

為ASA和FTD配置SNMP系統日誌陷阱

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[ASA配置](#)

[FDM管理的FTD配置](#)

[FMC管理的FTD配置](#)

[驗證](#)

[Show snmp-server statistics](#)

[顯示日誌記錄設定](#)

[相關資訊](#)

簡介

本文說明如何配置簡單網路管理協定(SNMP)陷阱以在Cisco自適應安全裝置(ASA)和Firepower威脅防禦(FTD)上傳送系統日誌消息。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ASA基礎知識
- Cisco FTD基礎知識
- SNMP協定基礎知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- 適用於AWS的Cisco Firepower威脅防禦6.6.0
- Firepower管理中心版本6.6.0
- 思科調適型安全裝置軟體版本9.12(3)9

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

背景資訊

Cisco ASA和FTD具有多種功能以提供日誌記錄資訊。但是，在某些特定位置，系統日誌伺服器不是選項。如果有可用的SNMP伺服器，則SNMP陷阱可以提供替代方案。

這是一個用於傳送特定消息以進行故障排除或監控的有用工具。例如，如果在故障切換場景中必須向下跟蹤相關問題，則可以使用FTD和ASA上class ha的SNMP陷阱僅關注這些消息。

有關系統日誌類的詳細資訊，請參閱[本文](#)。

本文旨在提供使用命令列介面(CLI)的ASA、FMC管理的FTD和Firepower裝置管理器(FDM)管理的FTD的配置示例。

如果將Cisco Defense Orchestrator(CDO)用於FTD，則必須將此配置新增到FDM介面。

注意：對於高系統日誌速率，建議在系統日誌消息上配置速率限制，以防止影響其他操作。

這是用於本文檔中所有示例的資訊。

SNMP版本:**SNMPv3**

SNMPv3組：**group-name**

SNMPv3使用者：**具有用於身份驗證的HMAC SHA演算法的管理員使用者**

SNMP伺服器IP地址：**10.20.15.12**

用於與SNMP伺服器通訊的ASA/FTD介面：**外部**

系統日誌消息ID:**111009**

設定

ASA配置

按照以下資訊，可以使用這些步驟在ASA上配置SNMP陷阱。

步驟1.配置要新增到系統日誌清單中的消息。

```
logging list syslog-list message 111009
```

步驟2.配置SNMPv3伺服器引數。

```
snmp-server enable
```

```
snmp-server group group-name v3 auth
```

```
snmp-server user admin-user group-name v3 auth sha cisco123
```

步驟3.啟用SNMP陷阱。

```
snmp-server enable traps syslog
```

步驟4.將SNMP陷阱新增為日誌記錄目標。

logging history syslog-list

FDM管理的FTD配置

這些步驟可用於配置特定系統日誌清單，以便在FDM管理FTD時傳送到SNMP伺服器。

步驟1. 導覽至**對象>事件清單過濾器**，然後在**+按鈕**上選擇。

步驟2. 命名偶數清單並包含相關類或消息ID。然後，選擇確定。

Edit Event List Filter

Name
logging-list

Description
Logs to send through SNMP traps

Severity and Log Class
+

Syslog Range / Message ID
111009
100000 - 999999
[Add Another Syslog Range / Message ID](#)

CANCEL OK

步驟3. 從FDM主屏幕導航到**Advanced Configuration > FlexConfig > FlexConfig Objects**，然後選擇**+按鈕**。

使用所列資訊建立下一個FlexConfig對象：

名稱：**SNMP-Server**

說明（可選）：**SNMP伺服器資訊**

模板：

```
snmp-server enable
snmp-server group group-name v3 auth
snmp-server user admin-user group-name v3 auth sha cisco123
snmp-server host outside 10.20.15.12 version 3 admin-user
```

否定模板：

```
no snmp-server host outside 10.20.15.12 version 3 admin-user
no snmp-server user admin-user group-name v3 auth sha cisco123
no snmp-server group group-name v3 auth
no snmp-server enable
```

Edit FlexConfig Object



Name

SNMP-Server

Description

SNMP Server Information

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand

Reset

```
1 snmp-server enable
2 snmp-server group group-name v3 auth
3 snmp-server user admin-user group-name v3 auth sha cisco123
4 snmp-server host outside 10.20.15.12 version 3 admin-user
```

Negate Template

Expand

Reset

```
1 no snmp-server host outside 10.20.15.12 version 3 admin-user
2 no snmp-server user admin-user group-name v3 auth sha cisco123
3 no snmp-server group group-name v3 auth
4 no snmp-server enable
```

