

Configurazione di SNMP Syslog Trap per ASA e FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione ASA](#)

[Configurazione FTD gestita da FDM](#)

[Configurazione FTD gestita da FMC](#)

[Verifica](#)

[Mostra statistiche snmp-server](#)

[Mostra impostazione di registrazione](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare le trap SNMP (Simple Network Management Protocol) per inviare messaggi Syslog su Cisco Adaptive Security Appliance (ASA) e Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Cisco ASA
- Conoscenze base di Cisco FTD
- Conoscenze base del protocollo SNMP

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

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

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

Cisco ASA e FTD hanno diverse funzionalità per fornire informazioni di log. Tuttavia, esistono percorsi specifici in cui un server Syslog non è un'opzione. Le trap SNMP rappresentano un'alternativa se è disponibile un server SNMP.

Si tratta di uno strumento utile per inviare messaggi specifici a scopo di risoluzione dei problemi o monitoraggio. Ad esempio, se esiste un problema rilevante che deve essere individuato durante gli scenari di failover, le trap SNMP per la classe ha su FTD e ASA possono essere utilizzate solo per concentrarsi su questi messaggi.

Ulteriori informazioni relative alle classi Syslog sono disponibili in [questo documento](#).

Lo scopo di questo articolo è quello di fornire esempi di configurazione per ASA utilizzando l'interfaccia della riga di comando (CLI), FTD gestito da FMC e FTD gestito da Firepower Device Manager (FDM).

Se Cisco Defense Orchestrator (CDO) viene utilizzato per FTD, questa configurazione deve essere aggiunta all'interfaccia FDM.

Attenzione: Per velocità di syslog elevate, si consiglia di configurare un limite di velocità per i messaggi syslog per evitare l'impatto su altre operazioni.

Queste sono le informazioni usate in tutti gli esempi riportati nel presente documento.

Versione SNMP: **SNMPv3**

Gruppo SNMPv3: **nome-gruppo**

Utente SNMPv3: **utente-amministratore** con algoritmo SHA HMAC per l'autenticazione

Indirizzo IP server SNMP: **10.20.15.12**

Interfaccia ASA/FTD da utilizzare per comunicare con il server SNMP: **esterna**

ID messaggio syslog: **111009**

Configurazione

Configurazione ASA

La procedura descritta di seguito può essere utilizzata per configurare le trap SNMP su un'ASA.

Passaggio 1. Configurare i messaggi da aggiungere all'elenco syslog.

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

Passaggio 2. Configurare i parametri del server SNMPv3.

```
snmp-server enable
```

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

Passaggio 3. Abilitare le trap SNMP.

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

Passaggio 4. Aggiungere le trap SNMP come destinazione di registrazione.

```
logging history syslog-list
```

Configurazione FTD gestita da FDM

Questa procedura può essere utilizzata per configurare un elenco Syslog specifico da inviare al server SNMP quando FTD è gestito da FDM.

Passaggio 1. Passare a **Oggetti > Filtri elenco eventi** e selezionare il pulsante **+**.

Passaggio 2. Assegnare un nome all'Elenco pari e includere le classi o gli ID messaggio rilevanti. Quindi, selezionare 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

Passaggio 3. Passare a **Configurazione** avanzata > **FlexConfig** > **Oggetti FlexConfig** dalla schermata principale di FDM e selezionare il pulsante +.

Creare gli oggetti FlexConfig successivi con le informazioni elencate:

Nome: **SNMP-Server**

Descrizione (facoltativa): **Informazioni server SNMP**

Modello:

```
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
```

Nega modello:

```
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-Trap**

Descrizione (facoltativa): **Abilita trap SNMP**

Modello:

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

Nega modello:

```
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**

Descrizione (facoltativa): **oggetto per impostare i messaggi syslog delle trap SNMP**

