Problemen oplossen bij het verzenden van logboeken door firewall naar een eerder geconfigureerde (oudere) Syslog-server

Inhoud

uitgeven

De firewall stuurt syslog-berichten naar een eerder geconfigureerde (legacy) syslog-server op IP-adres 198.51.100.100. Dit IP-adres ontbreekt in de firewallconfiguratie.

milieu

De getroffen platforms zijn specifiek Firepower 2100 die ASA in platformmodus draait.

resolutie

Stap 1. Zoek het IP-adres van de syslog-berichten:

Op basis van de analyse van de berichten die door de oudere syslog-server zijn ontvangen, is het oorspronkelijke IP-adres het IP-adres voor beheer van het Firepower-chassis.

Het IP-adres dat is geconfigureerd in het Firepower eXtensible Operating System (FXOS) is 192.0.2.100:

<#root>

```
2026-04-27 15:22:49    User.Error
```

```
192.0.2.100

    Apr 27 09:22:49 firepower FPRM: <<%FPRM-3-NTP_CONFIG_FAILED>> [F1329][major][ntp-config-failed][sys
2026-04-27 15:22:54   User.Error

192.0.2.100

    Apr 27 09:22:54 firepower FPRM: <<%FPRM-3-NTP_CONFIG_FAILED>> [F1329][cleared][ntp-config-failed][s
```

Stap 2. Controleer en verifieer de configuratie van de FXOS-syslog:

- De FXOS Command Line Interface (CLI)-configuratie bevat niet het adres van de oudere syslog-server:

<#root>

```
device #

scope monitoring


device /monitoring #

show configuration | i 198.51.100.100


device /monitoring #

show configuration all | i 198.51.100.100
```

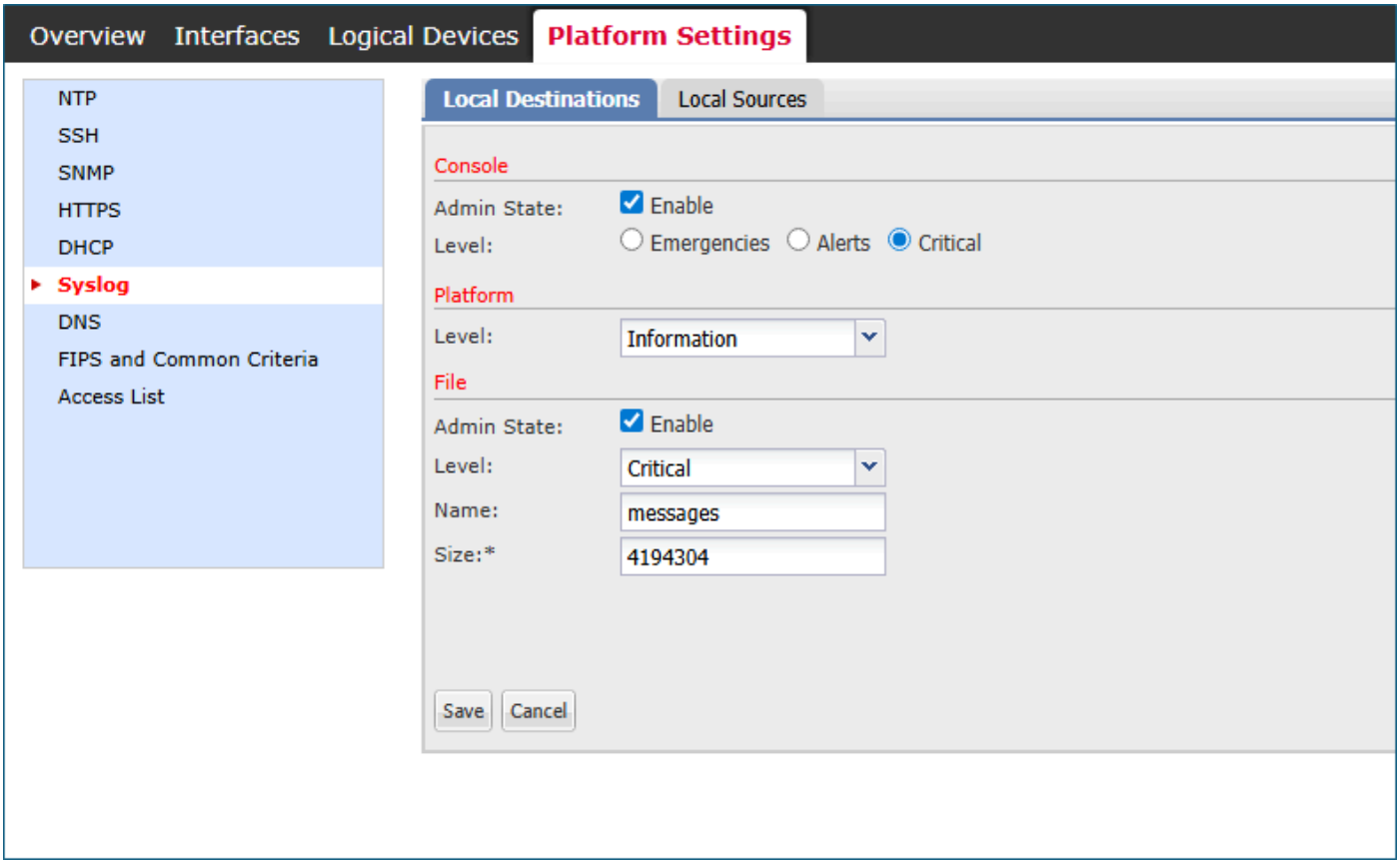
- Tegelijkertijd toont de uitvoer van de opdracht show syslog in het monitoringbereik het IP-adres van de server:

