對防火牆向先前配置的（舊版）系統日誌伺服器傳送日誌進行故障排除

目錄

問題

防火牆將系統日誌消息傳送到先前配置的IP地址為198.51.100.100的（舊版）系統日誌伺服器。此IP地址在防火牆配置中不存在。

環境

受影響的平台具體是指在平台模式下運行ASA的Firepower 2100。

解析

步驟1.查詢系統日誌消息的源IP地址：

根據對舊版系統日誌伺服器接收的消息的分析，發起方IP地址是Firepower機箱的管理IP地址。

Firepower可擴展作業系統(FXOS)中配置的IP地址為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
```

步驟2.檢查並驗證FXOS系統日誌配置：

- FXOS命令列介面(CLI)配置不包含舊版系統日誌伺服器的地址：

```
<#root>
device #

scope monitoring


device /monitoring #

show configuration | i 198.51.100.100


device /monitoring #

show configuration all | i 198.51.100.100
```

- 同時，監控範圍中show syslog命令的輸出顯示了伺服器的IP地址：

```
<#root>
device #

scope monitoring


device /monitoring #

show syslog



console
    state: Disabled
    level: Critical

platform
    state: Enabled
    level: Information
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
```

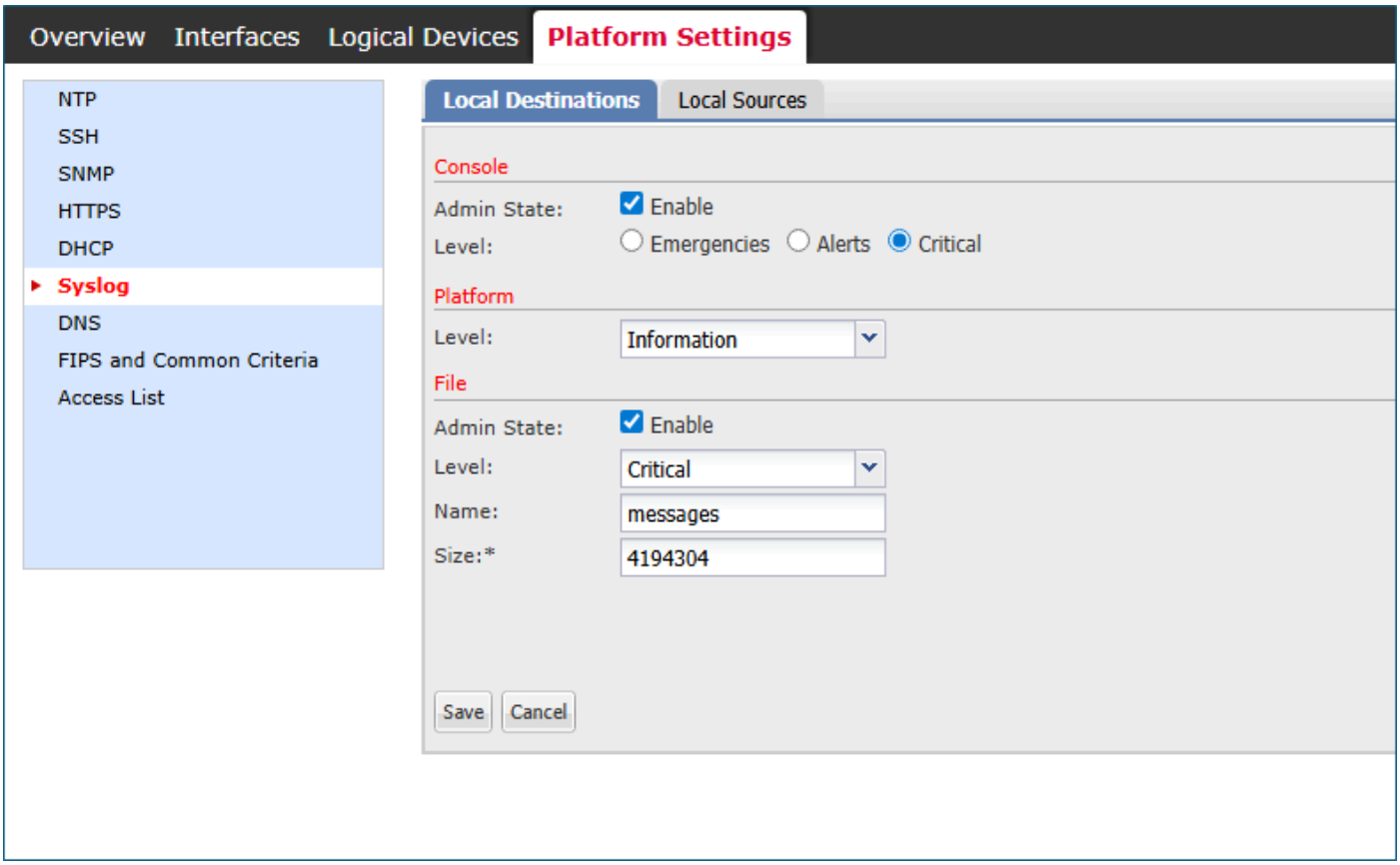
```
    Server 1 198.51.100.10        Enabled  Warnings      Local7

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機箱管理器(FCM)使用者介面(UI)> Platform Settings > Syslog不指示系統日誌伺服器配置。



fcm_syslogs_configuration.png

步驟3.嘗試修改或刪除系統日誌伺服器：

```
<#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
```

結論是，FXOS CLI和FCM UI都不提供建立、修改或刪除任何系統日誌伺服器（包括198.51.100.100）的方法。

原因

考慮三個軟體缺陷：

思科錯誤ID CSCvn19025

修正此缺陷的軟體版本不允許在CLI或FCM UI中進行FXOS遠端系統日誌配置。

思科錯誤ID CSCvt85766

此缺陷的修復程式從FXOS show syslog命令輸出中刪除「遠端目標」部分。

沒有修正程式的版本：

```
<#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
```

具有此修復程式的版本缺少「遠端目標」部分：

```
<#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
```

儘管缺少「遠端目標」部分，系統日誌伺服器仍可以在「平台」部分看到。

思科錯誤ID CSCwu12470

軟體升級至修正了Cisco錯誤ID CSCvn19025的版本後，在FXOS CLI或FCM UI中不允許管理遠端系統日誌伺服器，即建立、修改或刪除。此限制也適用於升級前配置的伺服器。儘管如此，在軟體升級後，FXOS軟體在show syslog指令輸出的「平台」部分顯示syslog伺服器，並傳送syslog訊息給這些伺服器。使用者無法管理現有的FXOS遠端系統日誌配置，該配置在思科錯誤ID CSCwu12470中跟蹤。

相關內容

- 思科錯誤ID CSCvn19025
- 思科錯誤ID CSCvt85766
- 思科錯誤ID CSCwu12470

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。