Modello:

```
logging history logging-list
```

Nega modello:

```
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

Passaggio 4. Passare a **Configurazione avanzata > FlexConfig > Policy FlexConfig** e aggiungere tutti gli oggetti creati nel passaggio precedente. L'ordine è irrilevante in quanto i comandi dipendenti sono inclusi nello stesso oggetto (SNMP-Server). Selezionare **Save** quando i tre oggetti sono presenti e la sezione **Preview** mostra l'elenco dei comandi.

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

Passaggio 5. Selezionare l'icona **Distribuisci** per applicare le modifiche.

Configurazione FTD gestita da FMC

Gli esempi riportati sopra illustrano scenari simili a quelli precedenti, ma queste modifiche vengono configurate nel CCP e quindi distribuite in un FTD gestito dal CCP. È possibile utilizzare anche SNMPv2. [Questo articolo](#) spiega come utilizzare la configurazione di un server SNMP con questa versione su FTD utilizzando la gestione FMC.

Passaggio 1. Passare a **Dispositivi > Impostazioni piattaforma** e selezionare **Modifica** nel criterio assegnato al dispositivo gestito a cui applicare la configurazione.

Passaggio 2. Passare a **SNMP** e selezionare l'opzione **Enable SNMP Servers** (Abilita server 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					

Passaggio 3. Selezionare la scheda **Utenti** e selezionare il pulsante **Aggiungi**. Immettere le informazioni sull'utente.

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

Passaggio 4. Selezionare **Add** nella scheda **Hosts**. Immettere le informazioni relative al server SNMP. Se si utilizza un'interfaccia invece di una zona, assicurarsi di aggiungere manualmente il nome dell'interfaccia nella sezione ad angolo destro. Selezionare OK dopo aver incluso tutte le informazioni necessarie.

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



Add

Add

OK

Cancel

Passaggio 5. Selezionare la scheda **SNMP Trap** e selezionare la casella **Syslog**. Assicurarsi di rimuovere tutti gli altri segni di spunta se non sono necessari.

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

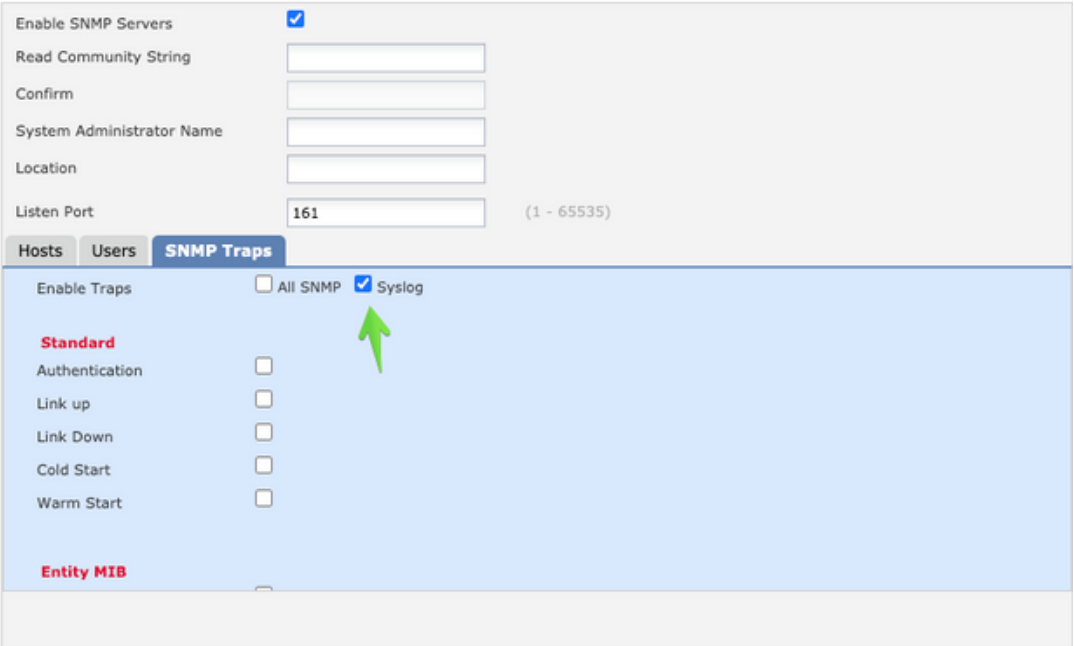
Link up

Link Down

Cold Start

Warm Start

Entity MIB



Passaggio 6. Passare a **Syslog** e selezionare la scheda **Elenchi eventi**. Selezionare il pulsante **Aggiungi**. Aggiungere un nome e i messaggi da includere nell'elenco. Selezionare **OK** per continuare.

Add Event List ? X

Name*

Severity/EventClass **Message ID**

+ Add

Message IDs
111009

OK Cancel

Passaggio 7. Selezionare la scheda **Destinazioni di logging** e selezionare il pulsante **Aggiungi**.

Modificare la destinazione di registrazione in **Trap SNMP**.

Selezionare **Elenco eventi utente** e scegliere l'elenco di eventi creato nel passo 6 accanto ad esso.

Selezionare **OK** per completare la modifica della sezione.



Passaggio 8. Selezionare il pulsante **Salva e Distribuire** le modifiche al dispositivo gestito.

Verifica

I comandi riportati di seguito possono essere utilizzati sia nella CLI FTD CLISH che nella CLI ASA.

Mostra statistiche snmp-server

Il comando "**show snmp-server statistics**" fornisce informazioni sul numero di invii di una trap. Questo contatore può includere altre trap.

```
# 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
```

L'ID messaggio utilizzato in questo esempio viene attivato ogni volta che un utente esegue un

comando. Ogni volta che viene emesso un comando "show", il contatore aumenta.

Mostra impostazione di registrazione

L'impostazione "show logging" fornisce informazioni sui messaggi inviati da ciascuna destinazione. La registrazione della cronologia indica i contatori delle trap SNMP. Le statistiche di registrazione dei trap sono correlate ai contatori degli host 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
```

Utilizzare il comando "show logging queue" per assicurarsi che non vengano eliminati messaggi.

```
# 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
```

Informazioni correlate

- [Messaggi syslog Cisco serie ASA](#)
- [CLI Book 1: Guida alla configurazione della CLI per le operazioni generali della serie Cisco ASA, 9.12](#)
- [Configurazione di SNMP su appliance Firepower NGFW](#)