

为ASA和FTD配置SNMP系统日志陷阱

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[ASA 配置](#)

[FDM管理的FTD配置](#)

[FMC管理的FTD配置](#)

[验证](#)

[显示snmp-server statistics](#)

[显示日志记录设置](#)

[相关信息](#)

简介

本文档介绍如何配置简单网络管理协议(SNMP)陷阱，以在思科自适应安全设备(ASA)和Firepower威胁防御(FTD)上发送系统日志消息。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco ASA的基本知识
- 思科FTD的基本知识
- SNMP协议的基本知识

使用的组件

本文档中的信息基于以下软件版本：

- 适用于AWS 6.6.0的思科Firepower威胁防御
- Firepower管理中心版本6.6.0
- 思科自适应安全设备软件版本9.12(3)9

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco ASA和FTD具有多种功能来提供日志记录信息。但是，有些特定位置不允许使用系统日志服务器。如果SNMP服务器可用，则SNMP陷阱提供备用。

这是发送特定消息以用于故障排除或监控目的的有用工具。例如，如果在故障切换方案期间有相关问题必须跟踪，则FTD和ASA上类ha的SNMP陷阱只能用于关注这些消息。

有关系统日志类的详细信息，请参[阅本文](#)。

本文的目的是为使用命令行界面(CLI)的ASA、由FMC管理的FTD和由Firepower设备管理器(FDM)管理的FTD提供配置示例。

如果Cisco Defense Orchestrator(CDO)用于FTD，则必须将此配置添加到FDM界面。

警告：对于高系统日志速率，建议对系统日志消息配置速率限制，以防止其他操作的影响。

这是本文档中所有示例所使用的信息。

SNMP版本：**SNMPv3**

SNMPv3组：**组名**

SNMPv3用户：**使用HMAC SHA算法进行身份验证的**管理员用户

SNMP服务器IP地址：**10.20.15.12**

用于与SNMP服务器通信的ASA/FTD接口：**外部**

系统日志消息ID:**111009**

配置

ASA 配置

按照以下信息，这些步骤可用于在ASA上配置SNMP陷阱。

步骤1.配置要添加到系统日志列表的消息。

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

步骤2.配置SNMPv3服务器参数。

```
snmp-server enable
```

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

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

步骤3.启用SNMP陷阱。

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

步骤4.将SNMP陷阱添加为日志记录目标。

logging history syslog-list

FDM管理的FTD配置

当FTD由FDM管理时，这些步骤可用于配置要发送到SNMP服务器的特定系统日志列表。

步骤1.导航至“对象”>“事件列表过滤器”，然后在+按钮上选择。

步骤2.命名偶数列表并包括相关类或消息ID。然后，选择OK。

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

步骤3.从FDM主屏幕导航到“高级配置”>“FlexConfig”>“FlexConfig对象”，然后选择+按钮。

使用列出的信息创建下一个FlexConfig对象：

名称：**SNMP-Server**

说明（可选）：**SNMP服务器信息**

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

名称：SNMP-Traps

说明 (可选) : 启用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

名称 : 日志记录

说明 (可选) : 设置SNMP陷阱系统日志消息的对象

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

步骤4. 导航至“高级配置”>“FlexConfig”>“FlexConfig策略”，然后添加在上一步中创建的所有对象。顺序无关，因为相关命令包含在同一对象(SNMP-Server)中。在三个对象出现后，选择“保存”，“预览”部分显示命令列表。

Successfully saved.

