMP ricevuto su questa interfaccia e lo inoltra al software FXOS.

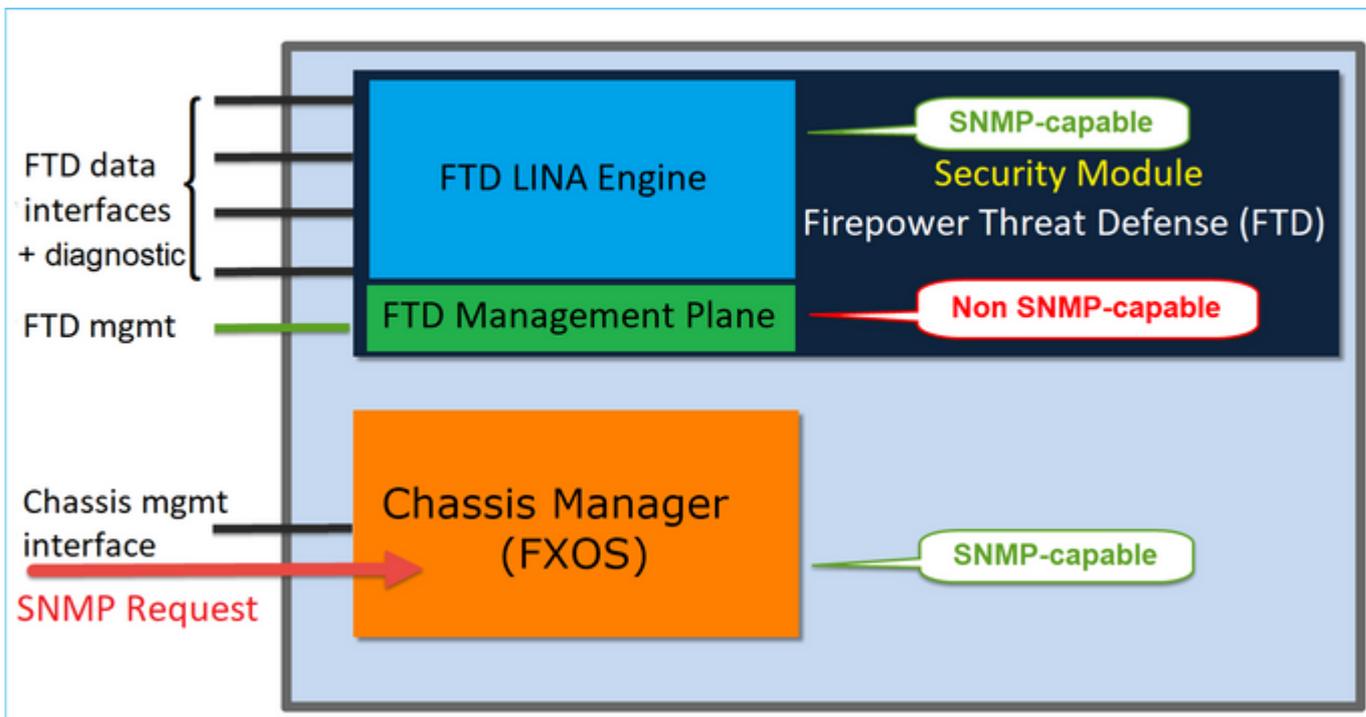


Sulle appliance FTD con release software successive alla 6.6, sono state introdotte alcune modifiche:

- SNMP sull'interfaccia di gestione.
- Sulle piattaforme FPR1000 o FPR2100, i protocolli SNMP di LINA e di FXOS sono gestiti su un'unica interfaccia. Inoltre, viene fornito un unico punto di configurazione sull'FMC in **Platform settings > SNMP** (Impostazioni piattaforma > SNMP).

Configurazione

Chassis (FXOS) SNMP sulle appliance FPR4100/FPR9300



Configurazione di FXOS SNMPv1/v2c dalla GUI

Passaggio 1. Aprire l'interfaccia utente di Firepower Chassis Manager (FCM) e selezionare **Impostazioni piattaforma** > scheda **SNMP**. Selezionare la casella di controllo SNMP, nella stringa **Community** specificare l'uso delle richieste SNMP e fare clic su **Save** (Salva).

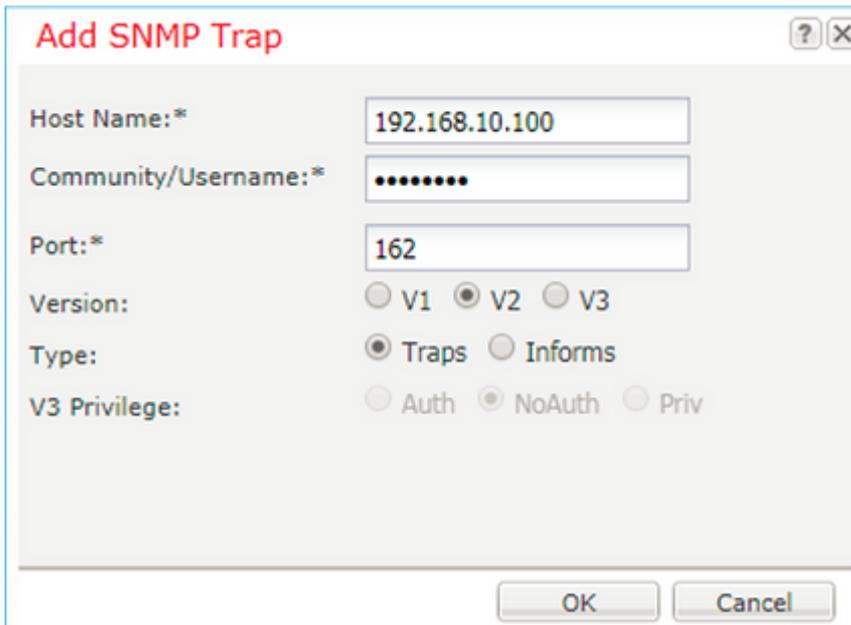
The screenshot shows the 'Platform Settings' page for SNMP configuration. The 'Admin State' is set to 'Enable' (1). The 'Port' is 161. The 'Community/Username' field is empty, and the 'Set' dropdown is 'No' (2). The 'SNMP Traps' section has an 'Add' button (4). The 'Save' button is highlighted (3).

Name	Port	Version	V3 Privilege	Type

Name	Auth Type	AES-128

Nota: se il campo Community/Username è già impostato, il testo a destra del campo vuoto è **Set: Yes**. Se nel campo Community/Username non è stato ancora inserito un valore, il testo a destra del campo vuoto è **Set: No**

Passaggio 2. Configurare il server di destinazione delle trap SNMP.



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

Nota: i valori della community per le query e l'host trap sono indipendenti e possono essere diversi

L'host può essere definito con l'indirizzo IP o con il nome. Selezionare **OK**, la configurazione del server delle trap SNMP viene salvata automaticamente. Non è necessario selezionare il pulsante Save (Salva) dalla pagina principale SNMP. Lo stesso avviene quando si elimina un host.

Configurazione di FXOS SNMPv1/v2c dall'interfaccia a riga di comando (CLI)

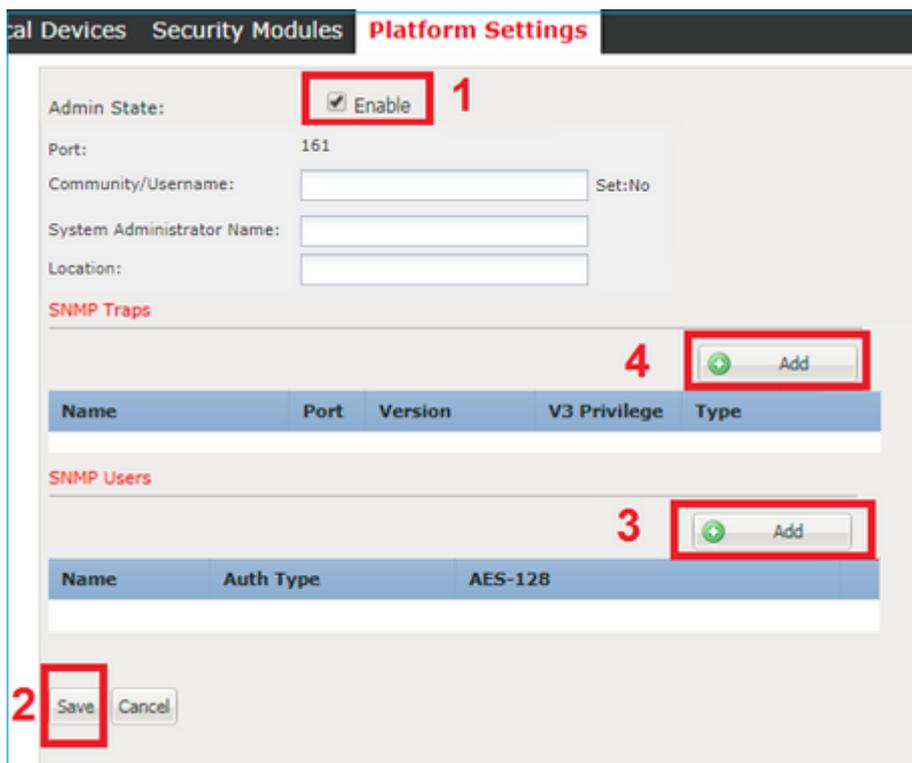
```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring* #
set snmp community
Enter a snmp community:
ksec-fpr9k-1-A /monitoring* #
  enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /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
```

Configurazione di FXOS SNMPv3 dalla GUI

Passaggio 1. Aprire FCM e selezionare **Impostazioni piattaforma** > scheda **SNMP**.

Passaggio 2. Per SNMP v3 non è necessario impostare alcuna stringa della community nella sezione superiore. Ogni utente creato è in grado di eseguire correttamente le query sul motore FXOS SNMP. La prima operazione da eseguire è abilitare SNMP nella piattaforma. Quindi, è possibile creare gli host degli utenti e delle trap di destinazione. Gli host degli utenti SNMP e delle trap SNMP vengono salvati automaticamente.



Passaggio 3. Come mostrato nell'immagine, aggiungere l'utente SNMP. Il tipo di autenticazione è sempre SHA, ma è possibile usare AES o DES per la crittografia:

Add SNMP User

Name:* user1

Auth Type: SHA

Use AES-128:

Password:

Confirm Password:

Privacy Password:

Confirm Privacy Password:

OK Cancel

Passaggio 4. Aggiungere l'host di trap SNMP, come mostrato nell'immagine:

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

Configurazione di FXOS SNMPv3 dalla CLI

```
<#root>
```

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

```
scope monitoring
```

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

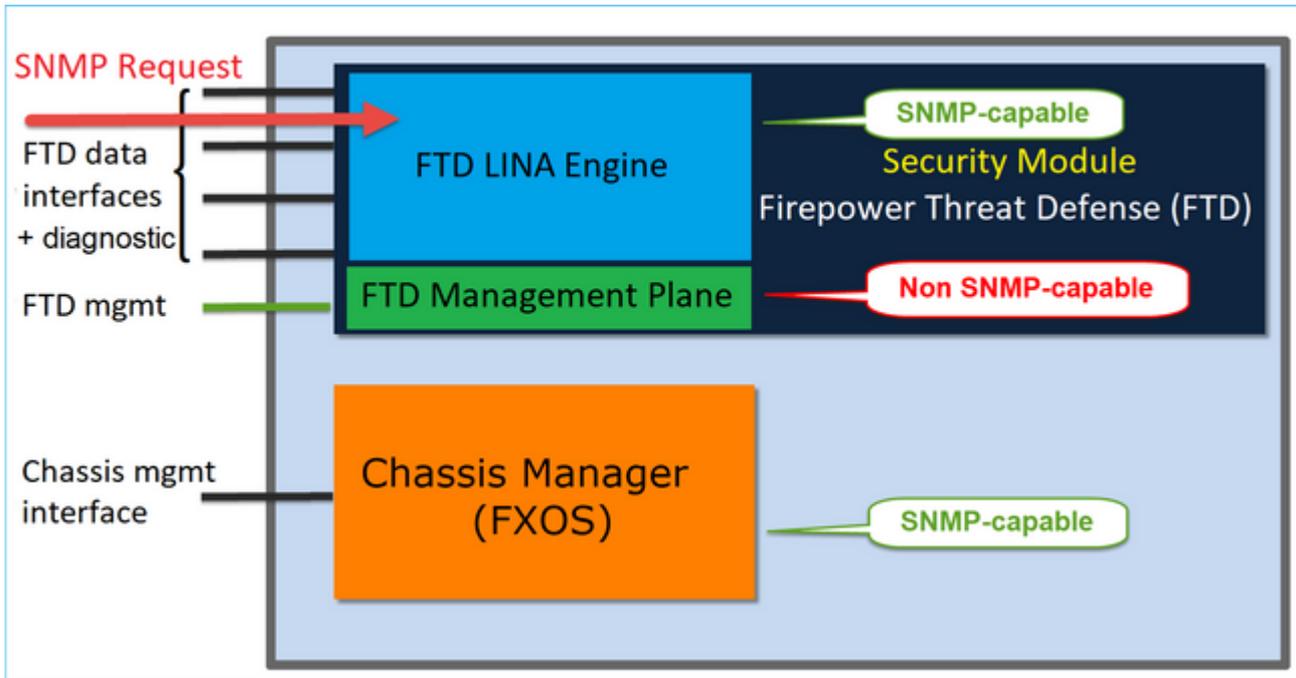
```
enable snmp
```

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

```
create snmp-user user1
```

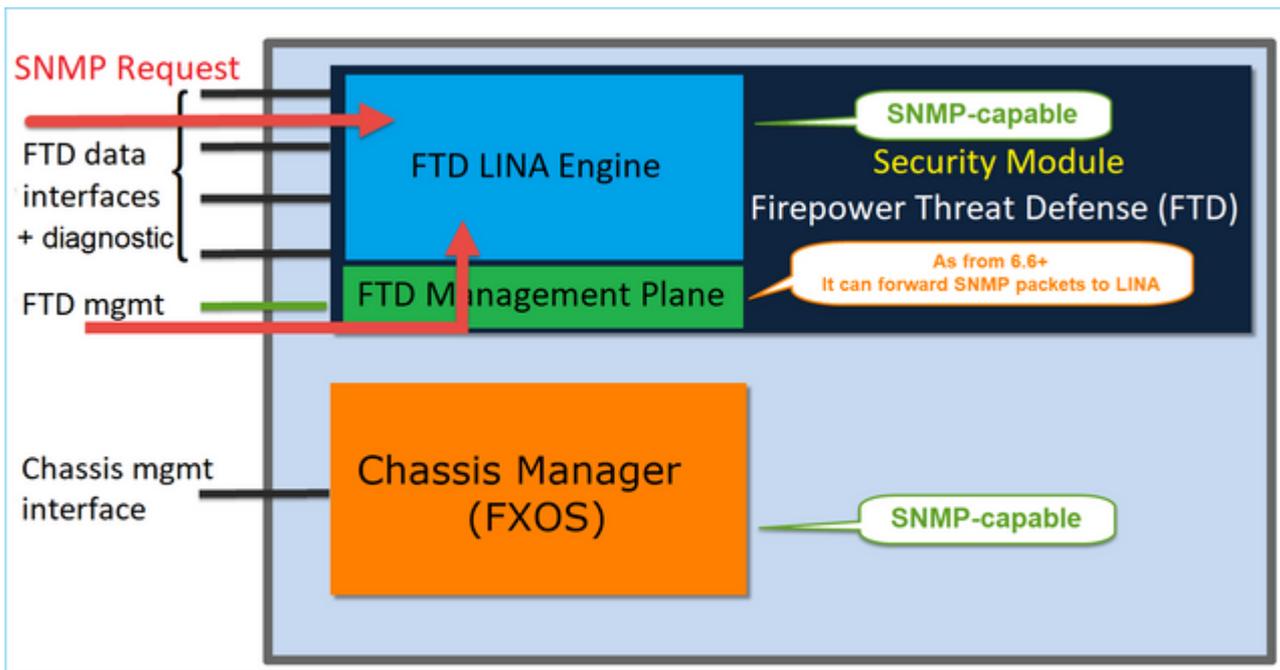
```
Password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set auth sha
ksec-fpr9k-1-A /monitoring/snmp-user* #
set priv-password
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter 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
```

FTD (LINA) SNMP sulle appliance FPR4100/FPR9300



Modifiche delle release successive alla 6.6

- Nelle release successive alla 6.6, è possibile usare anche l'interfaccia di gestione FTD per effettuare il polling e richiamare le trap.



La funzione di gestione SNMP Single IP è supportata a partire dalla versione 6.6 su tutte le piattaforme FTD:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 con FTD
- FTDv

Configurazione di LINA SNMPv2c

Passaggio 1. Nell'interfaccia utente di FMC, selezionare **Dispositivi > Impostazioni piattaforma > SNMP**. Selezionare l'opzione **Enable SNMP Servers**™ (Abilita server SNMP) e configurare le impostazioni SNMPv2 come indicato di seguito:

Passaggio 2. Nella scheda **Host**, selezionare il pulsante **Add** (Aggiungi) e specificare le impostazioni del server SNMP:

The screenshot shows the 'Edit SNMP Management Hosts' configuration window. The following fields are highlighted with orange boxes:

- IP Address*: SNMP-SERVER
- SNMP Version: 2c
- Poll:
- Trap:
- Selected Zones/Interfaces: OUTSIDE3

The 'Available Zones' list includes:

- INSIDE_FTD4110
- OUTSIDE1_FTD4110
- OUTSIDE2_FTD4110
- NET1_4100-3
- NET2_4100-3
- NET3_4100-3

The 'Selected Zones/Interfaces' list includes:

- OUTSIDE3

Buttons: Add, OK, Cancel

È inoltre possibile specificare l'interfaccia **diagnostic**, o interfaccia di diagnostica, come origine dei messaggi SNMP. L'interfaccia di diagnostica è un'interfaccia dati che consente solo il traffico da e verso il dispositivo (solo gestione).

