

Configurar armadilhas de syslog SNMP para ASA e FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configuração do ASA](#)

[Configuração do FTD gerenciada pelo FDM](#)

[Configuração do FTD gerenciada pelo FMC](#)

[Verificar](#)

[Show snmp-server statistics](#)

[Mostrar configuração de registro](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar as armadilhas do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) para enviar mensagens de Syslog no Cisco Adaptive Security Appliance (ASA) e no Firepower Threat Defense (FTD).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Cisco ASA
- Conhecimento básico do Cisco FTD
- Conhecimento básico do protocolo SNMP

Componentes Utilizados

As informações neste documento são baseadas na seguinte versão de software:

- Cisco Firepower Threat Defense para AWS 6.6.0
- Firepower Management Center versão 6.6.0
- Software Cisco Adaptive Security Appliance versão 9.12(3)9

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco ASA e o FTD têm vários recursos para fornecer informações de registro. No entanto, há locais específicos onde um servidor Syslog não é uma opção. As interceptações SNMP (traps) oferecem uma alternativa se houver um servidor SNMP disponível.

Essa é uma ferramenta útil para enviar mensagens específicas para fins de solução de problemas ou monitoramento. Por exemplo, se houver um problema relevante que deve ser rastreado durante cenários de failover, as interceptações SNMP para class ha no FTD e no ASA podem ser usadas para focar apenas nessas mensagens.

Mais informações relacionadas às classes Syslog podem ser encontradas [neste documento](#).

A finalidade deste artigo é fornecer exemplos de configuração para o ASA que usa CLI (Command Line Interface, interface de linha de comando), FTD gerenciado pelo FMC e FTD gerenciado pelo Firepower Device Manager (FDM).

Se o Cisco Defense Orchestrator (CDO) for usado para o FTD, essa configuração deverá ser adicionada à interface do FDM.

Caution: Para altas taxas de syslog, é recomendável configurar um limite de taxa em mensagens de syslog para evitar o impacto em outras operações.

Estas são as informações usadas para todos os exemplos neste documento.

Versão SNMP: **SNMPv3**

Grupo SNMPv3: **group-name**

Usuário SNMPv3: **admin-user** com algoritmo HMAC SHA para autenticação

Endereço IP do servidor SNMP: **10.20.15.12**

Interface ASA/FTD a ser usada para comunicação com o Servidor SNMP: **Externo**

ID da mensagem do syslog: **111009**

Configurar

Configuração do ASA

Essas etapas podem ser usadas para configurar interceptações SNMP em um ASA, seguindo as informações abaixo.

Etapa 1. Configure as mensagens a serem adicionadas à lista de syslog.

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

Etapa 2. Configurar parâmetros do Servidor SNMPv3.

```
snmp-server enable
```

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

Etapa 3. Habilite interceptações SNMP (traps).

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

Etapa 4. Adicione as interceptações SNMP como um destino de registro.

```
logging history syslog-list
```

Configuração do FTD gerenciada pelo FDM

Essas etapas podem ser usadas para configurar uma lista de Syslog específica para enviar ao servidor SNMP quando o FTD é gerenciado pelo FDM.

Etapa 1. Navegue até **Objetos > Filtros da Lista de Eventos** e selecione no botão **+**.

Etapa 2. Nomeie a Lista par e inclua as classes ou IDs de mensagem relevantes. Em seguida, selecione 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

Etapa 3. Navegue até **Advanced Configuration > FlexConfig > FlexConfig Objects** na tela inicial do FDM e selecione o botão **+**.