<#root>

```
device #

scope monitoring


device /monitoring #

show syslog
```

```
console
    state: Disabled
    level: Critical

platform
    state: Enabled
    level: Information
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 198.51.100.10        Enabled  Warnings      Local7


Server 2 198.51.100.100       Enabled  Warnings      Local7 <---- legacy server


    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Disabled
```

- Firepower Chassis Manager (FCM) Gebruikersinterface (UI) > Platforminstellingen > Syslog geeft de configuratie van de syslog-server niet aan.



fcm_syslogs_configuration.png

Stap 3. Probeer de syslog-server te wijzigen of te verwijderen:

<#root>

```
device#

scope monitoring



device /monitoring #

delete


  <---
  snmp-trap  SNMP trap hostname or IP address
  snmp-user  SNMPv3 User

device /monitoring #

set syslog


  <---
  console   Console
  file      File
  platform  Platform

device /monitoring #

set syslog platform


 <---
  level  Level
```

De conclusie is dat noch FXOS CLI noch FCM UI een manier bieden om een syslog-server te maken, te wijzigen of te verwijderen, inclusief 198.51.100.100.

Oorzaak

Overweeg drie softwarefouten:

Cisco bug ID CSCvn19025

De softwareversies met de oplossing van dit defect staan de configuratie van de externe FXOS-

syslog in de CLI of FCM UI niet toe.

Cisco bug ID CSCvt85766

De oplossing van dit defect verwijdert de sectie "Externe bestemmingen" uit de FXOS show syslog command output.

Versies zonder fix:

<#root>

```
device#

scope monitoring


device /monitoring #

show syslog



console
    state: Enabled
    level: Critical

platform
    state: Enabled
    level: Information

file
    state: Enabled
    level: Critical
    name:  messages
    size:  4194304

remote destinations <----------------
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 192.0.2.1            Enabled  Information   Local7
    Server 2 192.0.2.2            Enabled  Information   Local7
    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Disabled
```

Versies met de fix missen de sectie "Externe bestemmingen":

<#root>

```
device #

scope monitoring


device /monitoring #

show syslog



console
    state: Enabled
    level: Critical

platform
    state: Enabled
    level: Information
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 192.0.2.1            Enabled  Information   Local7
    Server 2 192.0.2.2            Enabled  Information   Local7
    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Disabled
```

Ondanks het ontbreken van de sectie "Externe bestemmingen", zijn de syslog-servers zichtbaar in de sectie "Platform".

Cisco bug ID CSCwu12470

Na de software-upgrade naar de versie met de oplossing van Cisco bug ID CSCvn19025 is het beheer van externe syslog-servers, dat wil zeggen het maken, wijzigen of verwijderen, niet toegestaan in de FXOS CLI of FCM UI. Deze beperking geldt ook voor de servers die vóór de upgrade zijn geconfigureerd. Desondanks toont de FXOS-software na de software-upgrade de syslog-servers in de sectie "platform" van de show syslog-opdrachtuitvoer en verzendt de syslog-berichten naar deze servers. Gebruikers kunnen de bestaande FXOS-configuratie voor externe syslog niet beheren, die wordt bijgehouden in de Cisco-bug-ID CSCwu12470.

Verwante inhoud

- Cisco bug ID CSCvn19025
- Cisco bug ID CSCvt85766
- Cisco bug ID CSCwu12470

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.