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

- 2100_inside
- 2100_outside
- cluster_dmz
- cluster_inside
- cluster_outside

Selected Zones/Interfaces

- diagnostic

Interface Name

La schermata sopra è stata acquisita su un dispositivo con release 6.6 e Light Theme.

Inoltre, nelle release FTD successive alla 6.6 è possibile scegliere anche l'interfaccia di gestione:

Add SNMP Management Hosts

IP Address*
 +

SNMP Version

Username

Community String

Confirm

Poll
 Trap

Trap Port

(1 - 65535)

Reachable By:

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

Security Zones or Named Interface

Available Zones

- 2100_inside
- 2100_outside
- cluster_dmz
- cluster_inside
- cluster_outside

Selected Zones/Interfaces

diagnostic

Interface Name

Se si seleziona la nuova interfaccia di gestione, LINA SNMP risulta disponibile.

Il risultato:

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

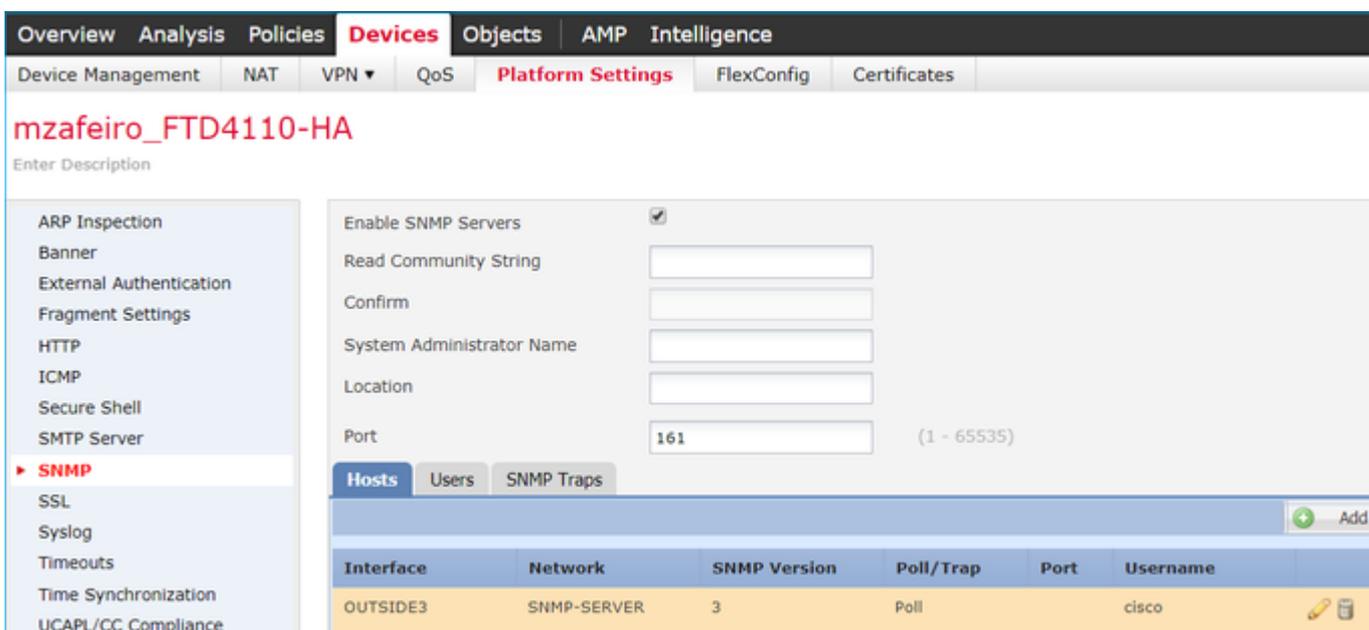
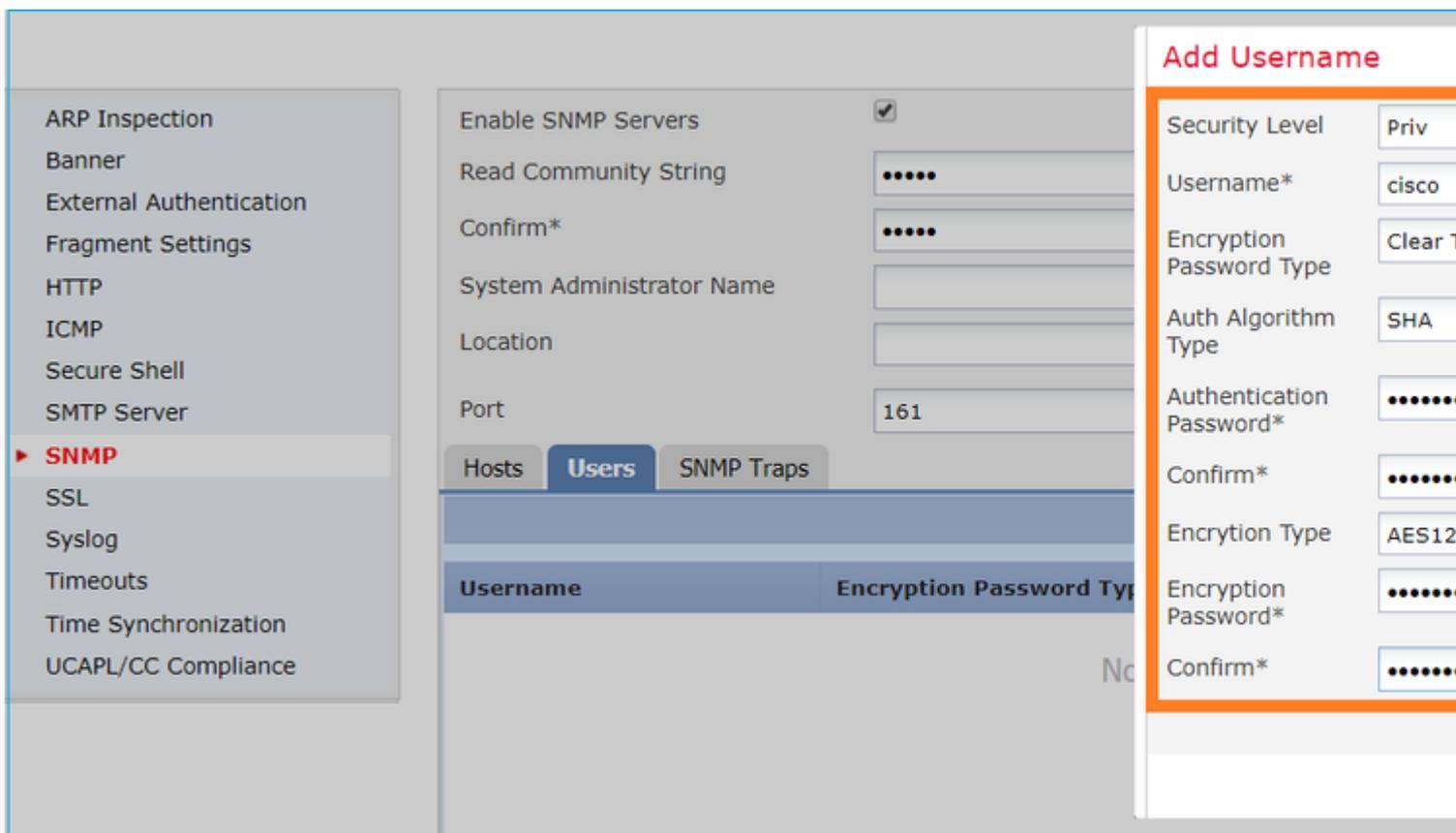
Port (1 - 65535)

Hosts Users SNMP Traps

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

Configurazione di LINA SNMPv3

Passaggio 1. Nell'interfaccia utente di FMC passare a **Dispositivi > Impostazioni piattaforma > SNMP**. Selezionare l'opzione **Enable SNMP Servers** (Abilita server SNMP) e configurare l'utente e l'host SNMPv3:



Passaggio 2. Configurare l'host anche per la ricezione di trap:

Edit SNMP Management Hosts

IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port (1 - 65535)

Available Zones

Selected Zones/Interfaces

OUTSIDE3

INSIDE_FTD4110

Passaggio 3. Le trap che si desidera ricevere possono essere selezionate nella sezione **Trap SNMP**:

SNMP

SSL

Syslog

Timeouts

Time Synchronization

UCAPL/CC Compliance

Hosts Users **SNMP Traps**

Enable Traps All SNMP Syslog

Standard

Authentication:

Link up

Link Down

Cold Start

Warm Start

Entity MIB

Unificazione SNMP blade MIO (FXOS 2.12.1, FTD 7.2, ASA 9.18.1)

Comportamento precedente alla versione 7.2

- Sulle piattaforme 9300 e 4100, i MIB SNMP per le informazioni sullo chassis non sono disponibili sul protocollo SNMP configurato sulle applicazioni FTD/ASA. È necessario configurarlo separatamente sull'MIO tramite lo chassis manager e accedervi separatamente. MIO è il modulo di gestione e I/O (Supervisor).
- È necessario configurare due criteri SNMP distinti, uno su Blade/App e l'altro su MIO per il monitoraggio SNMP.
- Vengono utilizzate porte separate, una per il blade e una per il monitoraggio di MIO per SNMP dello stesso dispositivo.
- Ciò può creare complessità quando si cerca di configurare e monitorare i dispositivi 9300 e 4100 tramite SNMP.

Come funziona sulle nuove versioni (FXOS 2.12.1, FTD 7.2, ASA 9.18.1 e versioni successive)

- Con l'unificazione SNMP del blade MIO, gli utenti possono eseguire il polling dei MIB LINA e MIO tramite le interfacce dell'applicazione (ASA/FTD).
- La funzione può essere attivata o disattivata tramite la nuova interfaccia utente MIO CLI e FCM (Chassis Mgr).
- Lo stato predefinito è disattivato. Ciò significa che l'agente SNMP MIO è in esecuzione come istanza autonoma. Le interfacce MIO devono essere utilizzate per il polling dei MIB chassis/DME. Una volta abilitata la funzione, le interfacce dell'applicazione possono essere utilizzate per eseguire il polling degli stessi MIB.
- La configurazione è disponibile nell'interfaccia utente di Chassis Manager in **Platform-settings > SNMP > Admin Instance**, in cui l'utente può specificare l'istanza FTD che raccoglierebbe/raccoglierebbe i MIB dello chassis per presentarlo all'NMS
- Sono supportate le applicazioni ASA/FTD native e MI.
- Questa funzione è applicabile solo alle piattaforme basate su MIO (FPR9300 e FPR4100).

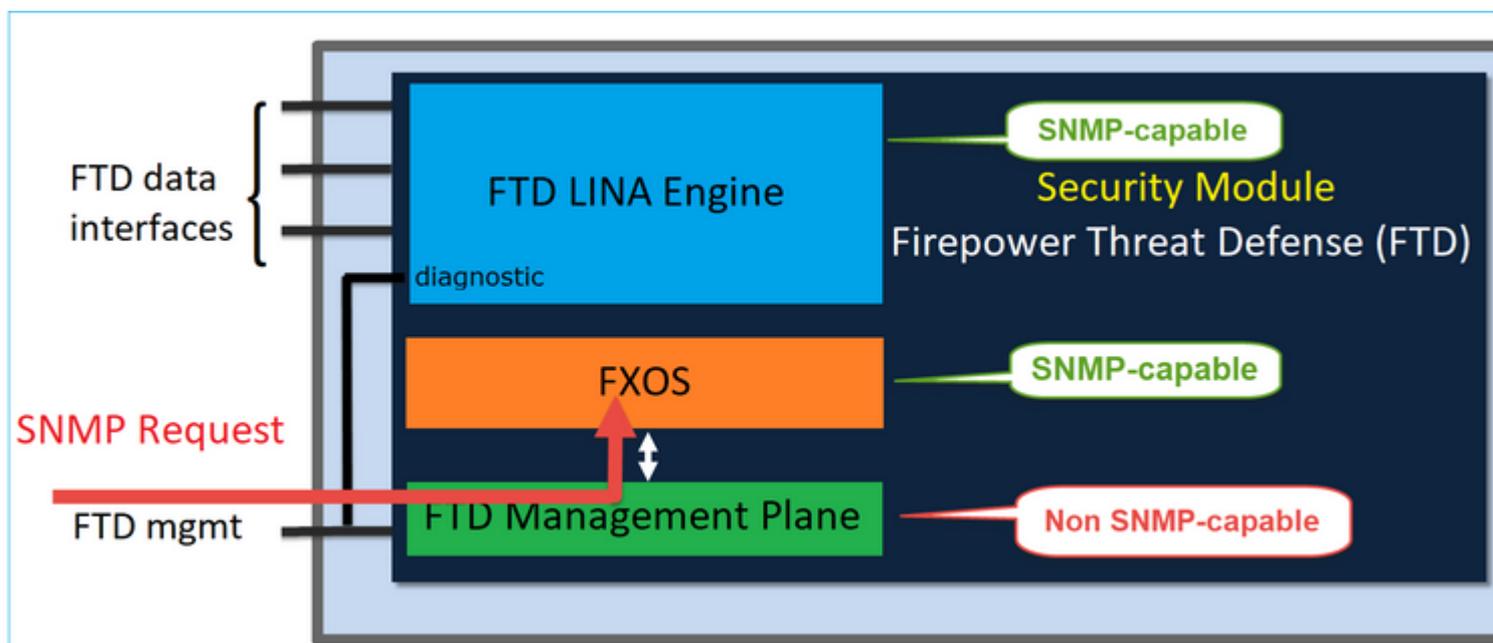
Prerequisiti, Piattaforme Supportate

- Versione minima di Gestione supportata: FCM 2.12.1
- Dispositivi gestiti: serie FPR9300/FP4100
- Versione minima del dispositivo gestito supportato: FXOS 2.12.1, FTD 7.2 o ASA 9.18.1

SNMP sulle appliance FPR2100

Sulle appliance FPR2100, FCM non è disponibile. L'unico modo per configurare il protocollo SNMP è usare FMC.

Chassis (FXOS) SNMP sulle appliance FPR2100



Sulle appliance FTD con release successive alla 6.6, è possibile usare anche l'interfaccia di gestione FTD per il protocollo SNMP. In questo caso, le informazioni SNMP di FXOS e LINA vengono trasferite sull'interfaccia di gestione FTD.

Configurazione di FXOS SNMPv1/v2c

Aprire l'interfaccia utente di FMC e selezionare **Dispositivi > Gestione dispositivi**. Selezionare il dispositivo e selezionare **SNMP**:

The screenshot shows the FMC configuration interface for device FTD2100-4. The 'SNMP' tab is selected. The 'Admin State' is 'Enable'. The 'Port' is set to 161. The 'Community' field is masked with dots. The 'SNMP Traps Configuration' table is empty, and an 'Add' button is visible. Red boxes and numbers highlight key elements: 1 points to the 'Enable' checkbox and 'Port' field; 2 points to the 'Add' button; 3 points to the 'Save' button; 4 points to the 'Deploy' button in the top navigation bar.

