Fehlerbehebung: Firewall - Protokolle an zuvor konfigurierten (älteren) Syslog-Server senden

Inhalt

Problem

Die Firewall sendet Syslog-Meldungen an einen zuvor konfigurierten (älteren) Syslog-Server mit der IP-Adresse 198.51.100.100. Diese IP-Adresse ist in der Firewall-Konfiguration nicht vorhanden.

Umwelt

Betroffen sind insbesondere Firepower 2100 mit ASA im Plattformmodus.

Auflösung

Schritt 1: Suchen Sie die Quell-IP-Adresse der Syslog-Meldungen:

Basierend auf der Analyse der vom Legacy-Syslog-Server empfangenen Meldungen ist die Ursprungs-IP-Adresse die Management-IP-Adresse des FirePOWER-Chassis.

Die im FirePOWER Extensible Operating System (FXOS) konfigurierte IP-Adresse lautet 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
```

Schritt 2: Überprüfen und Überprüfen der FXOS-Syslog-Konfiguration:

- Die FXOS-CLI-Konfiguration (Command Line Interface) enthält nicht die Adresse des Legacy-Syslog-Servers:

<#root>

```
device #

scope monitoring


device /monitoring #

show configuration | i 198.51.100.100


device /monitoring #

show configuration all | i 198.51.100.100
```

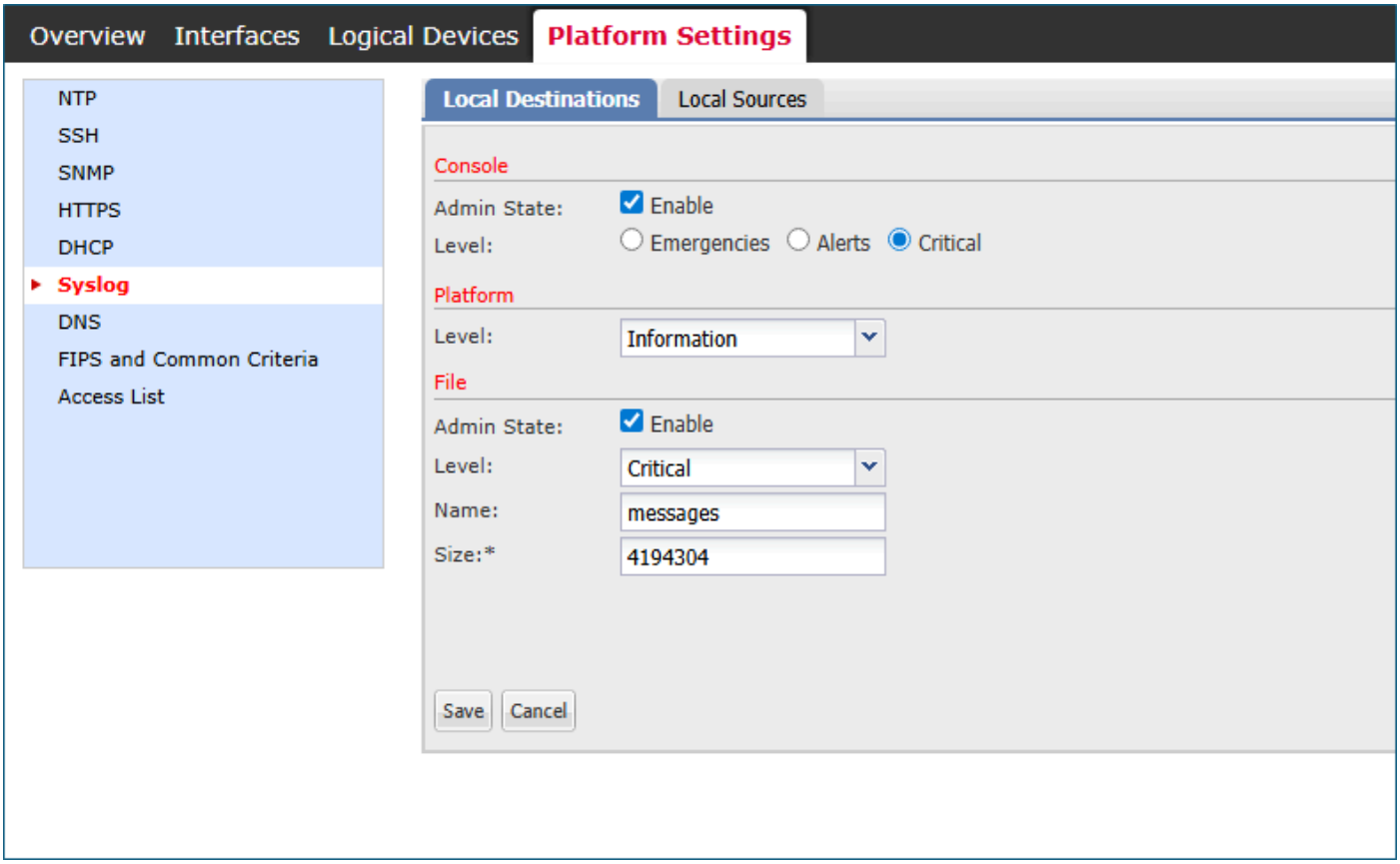
- Gleichzeitig wird in der Ausgabe des Befehls show syslog im Überwachungsbereich die IP-Adresse des Servers angezeigt:

<#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
```

- Die Benutzeroberfläche (UI) von FirePOWER Chassis Manager (FCM) > Plattformeinstellungen > Syslog gibt keine Syslog-Serverkonfiguration an.



fcm_syslogs_configuration.png

Schritt 3. Versuchen Sie, den Syslog-Server zu ändern oder zu löschen:

```
<#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
```

Die Schlussfolgerung lautet, dass weder die FXOS-CLI noch die FCM-UI eine Möglichkeit bieten, Syslog-Server zu erstellen, zu ändern oder zu löschen, einschließlich 198.51.100.100.

Ursache

Beachten Sie drei Softwarefehler:

Cisco Bug-ID CSCvn19025

Die Softwareversionen, die diesen Fehler beheben, verbieten die Remote-Syslog-Konfiguration von FXOS in der CLI oder der FCM-Benutzeroberfläche.

Cisco Bug-ID CSCvt85766

Die Behebung dieses Fehlers entfernt den Abschnitt "Remote-Ziele" aus der FXOS-Befehlsausgabe show syslog.

Versionen ohne das 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
```

Versionen mit der Fehlerbehebung enthalten keinen Abschnitt "Remote-Ziele":

<#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
```

Obwohl der Abschnitt "Remote-Ziele" fehlt, sind die Syslog-Server im Abschnitt "Plattform" sichtbar.

Cisco Bug-ID CSCwu12470

Nach dem Software-Upgrade auf die Version mit der Behebung des Cisco Bugs CSCvn19025 ist die Verwaltung von Remote-Syslog-Servern, d. h. das Erstellen, Ändern oder Löschen, in der FXOS CLI oder FCM UI nicht mehr zulässig. Diese Einschränkung gilt auch für die Server, die vor dem Upgrade konfiguriert wurden. Dennoch zeigt die FXOS-Software nach dem Software-Upgrade die Syslog-Server im Abschnitt "Plattform" der Ausgabe des Befehls show syslog an und sendet die Syslog-Meldungen an diese Server. Benutzer können die vorhandene Remote-Syslog-Konfiguration von FXOS, die in der Cisco Bug-ID CSCwu12470 nachverfolgt wird, nicht verwalten.

Verwandte Inhalte

- Cisco Bug-ID CSCvn19025

- Cisco Bug-ID CSCvt85766
- Cisco Bug-ID CSCwu12470

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.