CANCEL

OK

名稱：SNMP-Traps

說明 (可選) : 啟用SNMP陷阱

模板 :

```
snmp-server enable traps syslog
```

否定模板 :

```
no snmp-server enable traps syslog
```

Edit FlexConfig Object

Name

SNMP-Traps

Description

Enable SNMP traps

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template Expand Reset

```
1 snmp-server enable traps syslog
```

Negate Template ⚠ Expand Reset

```
1 no snmp-server enable traps syslog
```

CANCEL OK

名稱 : Logging-history

說明 (可選) : 用於設定SNMP陷阱系統日誌消息的對象

模板 :

```
logging history logging-list
```

否定模板 :

no logging history logging-list

Create FlexConfig Object



Name

Logging-List

Description

Syslog list to send through SNMP traps



Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 logging list syslog-list message 111009
2 logging trap syslog-list
```

Negate Template ⚠

Expand | Reset

```
1 no logging trap syslog-list
2 no logging list syslog-list message 111009
```

CANCEL

OK

步驟4.導覽至Advanced Configuration > FlexConfig > FlexConfig Policy，然後新增在上一步中建立的所有對象。順序不相關，因為從屬命令包含在同一對象(SNMP-Server)中。三個對象都存在後選擇Save，然後「Preview」部分將顯示命令清單。

Device Summary
FlexConfig Policy

Successfully saved.

Group List

- 1. Logging-history
- 2. SNMP-Server
- 3. SNMP-Traps