SNMP Trap Configuration

Hostname:* 10.48.26.190 (+)

Community String:*

Port:* 162 (1 - 65535)

SNMP Version: V2

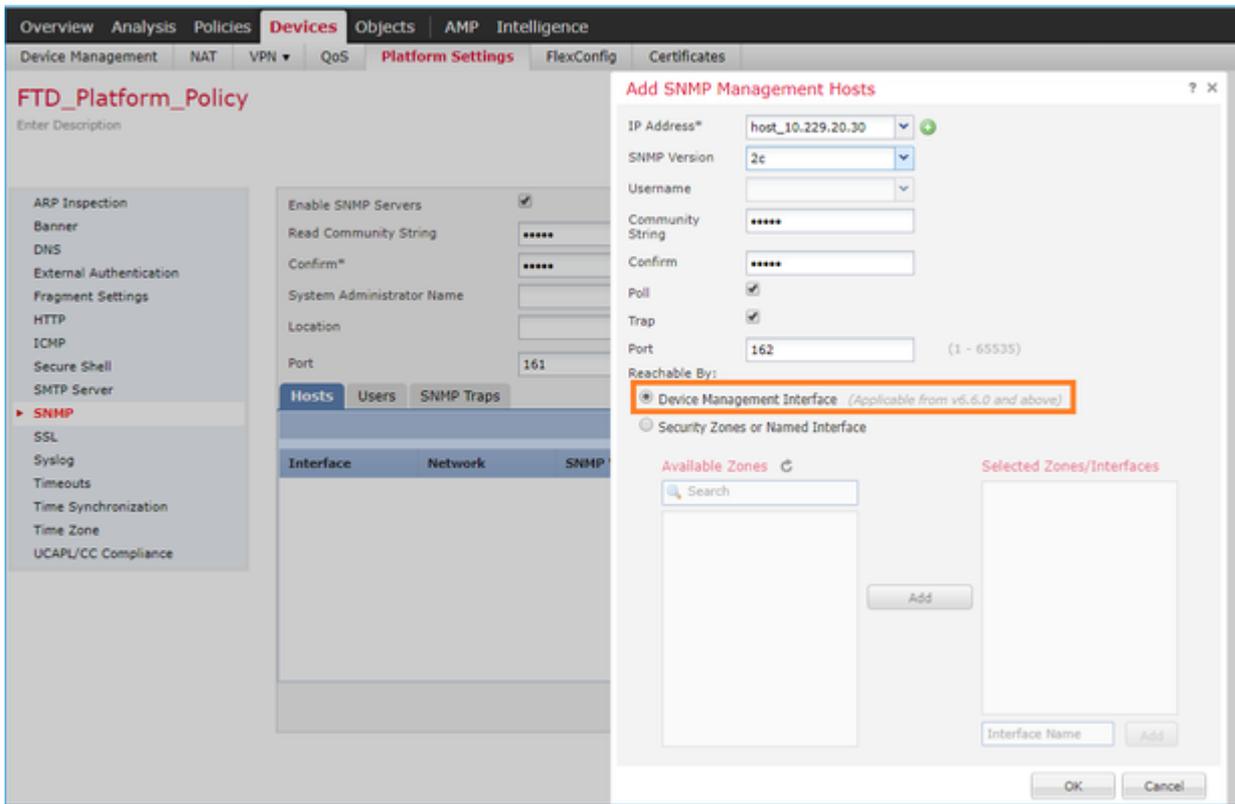
Type: TRAPS

Privilege: NO_AUTH

OK Cancel

Modifiche delle release FTD successive alla 6.6

È possibile specificare l'interfaccia di gestione FTD:



Poiché l'interfaccia di gestione può essere configurata anche per il protocollo SNMP, la pagina mostra questo messaggio di avviso:

La configurazione SNMP della piattaforma del dispositivo in questa pagina è disabilitata se le impostazioni SNMP sono configurate con l'interfaccia di gestione dei dispositivi tramite **Dispositivi > Impostazioni piattaforma (difesa dalle minacce) > SNMP > Host**.

Configurazione di FXOS SNMPv3

Aprire l'interfaccia utente di FMC e selezionare **Scegli dispositivi > Gestione dispositivi**. Scegliere il dispositivo e selezionare **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 ? X

Hostname:* 10.48.26.190 +

Community String:*

Port:* 163 (1 - 65535)

SNMP Version: V3

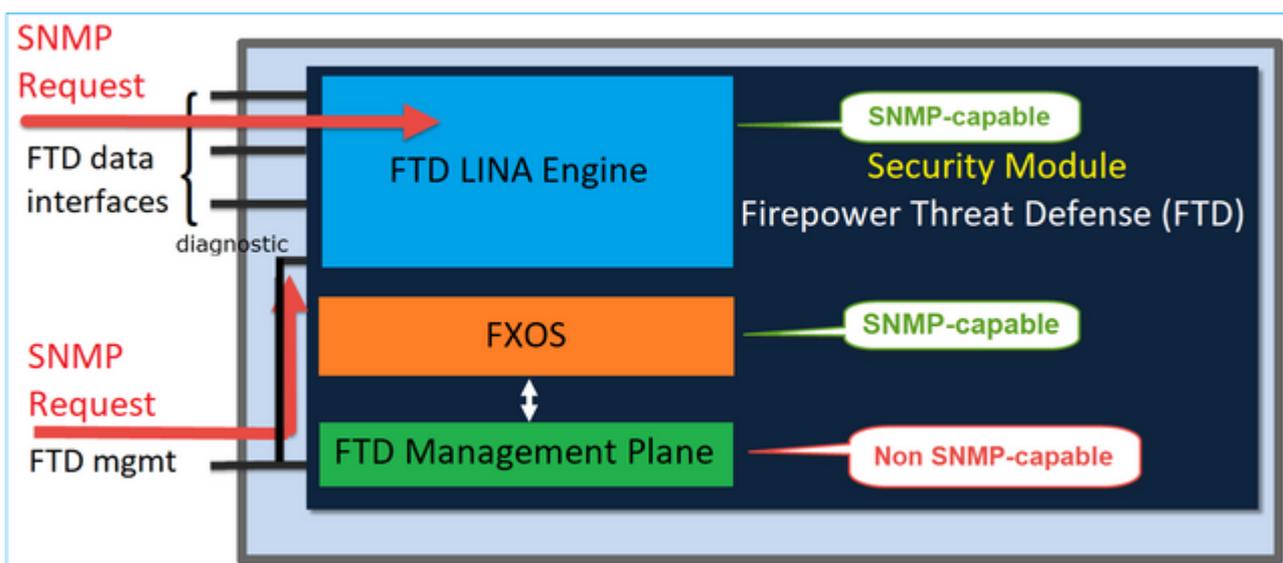
Type: TRAPS

Privilege: PRIV

OK Cancel

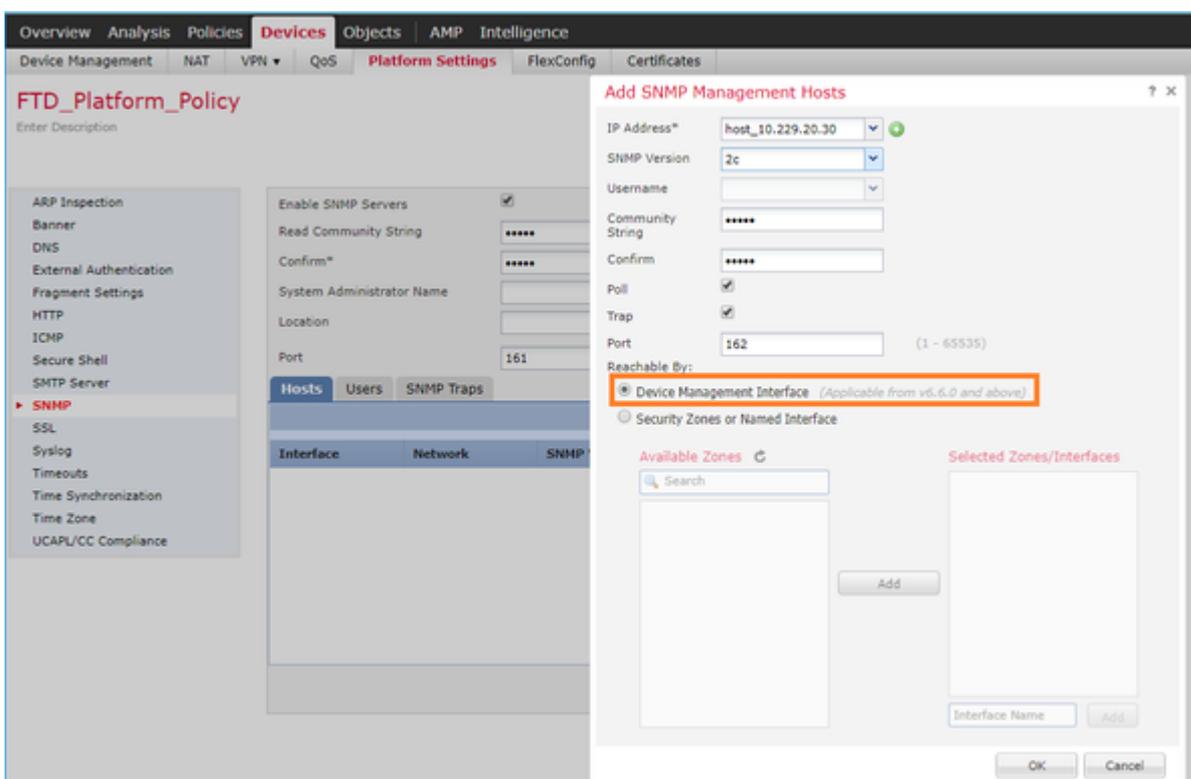
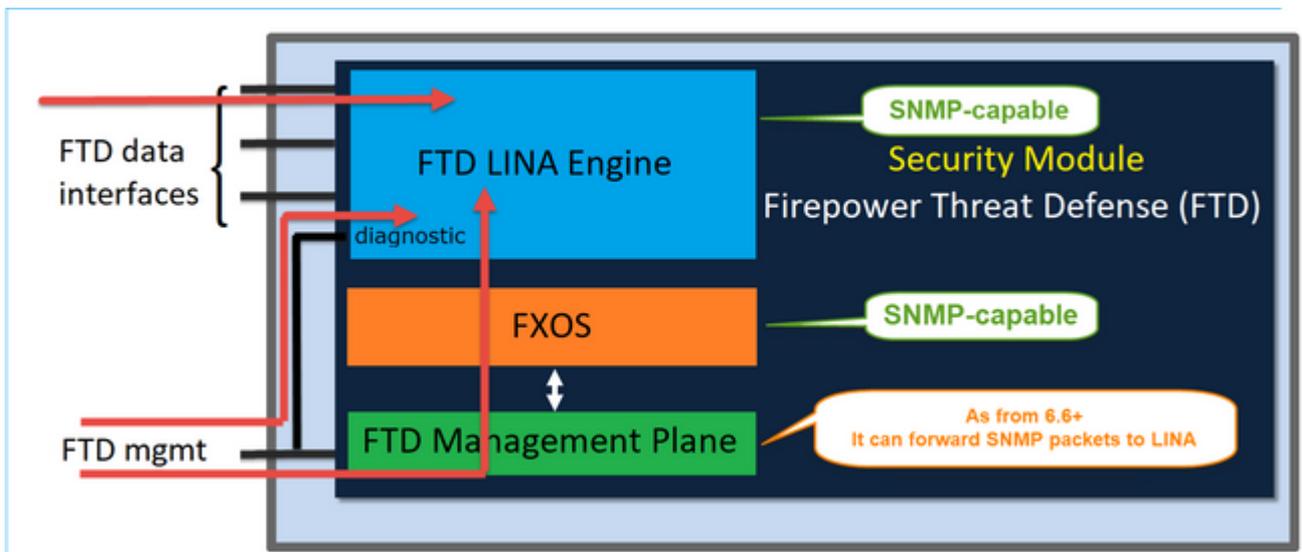
FTD (LINA) SNMP sulle appliance FPR2100

- Sulle release precedenti alla 6.6, la configurazione di LINA FTD SNMP sulle appliance FP1xxx/FP21xx è identica alla configurazione di FTD sulle appliance Firepower 4100 o 9300.



Release FTD successive alla 6.6

- Nelle release successive alla 6.6, è possibile usare anche l'interfaccia di gestione FTD per effettuare il polling e richiamare le trap di LINA.



Se si seleziona la nuova interfaccia di gestione:

- LINA SNMP è disponibile sull'interfaccia di gestione.
- In **Devices > Device Management** (Dispositivi > Gestione dispositivi), la scheda **SNMP** è disabilitata e non è più necessaria. Viene visualizzato un messaggio di avviso. La scheda dei dispositivi SNMP è visibile solo sulle piattaforme 2100/1100. Questa pagina non esiste sulle piattaforme FPR9300/FPR4100 e FTD55xx.

Terminata la configurazione, sull'interfaccia di gestione FTD viene visualizzato un messaggio informativo combinato su polling e trap del protocollo SNMP di LINA e FXOS (appliances FP1xxx/FP2xxx).

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**

ℹ 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				

La funzione di gestione SNMP Single IP è supportata a partire dalla versione 6.6 su tutte le piattaforme FTD:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 con FTD
- FTDv

Per ulteriori dettagli, fare clic su [Configure SNMP for Threat Defense \(Configura SNMP per Threat Defense\)](#).

Verifica

Verifica di FXOS SNMP sulle appliance FPR4100/FPR9300

Verifiche di FXOS SNMPv2c

Verifica della configurazione dalla CLI:

```
<#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      cisco456  V2c     Noauth      Traps
```

Nella modalità FXOS:

```
<#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
```

Verifiche aggiuntive:

```
<#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
...

```

Test delle richieste SNMP.

Eseguire una richiesta SNMP da un host valido.

Verifica della generazione delle trap.

Per verificare che le trap SNMP siano generate e inviate agli host definiti, è possibile usare lo strumento EthAnalyzer per indurre un'instabilità sull'interfaccia:

```
<#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
```

Avviso: un flap nell'interfaccia può causare un'interruzione del traffico. Eseguire questo test solo in un ambiente di laboratorio o durante un intervento di manutenzione.

Verifiche di FXOS SNMPv3

Passaggio 1. Apri **Impostazioni piattaforma** interfaccia utente FCM > **SNMP** > **Utente** mostra se è stata configurata una password e una password per la privacy:

The screenshot shows a configuration window titled "Edit user1". It contains the following fields and values:

- Name: user1
- Auth Type: SHA
- Use AES-128:
- Password: [Redacted] Set:Yes
- Confirm Password: [Redacted]
- Privacy Password: [Redacted] Set:Yes
- Confirm Privacy Password: [Redacted]

At the bottom of the window are "OK" and "Cancel" buttons.

Passaggio 2. Dalla CLI è possibile verificare la configurazione SNMP in Scope **Monitoring**:

```
<#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
```

Passaggio 3. In modalità FXOS è possibile espandere la configurazione SNMP e i dettagli:

```
<#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
-----
```

Test delle richieste SNMP.

È possibile verificare la configurazione ed eseguire una richiesta SNMP da qualsiasi dispositivo con funzionalità SNMP.

Per controllare come viene elaborata la richiesta SNMP, è possibile usare il debug SNMP:

```
<#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.10.10.1.1.10.10.10.1 =
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.10.10.1.2.10.10.10.2.83886080 = STRING: "mg
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.000000
```

Attenzione: il debug può influire sulle prestazioni del dispositivo.

Verifica di FXOS SNMP sulle appliance FPR2100

Verifiche di FXOS SNMPv2

Controllare la configurazione dalla CLI:

```
<#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
```

Verifica del comportamento SNMP.

È possibile verificare di poter eseguire il polling di FXOS e inviare una richiesta SNMP da un host o da qualsiasi dispositivo con funzionalità SNMP.

Usare il comando **capture-traffic** per verificare la richiesta SNMP e la risposta:

```
<#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.ifTable
```

```
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
```

Verifiche di FXOS SNMPv3

Controllare la configurazione dalla CLI:

```
<#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

Verifica del comportamento SNMP.

Inviare una richiesta SNMP per verificare che sia possibile eseguire il polling di FXOS.

Inoltre, è possibile acquisire la richiesta:

<#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
```

Verifica di FTD SNMP

Per verificare la configurazione di FTD LINA SNMP:

```
<#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 *****
```

Nelle release FTD successive alla 6.6, è possibile configurare e usare l'interfaccia di gestione FTD per SNMP:

```
<#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
```

Ulteriore verifica:

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

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

Dalla CLI del server SNMP eseguire il comando 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 Versio
```

```
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
```

```
...
```

Verifica delle statistiche del traffico SNMP.

```
<#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
```

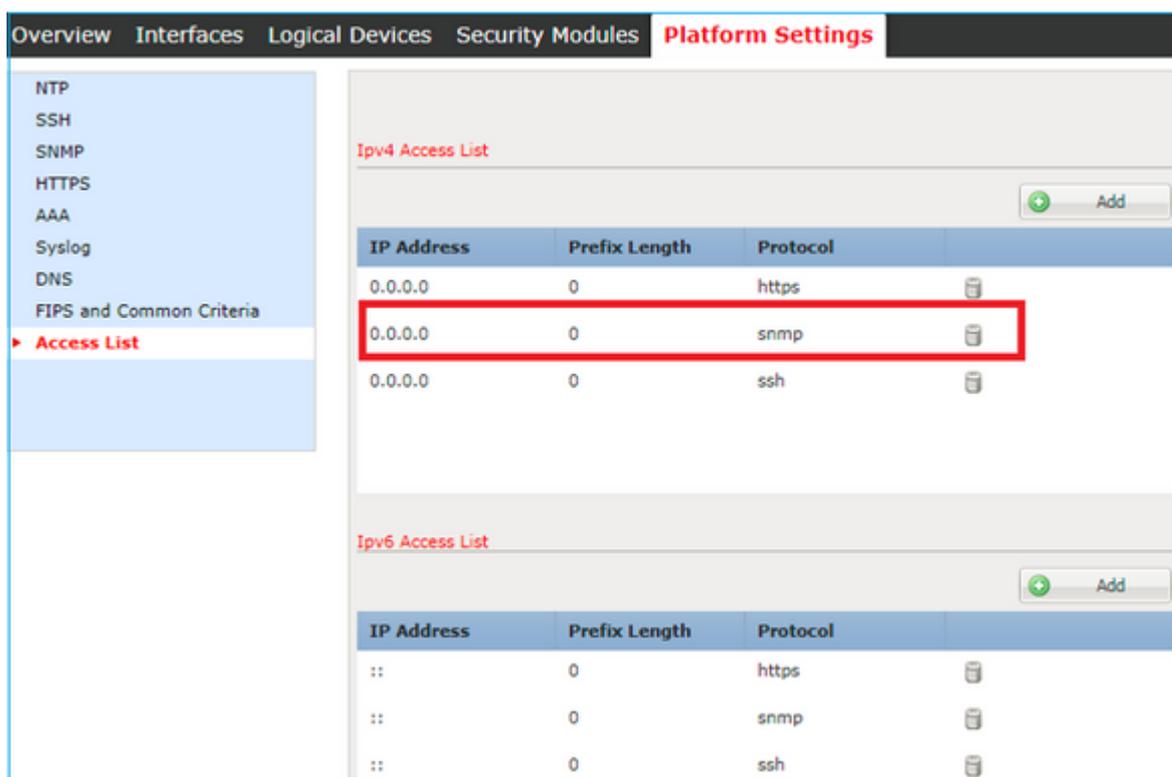
```
0 Bad values errors
```

```
0 General errors
```

Autorizzazione del traffico SNMP diretto a FXOS sulle appliance FPR4100/FPR9300

La configurazione di FXOS sulle appliance FPR4100/9300 può limitare l'accesso SNMP in base all'indirizzo IP di origine. La sezione di configurazione dell'elenco degli accessi definisce le reti e gli host che possono raggiungere il dispositivo tramite protocollo SSH, HTTPS o SNMP. Verificare quindi che le query SNMP provenienti dal server SNMP siano autorizzate.

Configurazione dell'elenco degli accessi globale dalla GUI



The screenshot displays the 'Platform Settings' configuration page in the FXOS GUI. The left sidebar shows the navigation 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 access list entries.

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	

Configurazione dell'elenco degli accessi globale dalla CLI

```
<#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
```

Verifica

<#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

Uso di OID Object Navigator

[Cisco SNMP Object Navigator](#) è uno strumento online che permette di convertire i diversi OID e ottenere una breve descrizione.

Tools & Resources

SNMP Object Navigator

HOME
SUPPORT
TOOLS & RESOURCES
SNMP Object Navigator

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	CISCO-PROCESS-MIB ; - View Supporting Images
Description	A table of overall CPU statistics.

Usare il comando **show snmp-server oid** dalla CLI di FTD LINA per recuperare l'intero elenco di LINA OID di cui è possibile eseguire il polling.

<#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#
```

Nota: il comando è nascosto.