Group List

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

Preview

```
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

步骤5.选择“部署”图标以应用更改。

FMC管理的FTD配置

以上示例说明了与上例类似的场景，但这些更改是在FMC上配置的，然后部署到由其管理的FTD。SNMPv2也可以使用。[本文介绍](#)如何使用FMC管理在FTD上使用此版本设置SNMP服务器。

步骤1.导航至**Devices > Platform Settings**，并在分配给受管设备的策略上选择**Edit**，以将配置应用到。

步骤2.导航至SNMP并选中**Enable SNMP Servers**选项。

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					

步骤3.选择“用户”选项卡并选择“添加”按钮。填写用户信息。



The image shows a dialog box titled "Add Username" with a close button (X) and a help button (?). The dialog contains the following fields and controls:

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

At the bottom of the dialog are two buttons: "OK" and "Cancel".

步骤4.在“主机”选项卡中选择“添加”。填写与SNMP服务器相关的信息。如果使用接口而非区域，请确保在右角手动添加接口名称。在包含所有必要信息后，选择“确定”。

Add SNMP Management Hosts ? X

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

outside

步骤5.选择SNMP Traps选项卡并选中Syslog框。如果不需要，请确保删除所有其他陷阱复选标记。

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

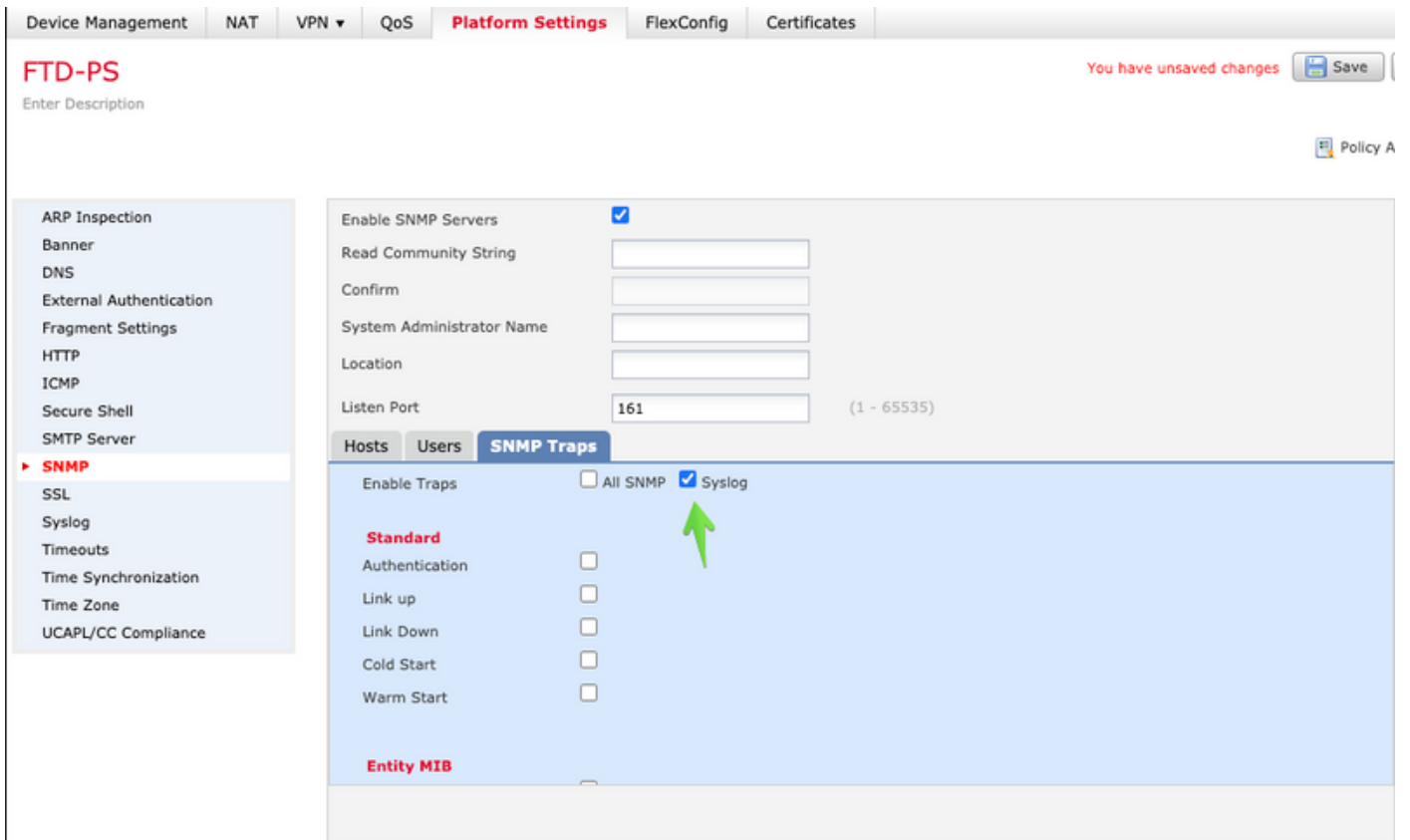
Link up

Link Down

Cold Start

Warm Start

Entity MIB



步骤6. 导航至Syslog，然后选择Event Lists选项卡。选择“添加”按钮。添加名称和要包含在列表中的消息。选择确定继续。



Add Event List ? ×

Name*

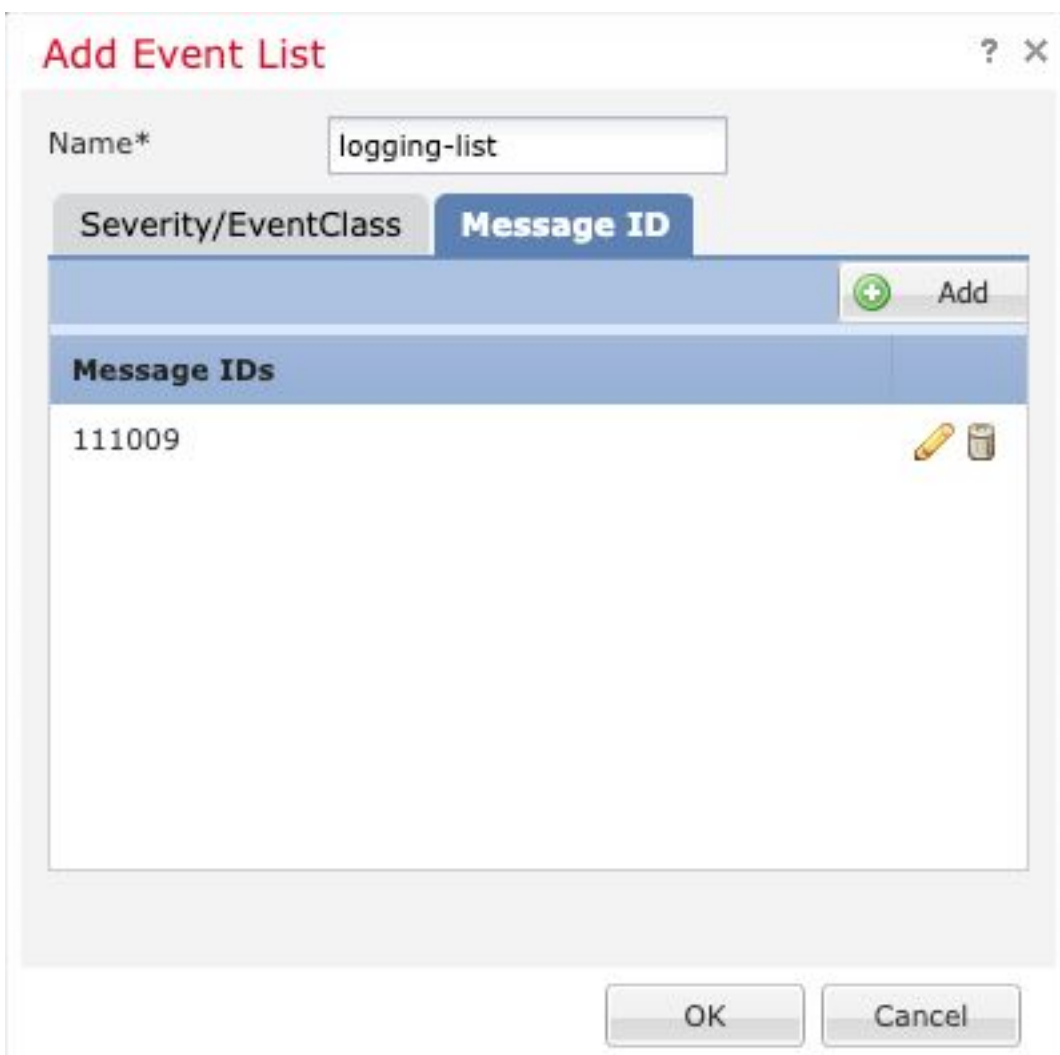
Severity/EventClass **Message ID**

+ Add

Message IDs

111009  