```
1 logging history logging-list
2 snmp-server enable
3 snmp-server group group-name v3 auth
4 snmp-server user admin-user group-name v3 auth sha cisco123
5 snmp-server host outside 10.20.15.12 version 3 admin-user
6 snmp-server enable traps syslog
```

SAVE

步驟5.選擇Deploy圖示以應用更改。

FMC管理的FTD配置

上述範例顯示與先前類似的案例，但這些變更是在FMC上設定，然後部署至由其管理的FTD。也可使用SNMPv2。[本文說明](#)如何使用FMC管理在FTD上使用此版本設定SNMP伺服器。

步驟1.導航到Devices > Platform Settings，並在分配給受管裝置的策略上選擇Edit，以應用配置。

步驟2.導覽至SNMP，並勾選Enable SNMP Servers選項。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help

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

FTD-PS You have unsaved changes Save

Enter Description Policy A

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

Enable SNMP Servers 

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

Hosts Users **SNMP Traps** Add

Interface	Network	SNMP Version	Poll/Trap	Trap Port	Username
No records to display					

步驟3.選擇Users頁籤，然後選擇Add按鈕。填充使用者資訊。

Add Username ? X

Security Level	Auth
Username*	user-admin
Encryption Password Type	Clear Text
Auth Algorithm Type	SHA
Authentication Password*	••••••••
Confirm*	••••••••
Encryption Type	
Encryption Password	
Confirm	

OK Cancel

步驟4.在Hosts索引標籤中選擇Add。填寫與SNMP伺服器相關的資訊。如果使用介面而不是區域，請確保在右角部分手動新增介面名稱。一旦包含所有必要資訊，請選擇「確定」。

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

Selected Zones/Interfaces

步驟5.選擇SNMP Traps頁籤並選中Syslog框。如果不需要其他所有陷阱複選標籤，請確保將其刪除。

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD-PS You have unsaved changes Save

Enter Description Policy A

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

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

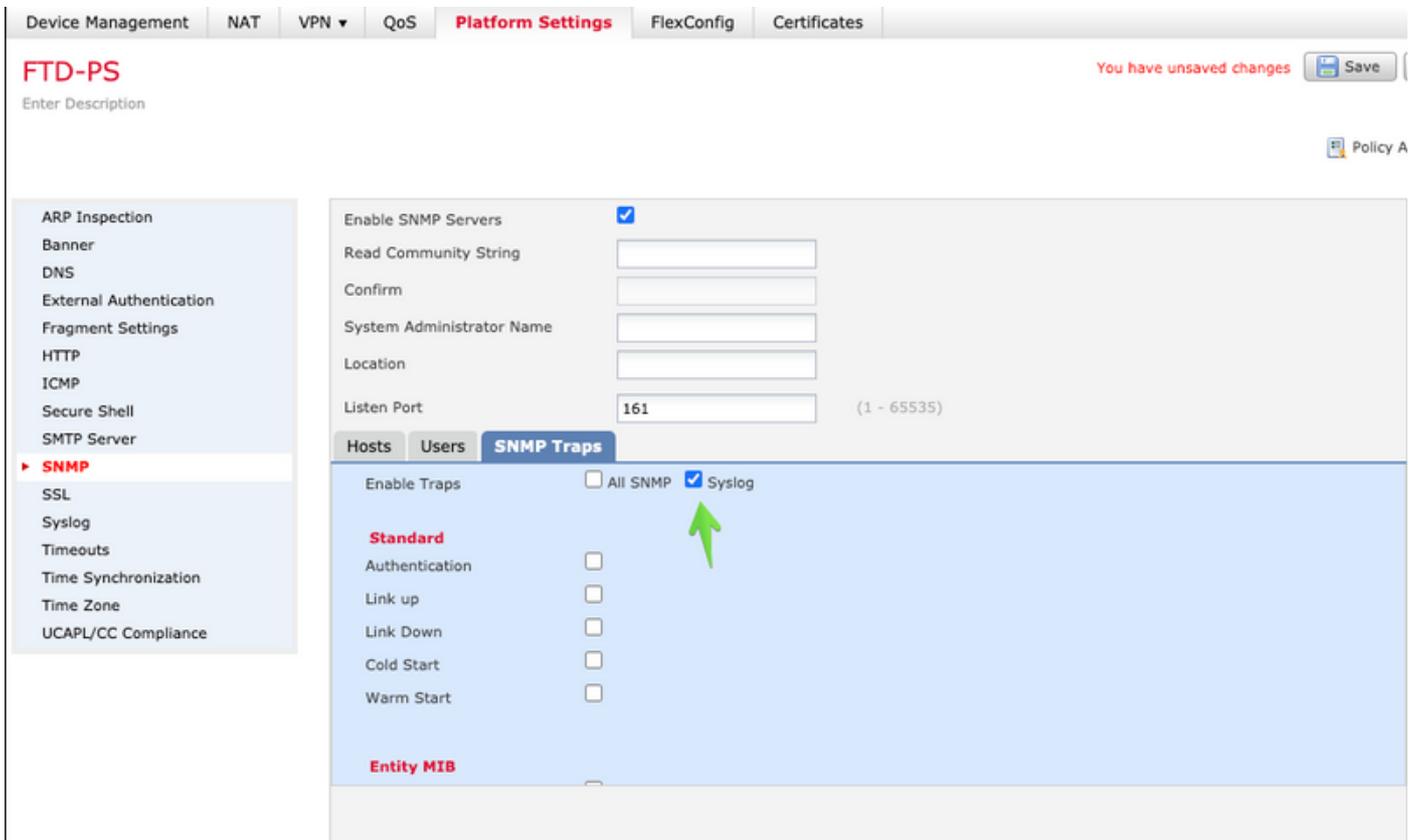
Hosts Users **SNMP Traps**

Enable Traps All SNMP Syslog

Standard

- Authentication
- Link up
- Link Down