Risoluzione dei problemi

Queste sono le cause di errore SNMP più comuni rilevate da Cisco TAC:

1. Impossibile eseguire il polling di FTD LINA SNMP
2. Impossibile eseguire il polling di FXOS SNMP
3. Quali sono i valori SNMP OID da usare?
4. Impossibile richiamare le trap SNMP
5. Impossibile monitorare FMC con il protocollo SNMP
6. Impossibile configurare il protocollo SNMP
7. Configurazione di SNMP su Firepower Device Manager

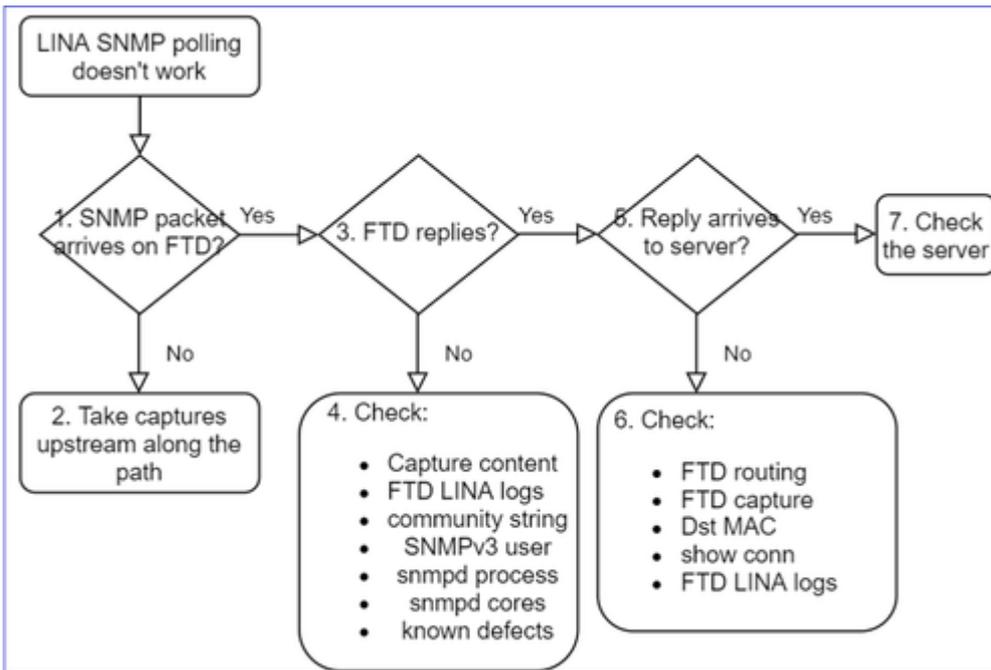
Impossibile eseguire il polling di FTD LINA SNMP

Descrizione del problema (situazioni reali gestite da Cisco TAC):

- "Impossibile recuperare i dati su SNMP."
- "Impossibile eseguire il polling del dispositivo su SNMPv2."
- "SNMP non funziona. Vogliamo monitorare il firewall con SNMP, ma dopo la configurazione, si verificano dei problemi."
- "Abbiamo due sistemi di monitoraggio che non sono in grado di monitorare FTD tramite SNMP v2c o 3."
- "Il comando SNMP walk non funziona sul firewall."

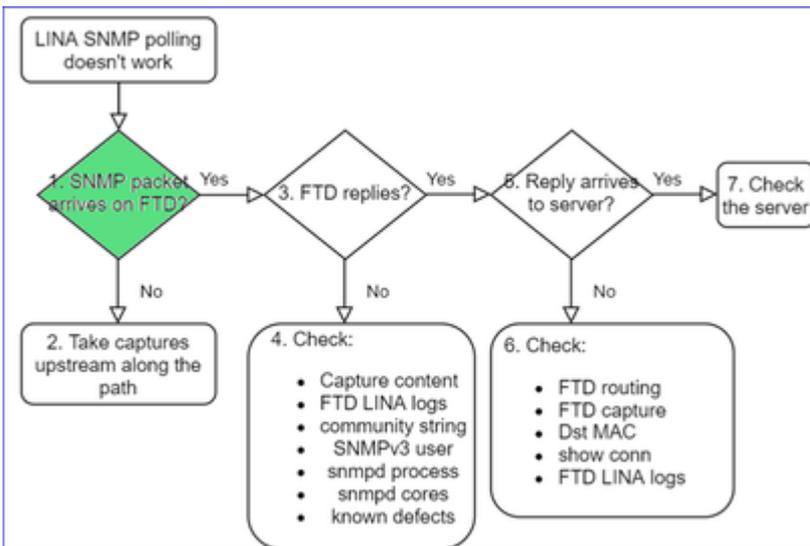
Suggerimenti per la risoluzione dei problemi

Questo è il processo consigliato per risolvere i problemi relativi al polling SNMP di LINA:



Analisi approfondita

1. Il pacchetto SNMP arriva su FTD?



- Abilitare le acquisizioni per verificare l'arrivo del pacchetto SNMP.

L'interfaccia di gestione SNMP su FTD (versione successiva alla 6.6) utilizza la parola chiave management:

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

Sulle interfacce dati FTD, il protocollo SNMP usa il nome dell'interfaccia:

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

Acquisire il traffico sull'interfaccia di gestione FTD:

```
<#root>
```

```
>
```

```
capture-traffic
```

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

```
0 - management1
```

```
1 - management0
```

```
2 - Global
```

```
Selection?
```

```
1
```

Acquisire il traffico sull'interfaccia dati FTD:

```
<#root>
```

```
firepower#
```

```
capture SNMP interface net201 trace match udp any any eq 161
```

Traccia del pacchetto sull'interfaccia dati FTD (scenario funzionale - release precedenti alla 6.6/9.14.1):

```
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)

Traccia del pacchetto sull'interfaccia dati FTD (scenario non funzionale - release successive alla 6.6/9.14.1):

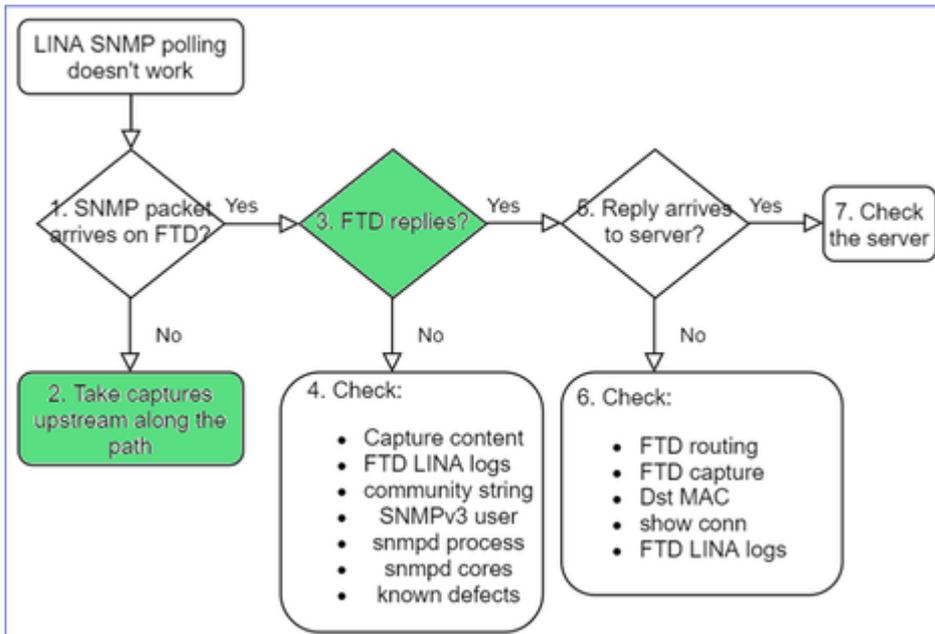
```
firepower# show capture SNMP packet-number 1 trace

  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. Nel caso in cui i pacchetti SNMP non vengano visualizzati nelle acquisizioni in entrata FTD:

- Acquisire il traffico sul percorso upstream.
- Verificare che il server SNMP usi l'indirizzo IP corretto dell'FTD.
- Iniziare dalla porta dello switch situata di fronte all'interfaccia FTD e spostarsi upstream.



3. Il protocollo FTD SNMP risponde?

Per verificare se FTD risponde, controllare:

1. Acquisizione del traffico FTD in uscita (interfaccia LINA o di gestione)

Controllare se sono presenti pacchetti SNMP con porta di origine 161:

```
<#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

```

Nelle versioni successive alla 6.6/9.14.1, è disponibile un punto di acquisizione aggiuntivo: Cattura sull'interfaccia del nastro NLP. L'indirizzo IP NATed è compreso nell'intervallo 162.254.x.x:

```
<#root>
```

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

```
sudo tcpdump -i tap_nlp
```

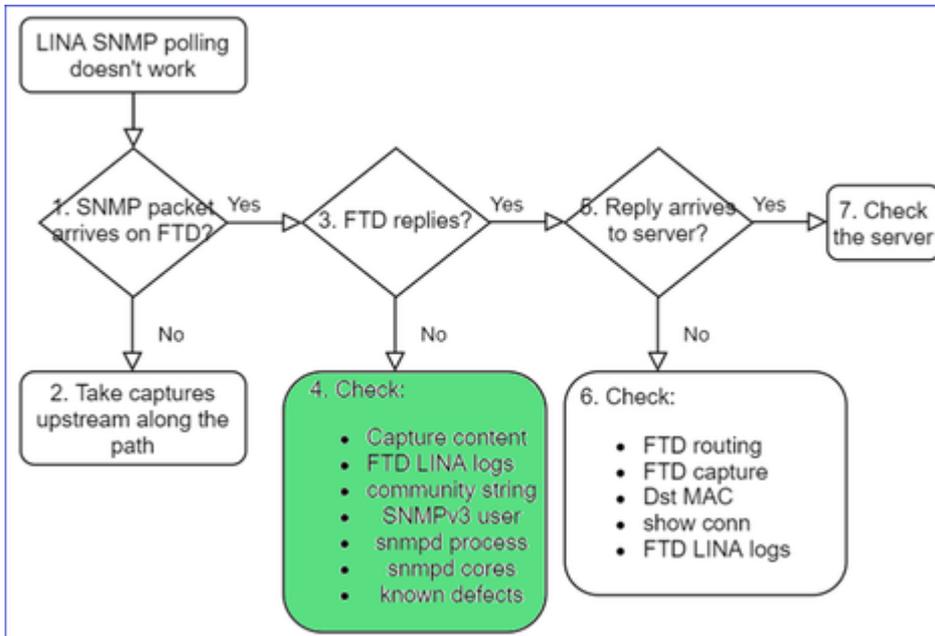
```
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```

16:46:28.372018 IP 192.168.2.100.49008 > 169.254.1.2.snmp: C="Cisc0123" GetNextRequest(28) E:cisco.9.1
16:46:28.372498 IP 192.168.1.2.snmp > 192.168.2.100.49008: C="Cisc0123" GetResponse(35) E:cisco.9.109

```

4. Controlli supplementari



r. Per i dispositivi Firepower 4100/9300, controllare la [tabella di compatibilità FXOS](#).

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
2.13(0.198)+ Note 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	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 4145 Firepower 4125 Firepower 4115	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(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)
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x)
2.12(0.31)+ Note 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	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 4145 Firepower 4125 Firepower 4115	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.13(1) 9.12(x)
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.12(x) 9.10(x) 9.9(x) 9.8(x)
2.11(1.154)+ Note 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	9.17(x) (recommended) 9.16(x) 9.15(1) 9.14(x)

b. Controllare le statistiche snmp-server di FTD LINA:

```
<#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
â€¦
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. Tabella delle connessioni LINA FTD

Questo controllo è molto utile nel caso in cui non si vedano i pacchetti nella cattura sull'interfaccia in entrata FTD. Questa è una verifica valida solo per il protocollo SNMP sull'interfaccia dati. Se il protocollo SNMP è su un'interfaccia di gestione (post-6.6/9.14.1), non viene creata alcuna connessione.

```
<#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. syslog FTD LINA

Anche questa è una verifica valida solo per il protocollo SNMP sull'interfaccia dati. Se il protocollo SNMP configurato è sull'interfaccia di gestione, non vengono creati log:

```
<#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 (192.0.2.100)

e. Controllare se l'FTD elimina i pacchetti SNMP a causa di un indirizzo IP di origine dell'host errato.

```
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
```

No UN-NAT phase!

```
firepower# show run snmp-server
snmp-server host net201 192.168.22.100
```

```
firepower# show asp table classify interface net201 dom
Input Table
in id=0x14f65b193b30, priority=501, domain=permit, den
hits=8, user_data=0x0, cs_id=0x0, use_real_addr
src ip/id=192.168.22.100, mask=255.255.255.255,
dst ip/id=169.254.1.2, mask=255.255.255.255, po
input_ifc=net201(vrfid:0), output_ifc=any
```

f. Credenziali errate (stringa della community SNMP)

Tra i contenuti acquisiti, è possibile verificare i valori della stringa della community (SNMP v1 e 2c):

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
v Simple Network Management Protocol
  version: v2c (1)
  community: cisco123
  data: get-next-request (1)
```

g. Configurazione errata (ad esempio, versione SNMP o stringa della community)

Esistono diversi modi per verificare la configurazione SNMP del dispositivo e le stringhe della community:

<#root>

firepower#

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

```
snmp-server host net201 192.168.2.100 community cISC0123 version 2c
```

Un metodo alternativo:

<#root>

firepower#

```
debug menu netsnmp 4
```

h. Eliminazioni di ASP in FTD LINA/ASA

Questo controllo è utile per verificare se i pacchetti SNMP vengono eliminati dall'FTD. Anzitutto, azzerare i contatori (clear asp drop), quindi verificare:

```
<#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. Acquisizioni ASP

Le acquisizioni di ASP permettono di visualizzare i pacchetti eliminati (ad esempio, ACL o adiacenze):

```
<#root>
```

```
firepower#
```

```
capture ASP type asp-drop all
```

Verificare i contenuti acquisiti:

```
<#root>
```

```
firepower#
```

```
show capture
```

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

j. Core SNMP (traceback) - Metodo di verifica 1

Questo controllo è utile se si sospettano problemi di stabilità del sistema:

```
<#root>
firepower#
show disk0: | i core

13 52286547   Jun 11 2021 12:25:16  coredumpfsys/core.snmpd.6208.1626214134.gz
```

Core SNMP (traceback) - Metodo di verifica 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
```

Se viene visualizzato un file core SNMP, raccogliere questi elementi e contattare Cisco TAC:

- File FTD TS (o ASA show tech)
- snmpd core files

Debug SNMP (sono comandi nascosti e disponibili solo nelle versioni più recenti):

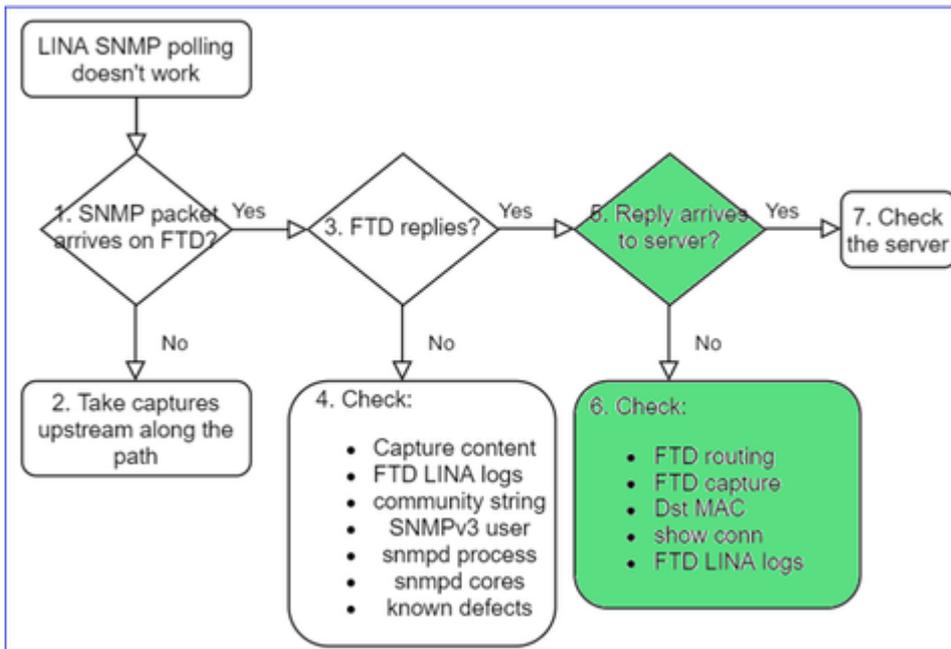
```
<#root>
firepower#
debug snmp trace [255]

firepower#
debug snmp verbose [255]

firepower#
debug snmp error [255]

firepower#
debug snmp packet [255]
```

La risposta SNMP del firewall arriva al server?