Crie os próximos Objetos FlexConfig com as informações listadas:

Nome: **SNMP-Server**

Descrição (Opcional): **Informações do servidor SNMP**

Modelo:

```
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
```

Negar modelo:

```
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

Nome: **SNMP-Traps**

Descrição (Opcional): **Ativar interceptações SNMP**

Modelo:

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

Negar modelo:

```
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

Nome: **Logging-history**

Descrição (Opcional): **Objeto para definir mensagens de syslog SNMP traps**

Modelo:

```
logging history logging-list
```

Negar modelo:

```
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

Etapa 4. Navegue até **Advanced Configuration > FlexConfig > FlexConfig Policy** e adicione todos os objetos criados na etapa anterior. O pedido é irrelevante, pois os comandos dependentes são incluídos no mesmo objeto (SNMP-Server). Selecione **Salvar** quando os três objetos estiverem lá e a seção **Visualizar** mostrar a lista de comandos.

Device Summary
FlexConfig Policy

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

Etapa 5. Selecione o ícone **Implantar** para aplicar as alterações.

Configuração do FTD gerenciada pelo FMC

Os exemplos acima ilustram cenários semelhantes aos anteriores, mas essas alterações são configuradas no FMC e implantadas em um FTD gerenciado por ele. SNMPv2 também pode ser usado. [Este artigo](#) explica como usar configurar um servidor SNMP com esta versão no FTD usando o gerenciamento do FMC.

Etapa 1. Navegue para **Dispositivos > Configurações da plataforma** e selecione **Editar** na Política atribuída ao dispositivo gerenciado para aplicar a configuração.

Etapa 2. Navegue até **SNMP** e marque a opção **Ativar servidores SNMP**.