- Cold Start
- Warm Start

Entity MIB



步驟6. 導航到Syslog，然後選擇Event Lists頁籤。選擇Add按鈕。新增名稱和要包括在清單中的消息。選擇確定以繼續。

Add Event List ? X

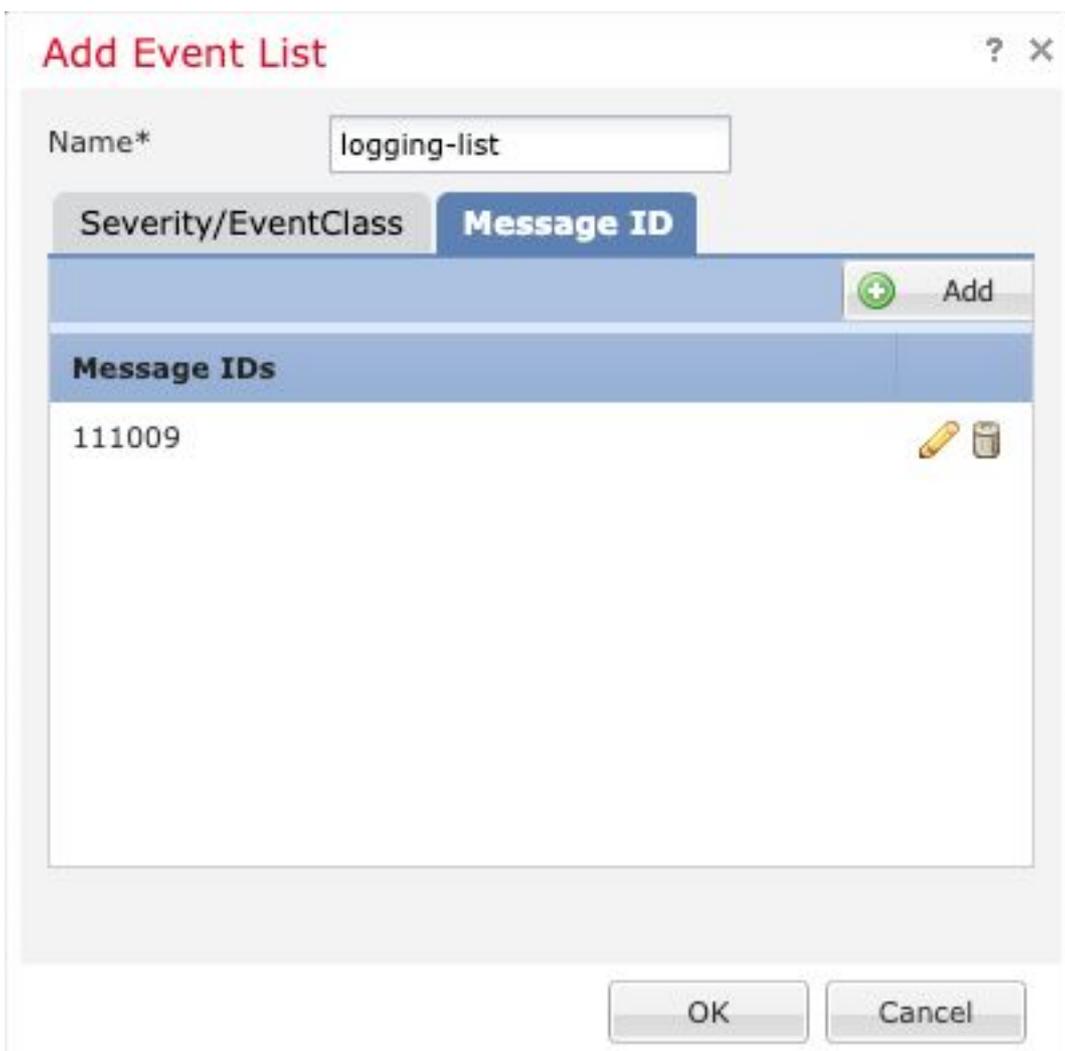
Name*

Severity/EventClass **Message ID**

Add

Message IDs

111009	 
--------	---



步驟7.選擇Logging Destinations選項卡，然後選擇Add按鈕。

將Logging Destination更改為SNMP Trap。

選擇User Event List，然後選擇在步驟6中建立的事件清單。

選擇確定以完成編輯此部分。

Add Logging Filter ? X

Logging Destination: SNMP Trap

Event Class: Use Event List logging-list

Event Class	Syslog Severity
No records to display	

+ Add

OK Cancel

步驟8.選擇Save按鈕並Deploy更改到受管裝置。

驗證

以下命令可用於FTD CLISH和ASA CLI。

Show snmp-server statistics

`show snmp-server statistics`命令會提供有關陷阱傳送次數的資訊。此計數器可以包括其他陷阱。

```
# show snmp-server statistics
0 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)
2 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
```

2 Trap PDUs

此示例中使用的消息ID在使用者每次執行命令時觸發。每次發出「show」命令時，計數器都會增加。

顯示日誌記錄設定

show logging setting提供了有關每個目標傳送的消息的資訊。歷史記錄指示SNMP陷阱的計數器。陷阱日誌記錄統計資訊與Syslog主機計數器相關。

```
# show logging setting
Syslog logging: enabled
Facility: 20
Timestamp logging: enabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 30 messages logged
Trap logging: level debugging, facility 20, 30 messages logged
Global TCP syslog stats::
NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
PARTIAL_REWRITE_CNT: 0
Permit-hostdown logging: disabled
History logging: list syslog-list, 14 messages logged
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

發出命令「**show logging queue**」以確保沒有丟棄任何消息。

```
# show logging queue

Logging Queue length limit : 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msg on queue, 231 msgs most on queue
```

相關資訊

- [Cisco ASA系列系統日誌消息](#)
- [CLI手冊1: Cisco ASA系列常規操作CLI配置指南, 9.12](#)
- [在Firepower NGFW裝置上配置SNMP](#)