Se l'FTD risponde, ma la risposta non raggiunge il server, controllare:

r. Routing FTD

Per il routing dell'interfaccia di gestione FTD:

```

<#root>
>
show network
  
```

Per il routing dell'interfaccia dati FTD LINA:

```

<#root>
firepower#
show route
  
```

b. Verifica dell'indirizzo MAC di destinazione

Verifica dell'indirizzo MAC di destinazione sull'interfaccia di gestione FTD:

```

<#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: 10.62.148.19

Verifica dell'indirizzo MAC di destinazione sull'interfaccia dati FTD LINA:

<#root>

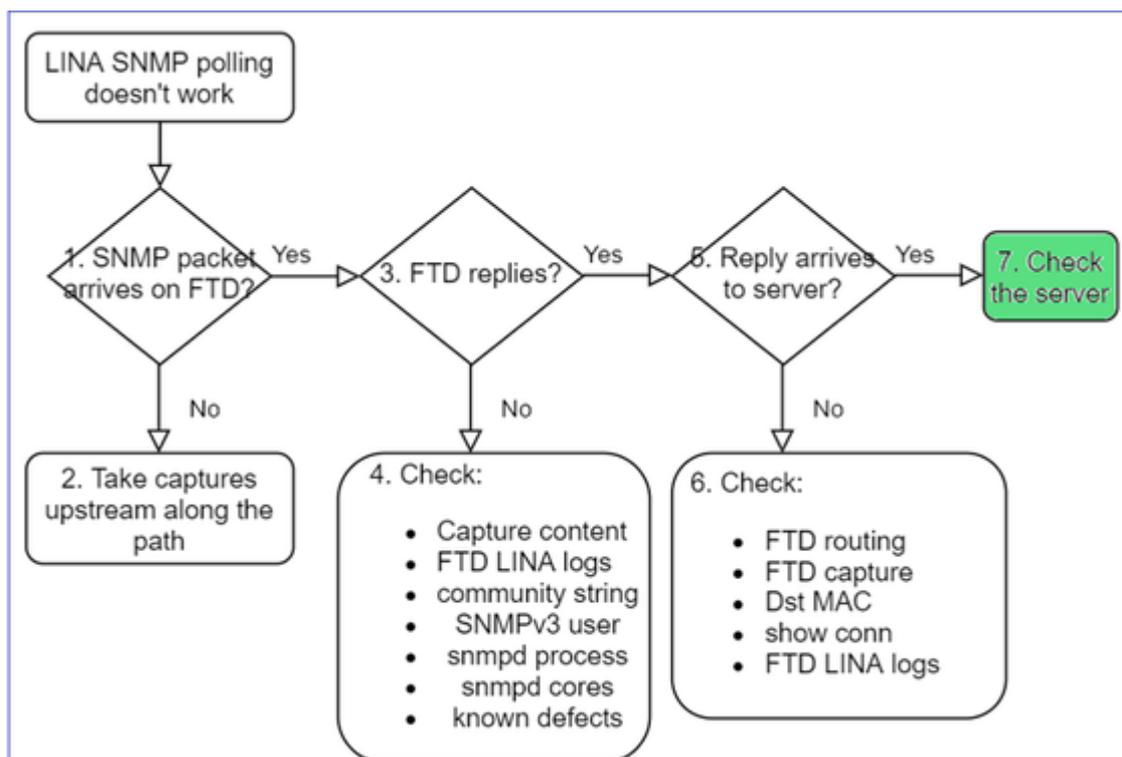
firepower#

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, i

c. Controllare i dispositivi lungo il percorso che probabilmente elimina o blocca i pacchetti SNMP.

Controllo del server SNMP



- r. Controllare il contenuto dell'acquisizione per verificare le impostazioni.
- b. Controllare la configurazione del server.
- c. Provare a modificare il nome della community SNMP, ad esempio senza caratteri speciali.

È possibile utilizzare un host finale o persino il CCP per verificare il sondaggio, purché vengano soddisfatte le due condizioni seguenti:

1. Connettività SNMP attiva.
2. Indirizzo IP di origine autorizzato a eseguire il polling del dispositivo.

```
<#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
```

Considerazioni sul polling di SNMPv3

- Licenza: SNMPv3 richiede una licenza di crittografia avanzata. Verificare di aver abilitato la funzionalità Export Controlled Functionality sul portale Smart Licensing
- Per risolvere il problema, provare con un nuovo utente/credenziali
- Se si utilizza la crittografia, è possibile decrittografare il traffico SNMPv3 e controllare il payload come descritto in: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>
- Prendere in considerazione AES128 per la crittografia in caso il software sia interessato dai seguenti bug:
- ID bug Cisco [CSCvy27283](#)

Il polling ASA/FTD SNMPv3 può non riuscire utilizzando gli algoritmi di privacy AES192/AES256

ID bug Cisco [CSCvx45604](#) La marcia di Snmpv3 non riesce sull'utente con auth sha e priv aes 192

Nota: se SNMPv3 non riesce a causa di una mancata corrispondenza degli algoritmi, il comando show output e i log non mostrano alcun elemento ovvio

```
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'

Considerazioni sul polling SNMPv3 - Case study

1. SNMPv3 snmpwalk - Scenario funzionale

<#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 9.0
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2315

Nell'acquisizione (snmpwalk), è presente una replica per ciascun pacchetto:

```
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
```

Il file di acquisizione non mostra nulla di insolito:

```

Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  > 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
  > msgAuthenticationParameters: 79ee0d463313558f4529954f
    > [Authentication: OK]
      > [Expert Info (Chat/Checksum): SNMP Authentication OK]
        [SNMP Authentication OK]
        [Severity level: Chat]
        [Group: Checksum]
      msgPrivacyParameters: 714e78d6bc292c88

```

2. SNMPv3 snmpwalk - Errore di crittografia

Suggerimento 1: Timeout:

```
<#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

Suggerimento 2: sono presenti molte richieste e 1 risposta:

```

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

Suggerimento 3: errore di decrittografia di Wireshark:

```
> 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: 0000000197eae1a
    > 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]
```

Caso n. 4. Verificare nel file ma_ctx2000.log la presenza di messaggi di "errore durante l'analisi di ScopedPDU":

```
<#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
```

L'errore durante l'analisi di ScopedPDU è un indizio evidente di un errore di crittografia. Il file ma_ctx2000.log mostra gli eventi solo per SNMPv3.

3. SNMPv3 snmpwalk è "Errore di autenticazione"

Suggerimento 1: errore di autenticazione

```
<#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)
```

Suggerimento 2: ci sono molte richieste e molte risposte

```
firepower# show capture SNMP
4 packets captured
1: 23:25:28.468847      802.1Q vlan#201 P0 192.168.21.100.34348 > 192.168.21.50.161: udp 64
2: 23:25:28.469412      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.34348: udp 132
3: 23:25:28.474386      802.1Q vlan#201 P0 192.168.21.100.34348 > 192.168.21.50.161: udp 157
4: 23:25:28.475561      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.34348: udp 137
```

Suggerimento n. 3: Wireshark con pacchetto non valido

```
> 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]
```

Caso n. 4. Controllare il file ma_ctx2000.log per i messaggi 'Autenticazione non riuscita':

```
<#root>
```

```
>
```

```
expert
```

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

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

```
Authentication failed for Cisco123
```

```
Authentication failed for Cisco123
```

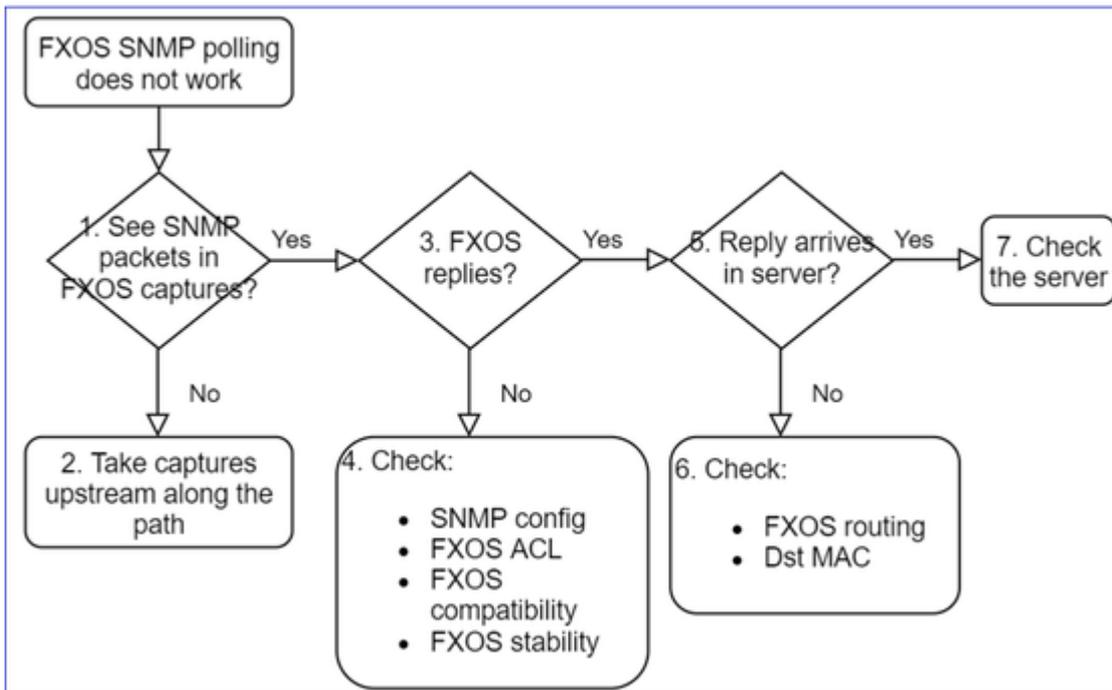
Impossibile eseguire il polling di FXOS SNMP

Descrizione del problema (situazioni reali gestite da Cisco TAC):

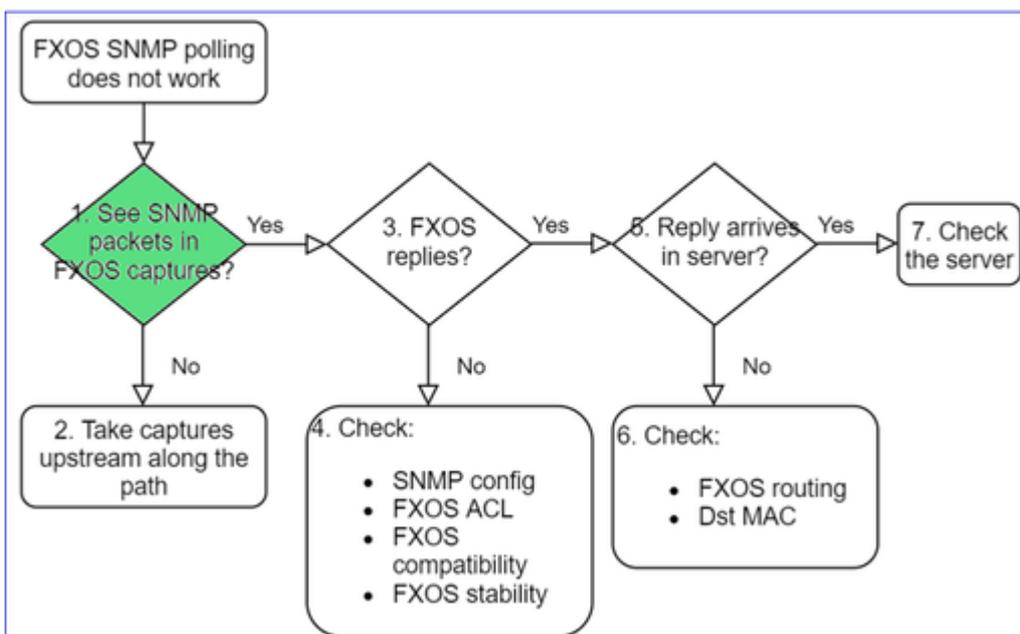
- "Il protocollo SNMP restituisce una versione errata di FXOS. Quando si esegue il polling con il protocollo SNMP per la versione di FXOS, è difficile interpretare l'output."
- "Impossibile impostare la stringa della community SNMP su FXOS FTD4115."
- "Dopo un aggiornamento FXOS dalla versione 2.8 alla versione 2.9 sul firewall di standby, si ottiene un timeout quando si tenta di ricevere informazioni tramite SNMP."
- "Il comando snmpwalk non restituisce risultati su 9300 FXOS ma funziona sulle appliance 4140 FXOS con medesima versione. Il problema non riguarda la raggiungibilità e la stringa della community."
- "Vorremmo aggiungere 25 server SNMP sulle appliance FPR4K FXOS, ma l'operazione non riesce."

Procedura di risoluzione consigliata

Questo è il processo per risolvere i problemi relativi al polling SNMP di FXOS:



1. Le acquisizioni FXOS restituiscono pacchetti SNMP?



FPR1xxx/21xx

- Sul modello FPR1xxx/21xx non è disponibile il software di gestione dello chassis (modalità accessorio).
- È possibile eseguire il polling del software FXOS dall'interfaccia di gestione.

<#root>

>

capture-traffic

Please choose domain to capture traffic from:

- 0 - management
- 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

- Sulle appliance Firepower 41xx/93xx, usare lo strumento EthAnalyzer dalla CLI per acquisire il traffico sullo chassis:

