对防火墙发送日志到先前配置的（传统）系统日志服务器进行故障排除

目录

问题

防火墙将系统日志消息发送到IP地址为198.51.100.100的先前配置的（传统）系统日志服务器。此IP地址在防火墙配置中不存在。

环境

受影响的平台具体是指在平台模式下运行ASA的Firepower 2100。

分辨率

步骤1.查找系统日志消息的源IP地址

根据对传统系统日志服务器接收的消息的分析，发起方IP地址是Firepower机箱的管理IP地址。

Firepower可扩展操作系统(FXOS)中配置的IP地址为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
```

步骤2.检查并检验FXOS系统日志配置

FXOS命令行界面(CLI)配置不包含旧版系统日志服务器的地址：

```
<#root>
device #

scope monitoring


device /monitoring #

show configuration | i 198.51.100.100


device /monitoring #

show configuration all | i 198.51.100.100
```

同时，监控范围中的show syslog命令的输出显示了服务器的IP地址：

```
<#root>
device #

scope monitoring


device /monitoring #

show syslog



console
    state: Disabled
    level: Critical
```

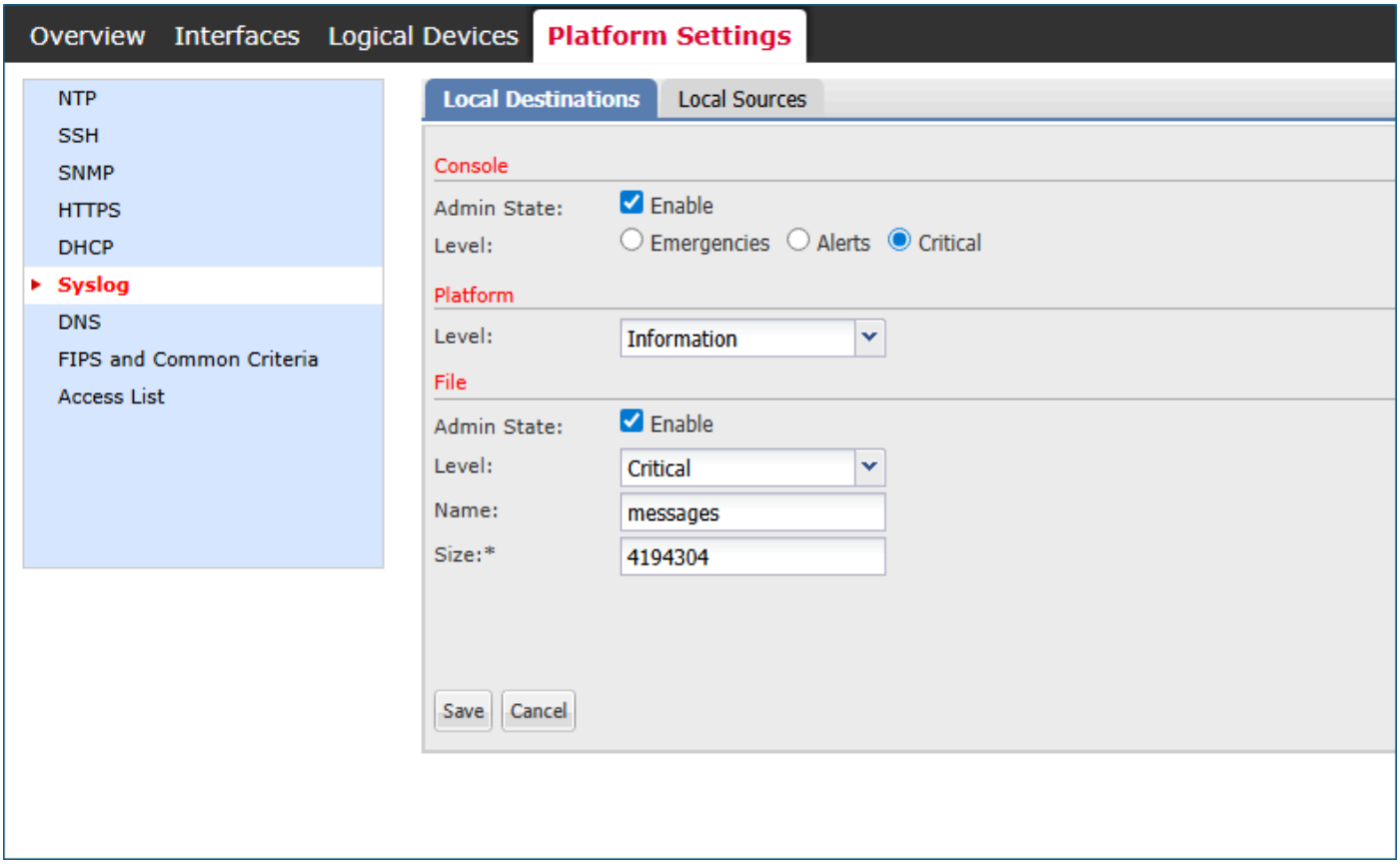
```
platform
    state: Enabled
    level: Information
    Name     Hostname              State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 198.51.100.10        Enabled  Warnings      Local7


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机箱管理器(FCM)用户界面(UI)>平台设置>Syslog不指示系统日志服务器配置：



fcm_syslogs_configuration.png

步骤3.尝试修改或删除系统日志服务器

```
<#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
```

结论是，FXOS CLI和FCM UI都不提供创建、修改或删除任何系统日志服务器（包括198.51.100.100）的方法。

原因

考虑三个软件缺陷：

思科漏洞ID CSCvn19025

带有此缺陷修复的软件版本不允许在CLI或FCM UI中进行FXOS远程系统日志配置。

Cisco Bug ID CSCvt85766

此缺陷的修复程序从FXOS show syslog命令输出中删除“remote destinations”部分。

没有修复程序的版本：

<#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
```

带有修复程序的版本缺少远程目标部分：

<#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
```

尽管缺少remote destinations部分，但platform部分中仍可以看到系统日志服务器。

思科漏洞ID CSCwu12470

在软件升级到Cisco Bug ID CSCvn19025的版本后，不允许在FXOS CLI或FCM UI中管理远程系统日志服务器，即创建、修改或删除。此限制也适用于升级前配置的服务器。尽管如此，在软件升级后，FXOS软件会在show syslog命令输出的platform部分显示syslog服务器，并将系统日志消息发送到这些服务器。用户无法管理现有的FXOS远程系统日志配置，该配置在Cisco Bug ID CSCwu12470中跟踪。

相关内容

- Cisco Bug ID CSCvn19025

- Cisco Bug ID CSCvt85766
- Cisco Bug ID CSCwu12470

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。