OK Cancel



步骤7.选择Logging Destinations选项卡，然后选择Add按钮。

将Logging Destination (日志记录目标) 更改为SNMP Trap。

选择用户事件列表，然后选择在步骤6中创建的事件列表旁边。

选择“确定”以完成编辑此部分。

The screenshot shows a window titled "Add Logging Filter". It features two dropdown menus: "Logging Destination" is set to "SNMP Trap" and "Event Class" is set to "Use Event List". To the right of the "Event Class" dropdown is a text input field containing "logging-list". Below these controls is a table with two columns: "Event Class" and "Syslog Severity". The table is currently empty, displaying "No records to display". There is an "Add" button with a plus icon in the top right of the table area. At the bottom of the dialog are "OK" and "Cancel" buttons.

步骤8.选择Save按钮并部署对受管设备的更改。

验证

以下命令可在FTD CLISH和ASA CLI中使用。

显示snmp-server statistics

“show snmp-server statistics”命令提供陷阱已发送多少次的信息。此计数器可包含其他陷阱。

```
# 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

用户每次执行命令时，本示例中使用的消息ID都会触发。每次发出“show”命令时，计数器都会增加。

显示日志记录设置

“show logging setting”提供有关每个目标发送的消息的信息。历史记录记录指示SNMP陷阱的计数器。陷阱日志记录统计信息与系统日志主机计数器相关。

```
# 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
```

发出命令show logging queue，确保未丢弃任何消息。

```
# 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
```

相关信息

- [Cisco ASA系列系统日志消息](#)
- [CLI手册1: Cisco ASA系列一般操作CLI配置指南，9.12](#)
- [在Firepower NGFW设备上配置SNMP](#)