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
firepower(fxos)#
```

```
ethanalyzer 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
```

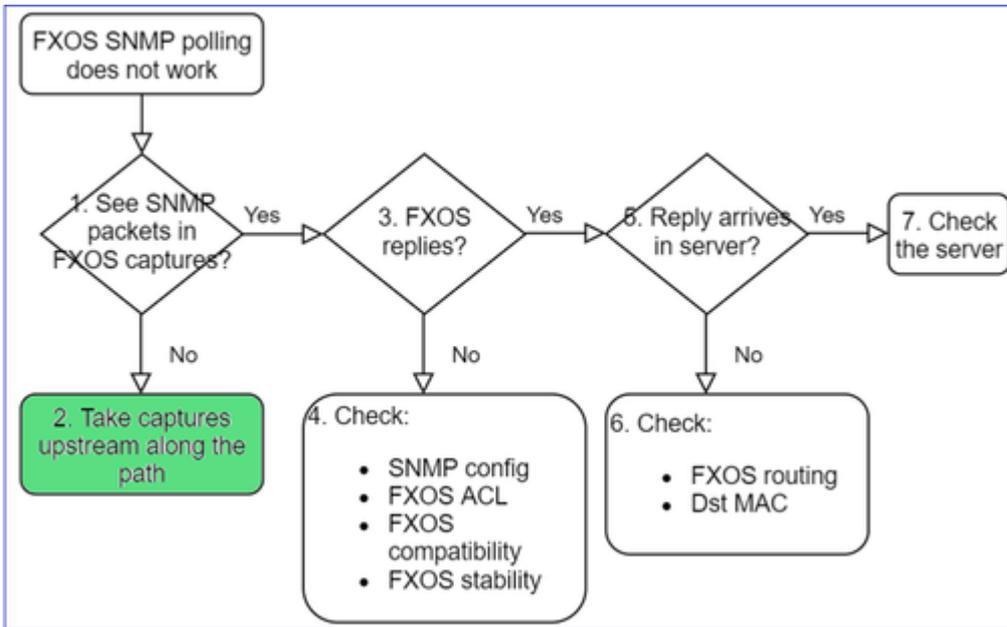
```
1
```

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

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

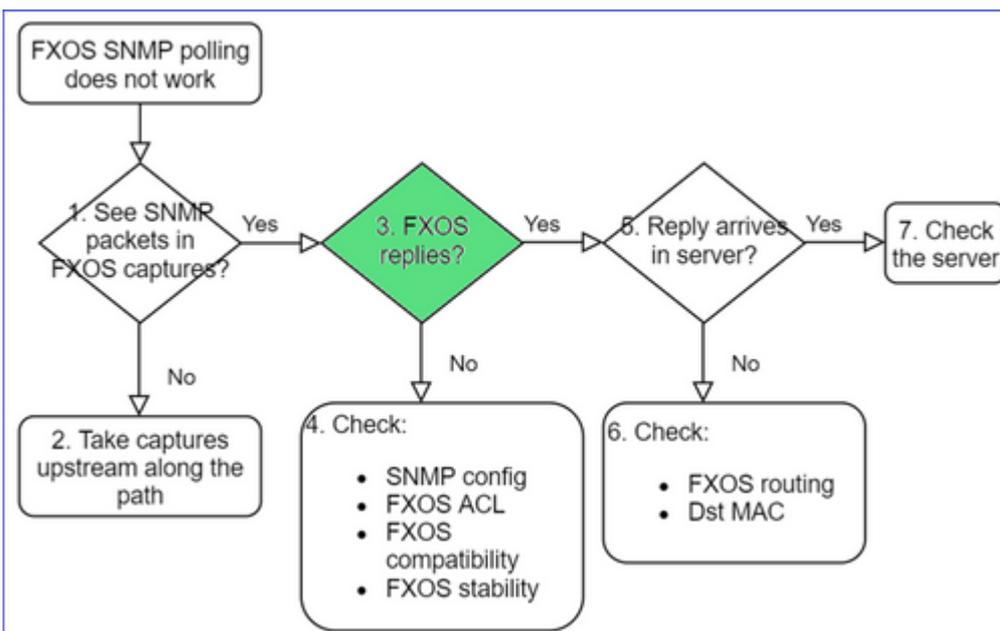
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. Le acquisizioni FXOS non restituiscono pacchetti?



- Acquisire il traffico sul percorso upstream

3. FXOS risponde?



- Scenario funzionale:

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.

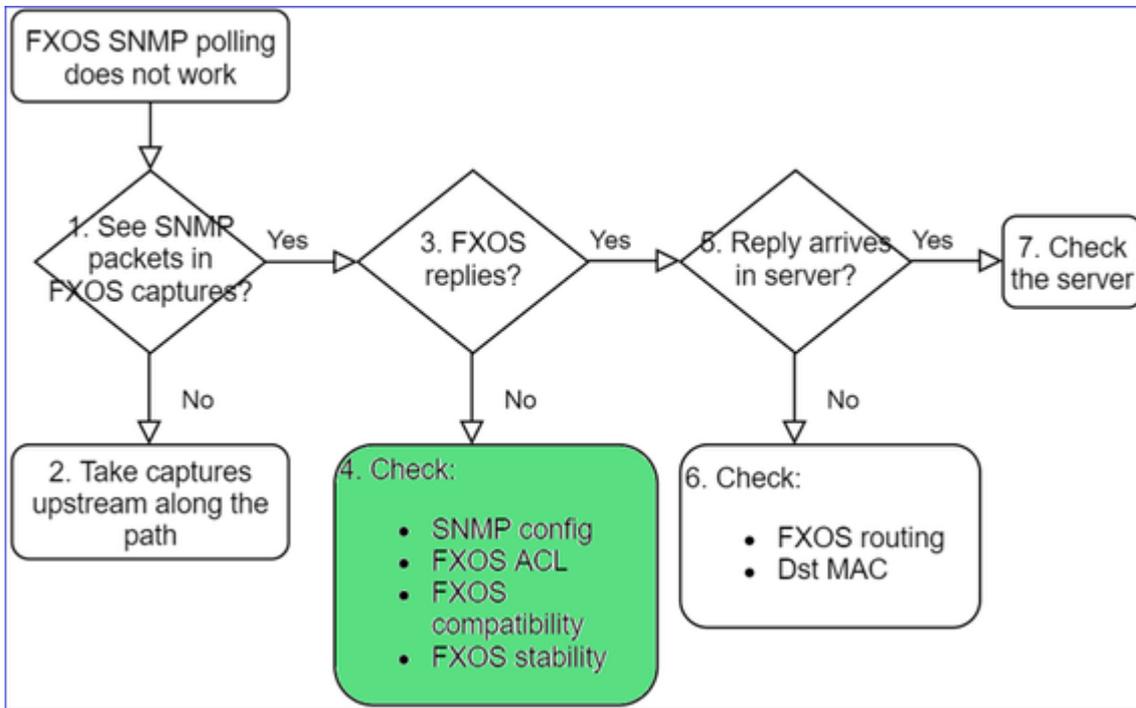
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

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 non risponde



Controlli aggiuntivi

- Verificare la configurazione del protocollo SNMP (dall'interfaccia utente o dalla CLI):

```
<#root>
```

```
firepower#
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

- Prestare attenzione ai caratteri speciali (ad esempio "\$"):

```
<#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		

- Sul protocollo SNMP v3, usare il comando show snmp-user [detail]
- Verificare la compatibilità FXOS

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id_59069

4. Nel caso in cui FXOS non risponda

Verificare i contatori FXOS SNMP:

```
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
```

The diagram shows four text boxes on the right with arrows pointing to specific lines in the terminal output on the left:

- Total requests (polling)** points to `2243 SNMP packets input`
- Bad community requests (v2c)** points to `28 Unknown community name`
- Total replies** points to `3483 SNMP packets output`
- Traps generated** points to `1296 Out Traps PDU`

- Verificare l'elenco di controllo degli accessi, o ACL (Access Control List), di FXOS. Valido solo sulle piattaforme FPR41xx/9300.

Se il traffico è bloccato dall'ACL FXOS, vengono visualizzate le richieste, ma non le risposte:

```
<#root>
```

```
firepower(fxos)#
```

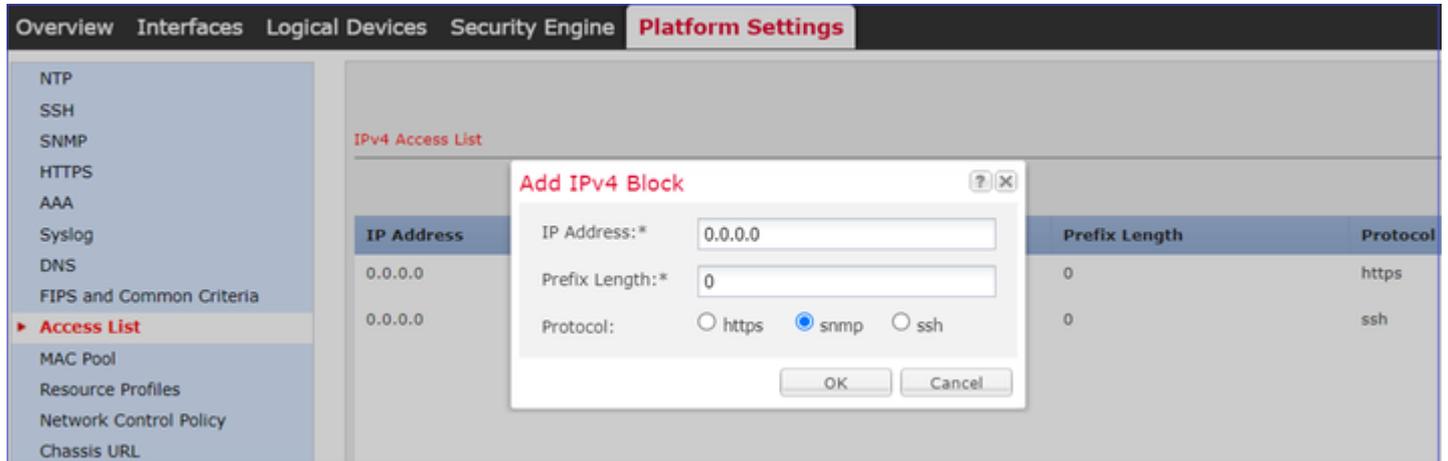
```
ethalyzer local interface mgmt capture-filter
```

```
"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 â†’ 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 â†’ 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 â†’ 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1
```

È possibile verificare l'ACL di FXOS dall'interfaccia utente (UI):



È possibile verificare l'ACL di FXOS anche dalla CLI:

```
<#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
```

- Debug SNMP (solo pacchetti). Valido solo sulle piattaforme 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) - Questo output di debug è molto dettagliato.

```
<#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
```

- Controllare se sono presenti errori FXOS relativi al protocollo SNMP:

```
<#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
```

- Verificare se sono presenti core snmpd:

Sulle appliance FPR41xx/FPR9300:

```
<#root>
firepower#
connect local-mgmt

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

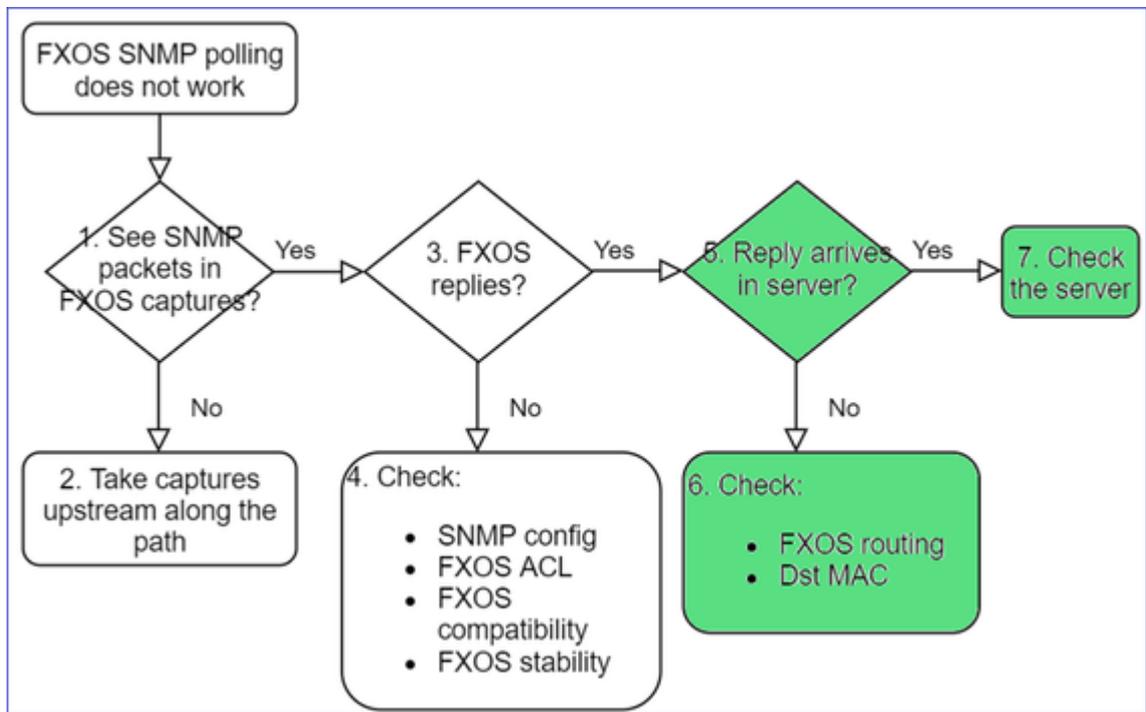
```
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz
```

Sulle appliance FPR1xxx/21xx:

```
<#root>  
firepower(local-mgmt)#  
dir cores_fxos
```

Se sono presenti core snmpd, recuperare i core con il bundle di risoluzione dei problemi FXOS e contattare Cisco TAC.

5. La risposta del protocollo SNMP arriva al server SNMP?



- Controllare il routing di FXOS

Questo output proviene dalle appliance FPR41xx/9300:

```
<#root>  
firepower#  
show fabric-interconnect
```

Fabric Interconnect:

ID	00B IP Addr	00B Gateway	00B Netmask	00B IPv6 Address	00B IPv6 Gateway	Prefix	Operab
A	192.168.2.37	192.168.2.1	10.255.255.128 ::	::		64	Operable

- Acquisire il traffico, esportare il file pcap e controllare l'indirizzo MAC di destinazione della risposta.
- Infine, controllare il server SNMP (acquisizioni, configurazione, applicazione e così via).

Quali sono i valori SNMP OID da usare?

Descrizione del problema (situazioni reali gestite da Cisco TAC):

- "Vorremmo monitorare l'apparecchiatura Cisco Firepower. Quali sono gli SNMP OID per CPU, memoria e dischi di ciascun core?"
- "Esiste un OID che può essere usato per monitorare lo stato dell'alimentazione sul dispositivo ASA 5555?"
- "Vorremmo ottenere i dati SNMP OID dello chassis sulle appliance FPR 2K e FPR 4K."
- "Vogliamo eseguire il polling della cache ASA ARP."
- "Dobbiamo sapere il valore SNMP OID per il peer BGP inattivo."

Come richiamare i valori SNMP OID

Questi documenti forniscono informazioni sui valori SNMP OID sulle appliance Firepower:

- White paper sul monitoraggio del protocollo SNMP in Cisco Firepower Threat Defense (FTD):

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

- Guida di riferimento di Cisco Firepower 4100/9300 FXOS MIB:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b_FXOS_4100_9300_MIBRef.html

- Come cercare un OID specifico sulle piattaforme FXOS:

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

- Controllare gli SNMP OID dalla CLI (ASA/LINA)

```
<#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
```

- Per ulteriori informazioni sugli OID, consultare SNMP Object Navigator

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

- Su FXOS (41xx/9300), eseguire questi 2 comandi dalla CLI di FXOS:

```
<#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 ieee8021paeMIB
```

```
1.0.88010.1.1.1.1.1.2
```

```
...
```

Riferimento rapido degli OID comuni

Requisito	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)
Memoria (LINA)	1.3.6.1.4.1.9.9.221.1.1
Memoria (Linux/FMC)	1.3.6.1.1.4.1.2021.4
Informazioni HA	1.3.6.1.4.1.9.9.491.1.4.2
Informazioni sul cluster	1.3.6.1.4.1.9.9.491.1.8.1

Informazioni VPN	<p>Sessioni RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.1 (7.x)</p> <p>Utenti RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.3 (7.x)</p> <p>Numero di sessioni di picco RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.41 (7.x)</p> <p>Sessioni VPN da sito a sito: 1.3.6.1.4.1.9.9.392.1.3.29</p> <p>N. di sessioni VPN da sito a sito: 1.3.6.1.4.1.9.9.392.1.3.31</p> <p>- Suggerimento: firepower# show snmp-server oid i ike</p>
Stato BGP	ID bug Cisco ENH CSCux13512 :Aggiungere BGP MIB per il polling SNMP
FPR1K/2K ASA/ASAv Smart Licensing	ID bug Cisco ENH CSCv83590 : ASAv/ASA su FPR1k/2k: è necessario l'OID SNMP per tenere traccia dello stato di Smart Licensing
LINA SNMP OID per i port-channel a livello di FXOS	ID bug Cisco ENH CSCvu91544 :Supporto per LINA SNMP OID per le statistiche dell'interfaccia port-channel a livello di FXOS

FMC 7.3 Aggiunte (per FMC 1600/2600/4600 e successivi)

Requisito	OID
Trap stato ventola	<p>OID Trap: 1.3.6.1.4.1.9.9.17.2.0.6</p> <p>OID valore: 1.3.6.1.4.1.9.9.117.1.4.1.1.1.<indice></p> <p>0 - ventola non in funzione</p> <p>1 - la ventola è in funzione</p>
Trap temperatura CPU/PSU	<p>OID Trap: 1.3.6.1.4.1.9.9.91.2.0.1</p> <p>OID soglia: 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<indice>.1</p> <p>OID valore: 1.3.6.1.4.1.9.9.91.1.1.1.1.4.<indice></p>
Trap stato PSU	<p>OID Trap: 1.3.6.1.4.1.9.9.17.2.0.2</p> <p>OperStatus OID: 1.3.6.1.4.1.9.9.17.1.1.2.1.2.<indice></p> <p>OID AdminStatus: 1.3.6.1.4.1.9.9.17.1.1.2.1.1.<indice></p> <p>0 - presenza alimentatore non rilevata</p>

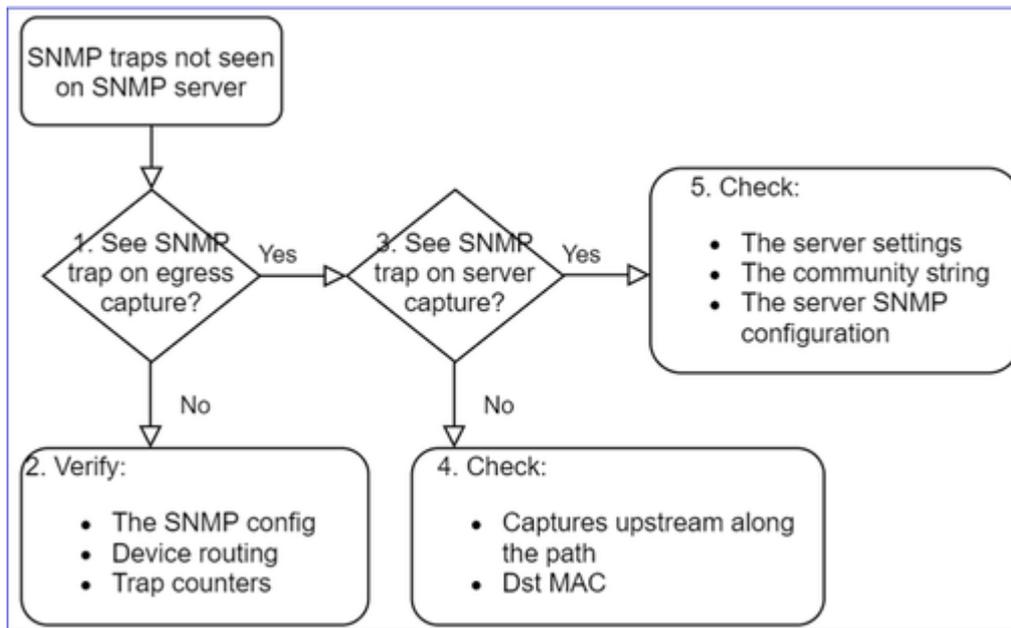
Impossibile richiamare le trap SNMP

Descrizione del problema (situazioni reali gestite da Cisco TAC):