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					

Etapa 3. Selecione a guia **Usuários** e selecione o botão **Adicionar**. Preencha as informações do usuário.

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

Etapa 4. Selecione **Adicionar** na guia **Hosts**. Preencha as informações relacionadas ao Servidor SNMP. Se você usar uma interface em vez de uma zona, certifique-se de adicionar manualmente o nome da interface na seção do canto direito. Selecione OK assim que todas as informações necessárias forem incluídas.

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

outside	<input type="button" value="trash"/>
---------	--------------------------------------

Etapa 5. Selecione a guia **SNMP Traps** e marque a caixa **Syslog**. Certifique-se de remover todas as outras marcas de seleção de armadilhas, se elas não forem necessárias.

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

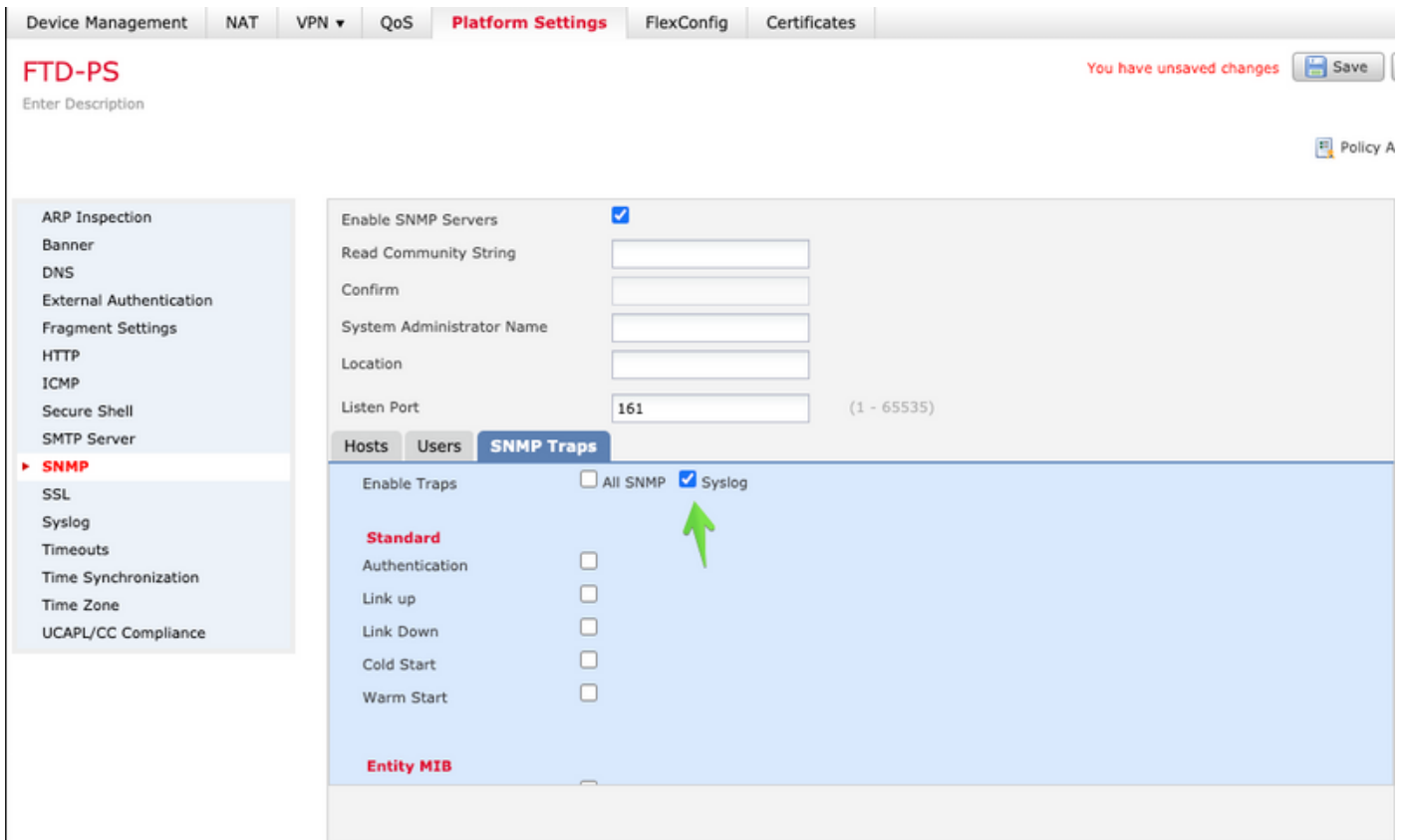
Link up

Link Down

Cold Start

Warm Start

Entity MIB





Etapa 6. Navegue até **Syslog** e selecione a guia **Listas de Eventos**. Selecione o botão **Adicionar**. Adicione um nome e as mensagens a serem incluídas na lista. Selecione **OK** para continuar.

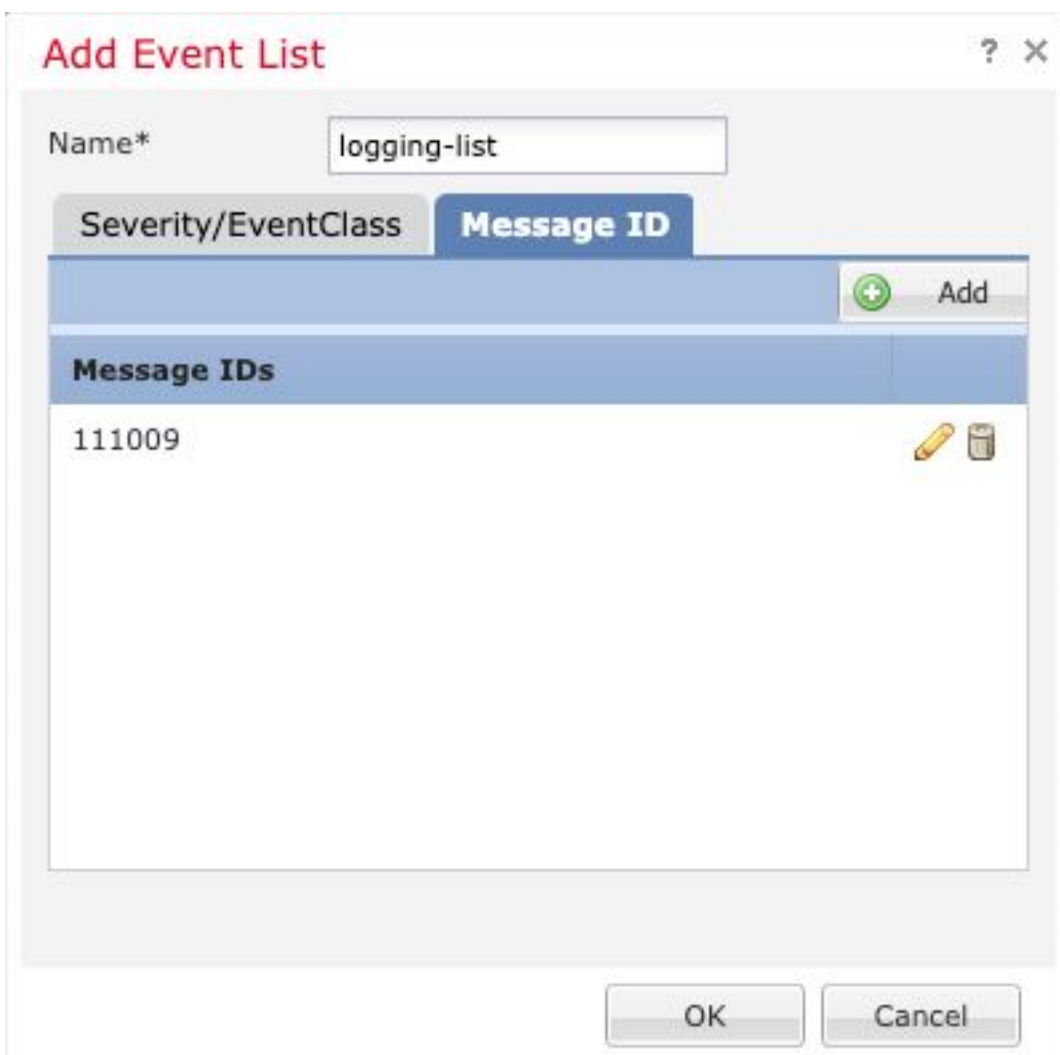
Add Event List ? X

Name*

Severity/EventClass **Message ID**

Message IDs

111009  



Passo 7. Selecione a guia **Logging Destinations** e selecione o botão **Add**.

Altere o destino de registro para **interceptação SNMP**.

Selecione **User Event List** e escolha a lista de eventos criada na Etapa 6 ao lado dela.

Selecione **OK** para concluir a edição desta seção.