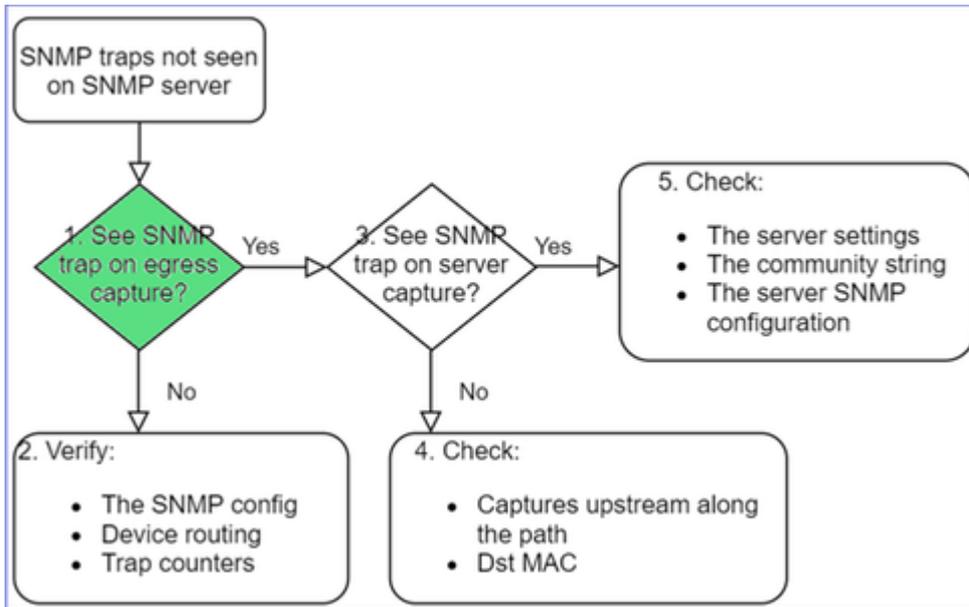
- "Il protocollo SNMPv3 di FTD non invia trap al server SNMP."
- "FMC e FTD non inviano messaggi trap SNMP."
- "Abbiamo configurato SNMP sul nostro FTD 4100 per FXOS e abbiamo provato a inviare trap con i protocolli SNMPv3 e SNMPv2, ma in entrambi i casi non è stato possibile."
- "Firepower SNMP non invia trap allo strumento di monitoraggio."
- "Il firewall FTD non invia trap SNMP a NMS."
- "Le trap del server SNMP non funzionano."
- "Abbiamo configurato SNMP sul nostro FTD 4100 per FXOS e abbiamo provato a inviare trap con i protocolli SNMPv3 e SNMPv2, ma in entrambi i casi non è stato possibile."

Procedura di risoluzione consigliata

Questo è il processo per la risoluzione dei problemi relativi alle trap SNMP di Firepower:



1. Sono presenti trap SNMP sulle acquisizioni del traffico in uscita?



Per acquisire le trap LINA/ASA sull'interfaccia di gestione:

```
<#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
```

Per acquisire le trap LINA/ASA sull'interfaccia dati:

```
<#root>
```

```
firepower#
```

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

Per acquisire le trap FXOS (41xx/9300):

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```

firepower(fxos)#
ethanalyzer 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 at 10.62.184.23 SNMP 160 snmpV2-trap 10.3.1.1.2.1.1.3.0
firepower(fxos)#
exit

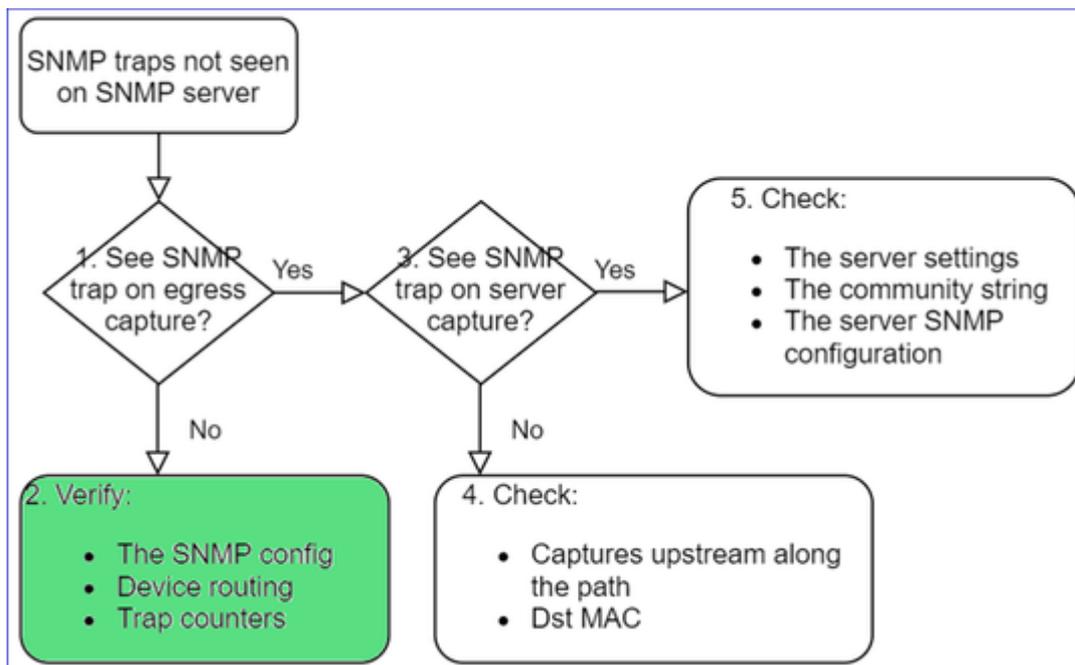
firepower#
connect local-mgmt

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. Se i pacchetti non vengono visualizzati sull'interfaccia di uscita



<#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

```

Configurazione delle trap FXOS SNMP:

```
<#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

Nota: su 1xxx/21xx queste impostazioni sono visibili solo nel caso di **Dispositivi > Gestione dispositivi > Configurazione SNMP!**

- Routing LINA/ASA delle trap sull'interfaccia di gestione:

```
<#root>
```

```
>
```

```
show network
```

- Routing LINA/ASA delle trap sull'interfaccia dati:

```
<#root>
```

```
firepower#
```

```
show route
```

- Routing FXOS (41xx/9300):

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- Contatori delle trap (LINA/ASA):

```
<#root>
```

firepower#

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

20 Trap PDUs

E FXOS:

<#root>

FP4145-1#

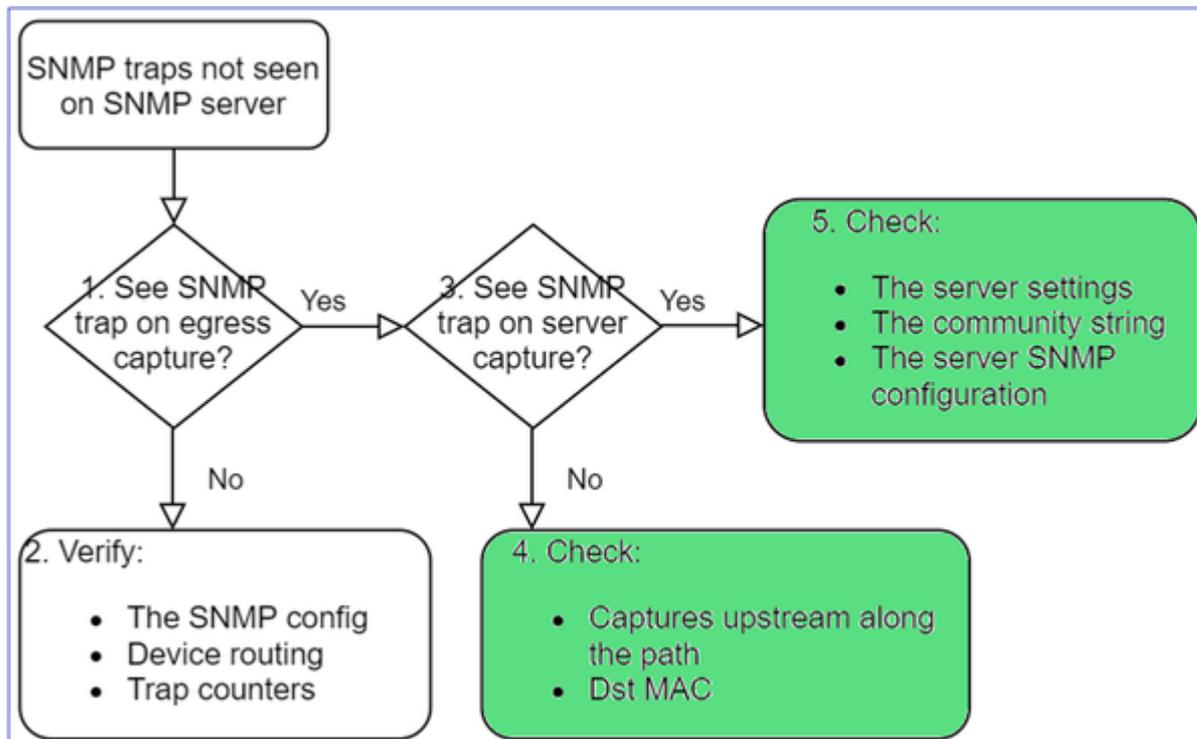
```
connect fxos
```

FP4145-1(fxos)#

```
show snmp | grep Trap
```

1296 Out Traps PDU

Controlli aggiuntivi



- Acquisire il traffico sul server SNMP di destinazione.

Altre cose da controllare:

- Acquisire il traffico lungo il percorso.
- Indirizzo MAC di destinazione dei pacchetti trap SNMP.
- Impostazioni e stato del server SNMP (ad esempio, firewall, porte aperte e così via).
- Stringa della community SNMP.

- Configurazione del server SNMP.

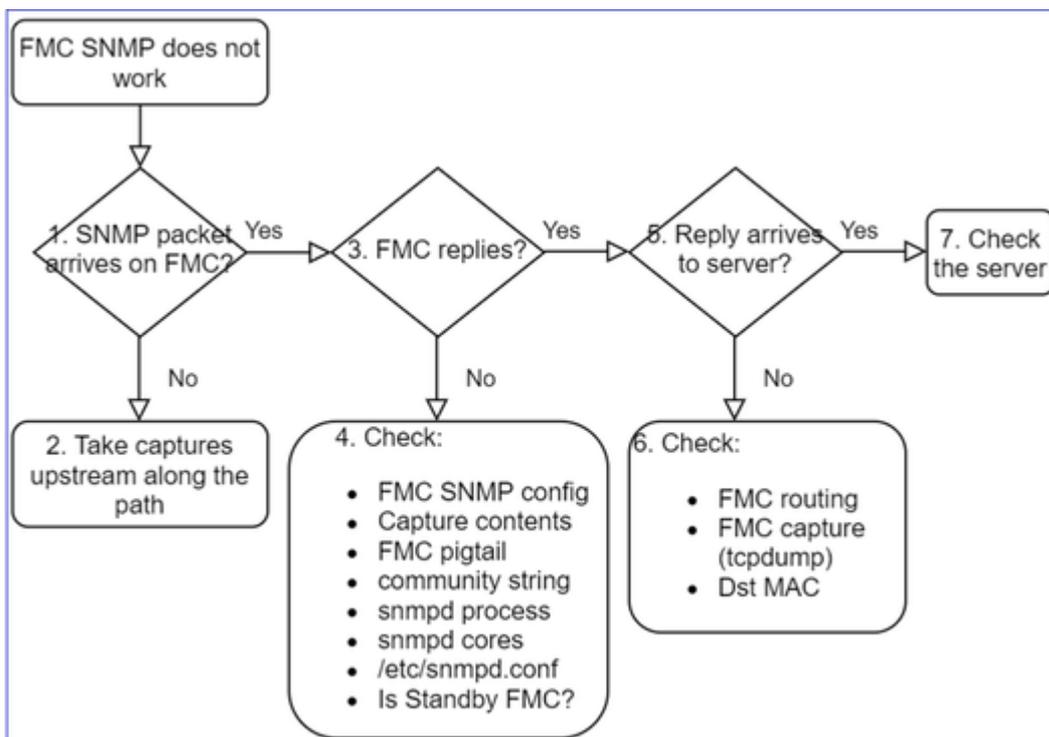
Impossibile monitorare FMC con il protocollo SNMP

Descrizione del problema (situazioni reali gestite da Cisco TAC):

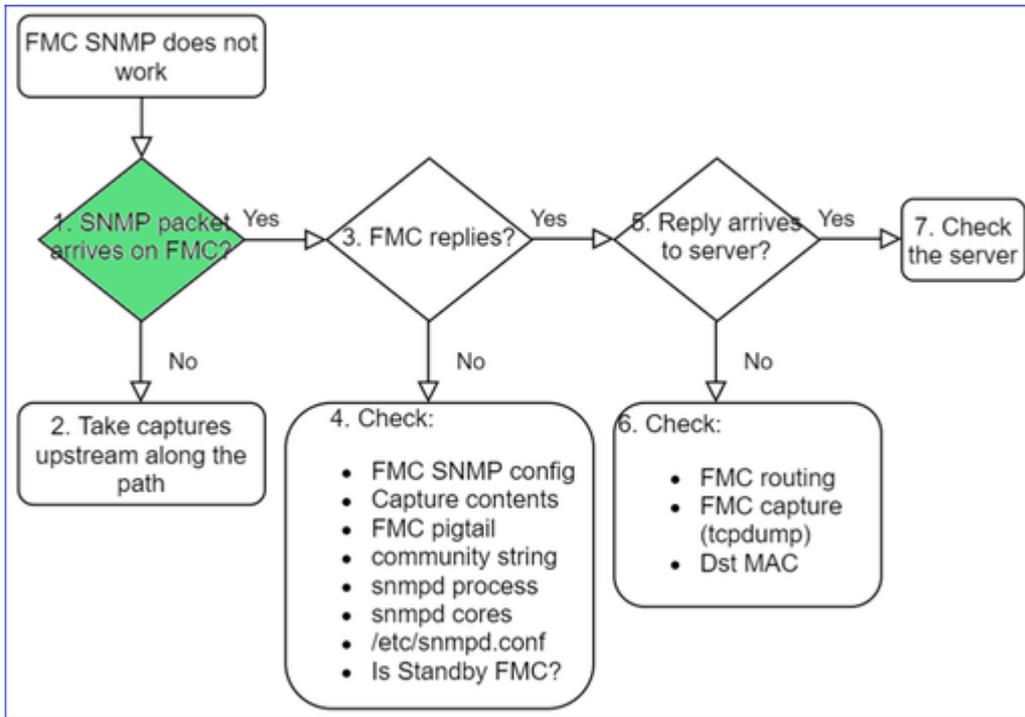
- "SNMP non funziona sull'FMC in standby."
- "Dobbiamo monitorare la memoria dell'FMC."
- "Il protocollo SNMP deve funzionare sull'FMC 192.168.4.0.8 in standby?"
- "Dobbiamo configurare i FMC per monitorare le loro risorse come CPU, memoria e così via".