The screenshot shows a dialog box titled "Add Logging Filter". At the top, there are two dropdown menus: "Logging Destination" set to "SNMP Trap" and "Event Class" set to "Use Event List". To the right of the "Event Class" dropdown is another dropdown menu set to "logging-list". Below these is a table with two columns: "Event Class" and "Syslog Severity". The table is currently empty, displaying "No records to display" in the center. At the bottom right of the table area is a green "+" button labeled "Add". At the bottom of the dialog box are "OK" and "Cancel" buttons.

Etapa 8. Selecione o botão **Salvar e Implantar** as alterações no dispositivo gerenciado.

Verificar

Os comandos abaixo podem ser usados na CLISH do FTD e na CLI do ASA.

Show snmp-server statistics

O comando "**show snmp-server statistics**" fornece informações sobre quantas vezes uma armadilha foi enviada. Este contador pode incluir outras armadilhas.

```
# 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

A ID da mensagem usada neste exemplo é acionada toda vez que um usuário executa um comando. Sempre que um comando "show" é emitido, o contador aumenta.

Mostrar configuração de registro

A "show logging setting" fornece informações sobre as mensagens enviadas por cada destino. O registro de histórico indica os contadores para interceptações SNMP. As estatísticas de registro de interceptação (Trap) estão relacionadas aos contadores dos hosts do Syslog.

```
# 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
```

Emita o comando "show logging queue" para garantir que nenhuma mensagem esteja sendo removida.

```
# 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
```

Informações Relacionadas

- [Mensagens de syslog do Cisco ASA Series](#)
- [Livro 1 da CLI: Guia de configuração da CLI de operações gerais do Cisco ASA Series, 9.12](#)
- [Configurar SNMP em dispositivos Firepower NGFW](#)