Risoluzione dei problemi

Questo è il processo per la risoluzione dei problemi relativi al diagramma di flusso per i problemi SNMP di FMC:



1. I pacchetti SNMP arrivano all'FMC?



- Acquisizione sull'interfaccia di gestione FMC:

<#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.
```

Suggerimento: salvare l'acquisizione nella directory /var/common/ del FMC e scaricarla dall'interfaccia utente del FMC

<#root>

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

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

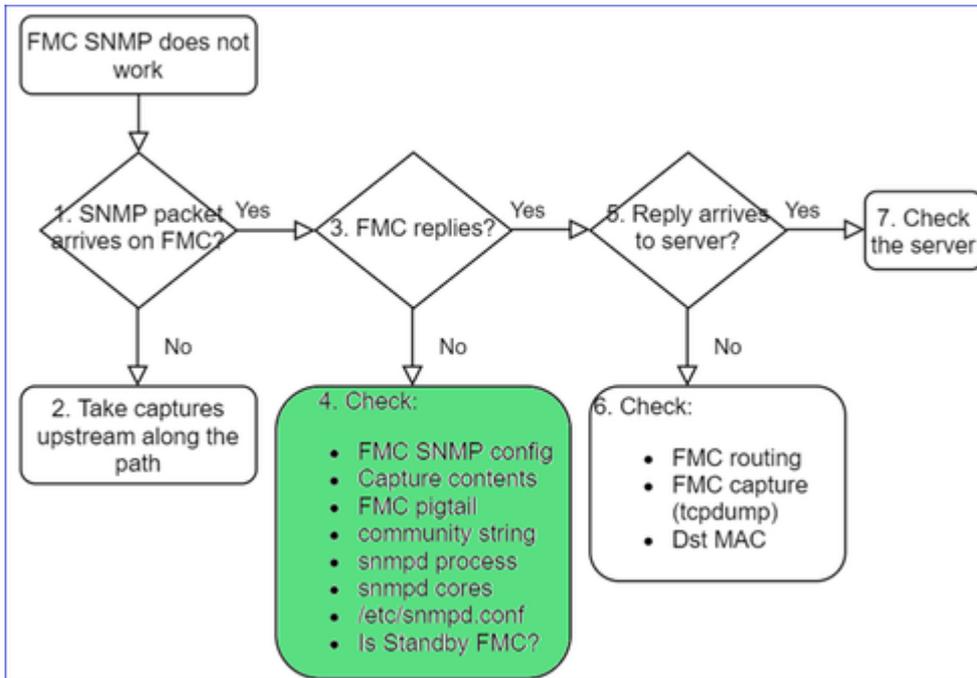
```
HS_PACKET_BUFFER_SIZE is set to 4.
```

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

```
^C46 packets captured
```

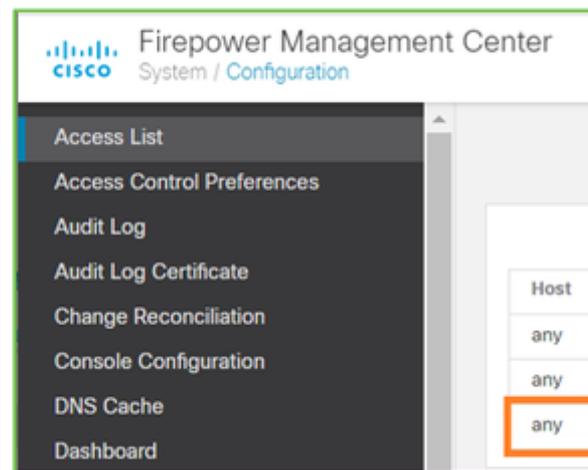
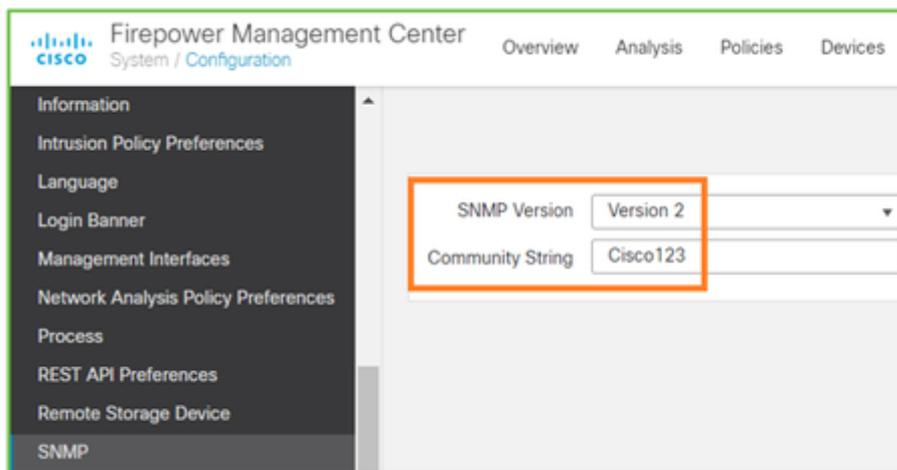
```
46 packets received by filter
```

L'FMC risponde?



Se FMC non risponde, controllare:

- Configurazione del protocollo SNMP di FMC da System > Configuration (Sistema > Configurazione)
 1. Sezione SNMP
 2. Sezione ACL



Se FMC non risponde, controllare:

- Acquisizione dei contenuti (pcap)
- Stringa della community (tramite acquisizione)
- Output di FMC pigtail (cercare eventuali errori o tracce) e contenuti di /var/log/snmpd.log
- Processo snmpd

```
<#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
```

- core snmpd

```
<#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
```

- File di configurazione backend in /etc/snmpd.conf:

```
<#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
```

Nota: se SNMP è disabilitato, il file snmpd.conf non esiste

- L'FMC è in standby?

Sulle release precedenti alla 6.4.0-9 e precedenti alla 6.6.0, l'FMC di standby non invia dati SNMP, quindi snmpd è nello stato Waiting (In attesa). Si tratta di un comportamento normale. Controllare la funzionalità migliorata nell>ID bug Cisco [CSCvs32303](#)

Impossibile configurare il protocollo SNMP

Descrizione del problema (situazioni reali gestite da Cisco TAC):

- "Vogliamo configurare SNMP per Cisco Firepower Management Center e Firepower 4115 Threat Defense."
- "Supporto con configurazione SNMP su FTD".
- "Vogliamo abilitare il monitoraggio SNMP sull'appliance FTD."
- "Cerchiamo di configurare il servizio SNMP in FXOS, ma alla fine il sistema non ci permette di eseguire il commit-buffer. "Errore: modifiche non consentite. Utilizzare 'Connect ftd' per apportare modifiche."
- "Vogliamo abilitare il monitoraggio SNMP sull'appliance FTD."

- "Impossibile configurare SNMP su FTD e rilevare il dispositivo in fase di monitoraggio."

Procedura per risolvere i problemi di configurazione SNMP

Prima cosa: la documentazione!

- Leggere questo documento.
- Guida alla configurazione di FMC:

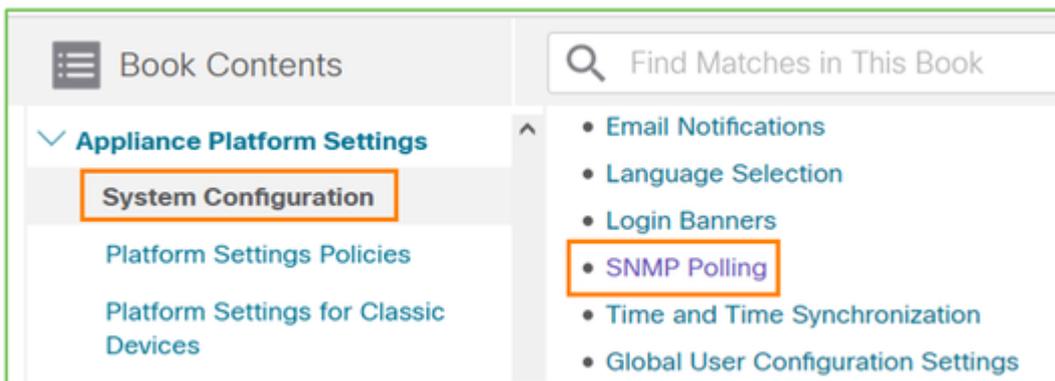
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- Guida alla configurazione di FXOS:

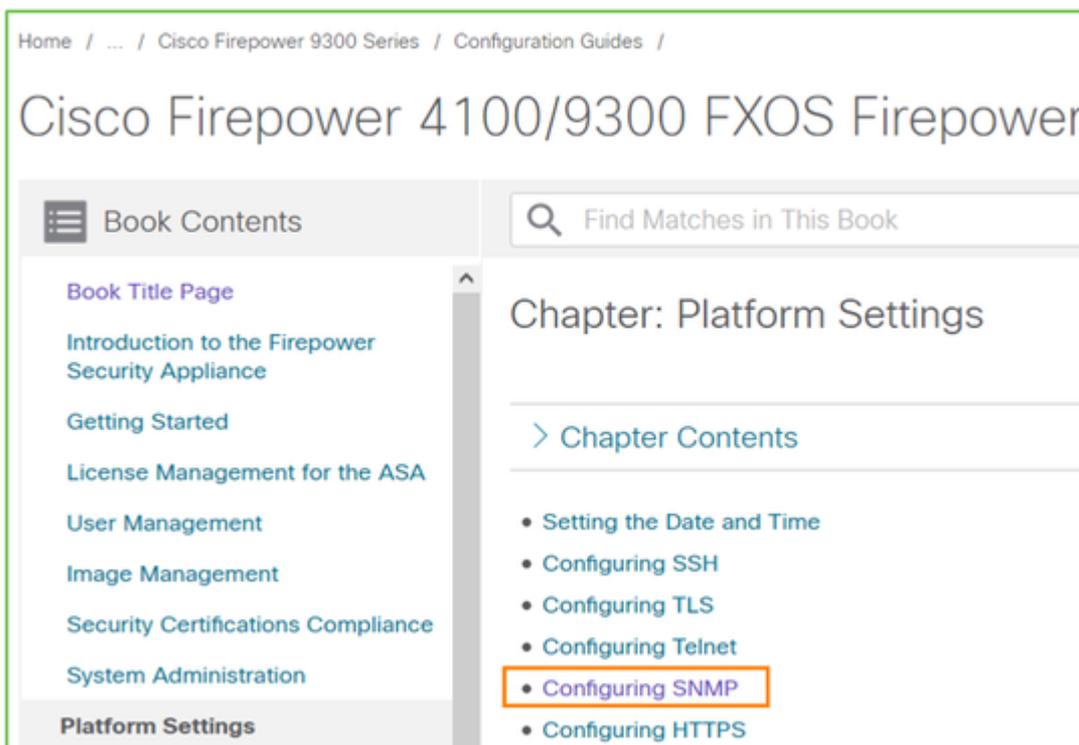
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB115F5

Prestare attenzione ai vari documenti SNMP.

Protocollo SNMP su FMC:



Protocollo SNMP su FXOS:



Configurazione del protocollo SNMP sulle appliance Firepower 41xx/9300:



Configurazione del protocollo SNMP sulle appliance Firepower 1xxx/21xx:



Configurazione del protocollo SNMP su Firepower Device Manager (FDM)

Descrizione del problema (situazioni reali gestite da Cisco TAC):

- "Quali sono le procedure per configurare il protocollo SNMPv3 sui dispositivi Firepower con FDM?"
- "La configurazione SNMP non funziona sul dispositivo FPR 2100 da FDM."
- "Impossibile far funzionare la configurazione SNMPv3 su FDM."
- "Richiesta di supporto per la configurazione del protocollo SNMP su FDM 6.7."
- "Abilitazione di SNMPv3 su Firepower FDM."

Suggerimenti per risolvere i problemi di configurazione SNMP su FDM

- Sulle versioni precedenti alla 6.7, è possibile eseguire la configurazione SNMP con FlexConfig:

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

- A partire da Firepower versione 6.7, la configurazione SNMP non viene più effettuata con FlexConfig, ma con l'API REST:

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

Appunti per la risoluzione dei problemi del protocollo SNMP

1xxx/21xx/41xx/9300 (LINA/ASA) – Informazioni da recuperare prima di inviare una richiesta di assistenza a Cisco TAC

Comando	Descrizione
firepower# show run snmp-server	Verifica la configurazione del protocollo SNMP in ASA/FTD LINA.
firepower# show snmp-server statistics	Verifica le statistiche SNMP su ASA/FTD LINA; in particolare i contatori dei pacchetti SNMP in ingresso e in uscita
> capture-traffic	Permette di acquisire il traffico sull'interfaccia di gestione.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	Acquisire il traffico sull'interfaccia dati (nome "net201") per UDP 161 (polling SNMP).
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	Acquisire il traffico sull'interfaccia dati (nome "net208") per UDP 162. (trap SNMP).
firepower# show capture SNMP-POLL packet-number 1 trace	Tracciare un pacchetto SNMP in entrata che arriva sull'interfaccia dati ASA/FTD LINA.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	Acquisizione sull'interfaccia di tap interna NLP (Non-Lina Process).
firepower# show conn all protocol udp port 161	Controllare tutte le connessioni ASA/FTD LINA su UDP 161 (polling SNMP).
firepower# show log i 302015.*161	Controlla il log ASA/FTD LINA 302015 per il polling SNMP.
firepower# more system:running-config i community	Controlla la stringa della community SNMP.
firepower# debug menu netsnmp 4	Verifica la configurazione e l'ID di processo del protocollo SNMP.
firepower# show asp table classify interface net201 domain permit match port=161	Controllare gli hitcount sull'ACL SNMP sull'interfaccia denominata "net201".
firepower# show disk0: i core	Controlla la presenza di core SNMP;

admin@firepower:~\$ ls -l /var/data/cores	Controlla la presenza di core SNMP; valido solo su FTD.
firepower# show route	Verifica la tabella di routing di ASA/FTD LINA.
> show network	Verifica la tabella di routing del piano di gestione FTD.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	Verifica il protocollo SNMPv3 su FTD per la risoluzione dei problemi.
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	Comandi nascosti nelle release più recenti; debug interni, utili quando si chiede aiuto a Cisco TAC per la risoluzione dei problemi SNMP.

41xx/9300 (FXOS) – Informazioni da recuperare prima di inviare una richiesta di assistenza a Cisco TAC

Comando	Descrizione
firepower# connect fxos firepower(fxos)# ethalyzer 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	Acquisizione FXOS per il polling SNMP (UDP 161) Caricamento su un server FTP remoto FTP IP: 192.0.2.100 Nome utente FTP: ftp
firepower# connect fxos firepower(fxos)# ethalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap	Acquisizione FXOS per le trap SNMP (UDP 162)
firepower# scope system	Controlla l'ACL di FXOS

firepower /system # scope services firepower /system/services # show ip-block detail	
firepower# show fault	Controlla se sono presenti errori FXOS
firepower# show fabric-interconnect	Verifica la configurazione dell'interfaccia di FXOS e le impostazioni del gateway predefinito
firepower# connect fxos firepower(fxos)# show running-config snmp all	Verifica la configurazione SNMP di FXOS
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	Verifica gli SNMP OID di FXOS
firepower# connect fxos firepower(fxos)# show snmp	Verifica le impostazioni e i contatori SNMP di FXOS
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	Esegue il debug SNMP di FXOS ("packets" o "all") Usare i comandi "terminal no monitor" e "undebbug all" per arrestarlo

1xxx/21xx (FXOS) – Informazioni da recuperare prima di inviare una richiesta di assistenza a Cisco TAC

Comando	Descrizione
> capture-traffic	Permette di acquisire il traffico sull'interfaccia di gestione
> show network	Verifica la tabella di routing del piano di gestione FTD
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user	Verifica la configurazione SNMP di FXOS

[detail] firepower /monitoring # show snmp-trap	
firepower# show fault	Controlla se sono presenti errori FXOS
firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores	Controlla se sono presenti file core FXOS (traceback)

FMC â€“ Informazioni da recuperare prima di inviare una richiesta di assistenza a Cisco TAC

Comando	Descrizione
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	Permette di acquisire il traffico sull'interfaccia di gestione per il polling SNMP
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	Permette di acquisire il traffico sull'interfaccia di gestione per il polling SNMP e di salvarlo su un file
admin@FS2600-2:~\$ sudo pmtool status grep snmpd	Controlla lo stato del processo SNMP
admin@FS2600-2:~\$ ls -al /var/common grep snmpd	Controlla se sono presenti file core SNMP (traceback)
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	Controlla i contenuti del file di configurazione SNMP

Esempi di snmpwalk

Questi comandi possono essere usati per la verifica e la risoluzione dei problemi:

Comando	Descrizione
# snmpwalk -c Cisco123 -v2c 192.0.2.1	Recupera tutti gli OID dall'host remoto con SNMP v2c Cisco123 = stringa della community 192.0.2.1 = host di destinazione

<pre># snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.9.109.1.1.1.1.3 iso.3.6.1.4.1.9.9.109.1.1.1.1.3.1 = Sagoma32: 0</pre>	<p>Recupera un OID specifico dall'host remoto con SNMP v2c.</p>
<pre># snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.4.1.9.9.109.1.1.1.1.1 -On .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = Sagoma32: 0</pre>	<p>Mostra gli OID acquisiti in formato numerico.</p>
<pre># snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1</pre>	<p>Recupera tutti gli OID dall'host remoto con SNMP v3</p> <p>Utente SNMPv3 = cisco</p> <p>Autenticazione SNMPv3 = SHA</p> <p>Autorizzazione SNMPv3 = AES</p>
<pre># snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1</pre>	<p>Recupera tutti gli OID dall'host remoto con SNMP v3 (MD5 e AES128)</p>
<pre># snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1</pre>	<p>Solo SNMPv3 con autenticazione</p>

Ricerca delle anomalie SNMP

1. Andare sul sito <https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV>
2. Immettere la parola chiave **snmp** e scegliere **Select from list** (Seleziona dall'elenco).

The screenshot shows the Cisco Bug Search Tool interface. The search term "snmp" is entered in the "Search For" field. The "Product" dropdown is set to "Series/Model", and the "Select from list" button is highlighted. The "Releases" dropdown is set to "Affecting or Fixed in these Releases". At the bottom, there are filter options for Modified Date, Status, Severity, Rating, Support Cases, and Bug Type (set to "Customer Visible").

The screenshot shows a search interface with the following elements:

- Search For: (Examples: CSCtd10124, router crash, etc...)
- Product: (Selected: Cisco Firepower Management Center Virtual Appliance)
- Releases:
- Filters: Modified Date, Status, Severity, Rating, Support Cases, Bug Type (Customer Visible)
- Results: Viewing 1 - 25 of 159 results. Sort by [dropdown]
- Result 1: **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)

Prodotti più comuni:

- Software di Cisco Adaptive Security Appliance (ASA)
- Cisco Firepower serie 9300
- Cisco Firepower Management Center Virtual Appliance
- Cisco Firepower NGFW

Informazioni correlate

- [Configurazione del protocollo SNMP per Threat Defense](#)
- [Configurazione di SNMP su FXOS \(UI\)](#)
- [Documentazione e supporto tecnico “Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).