

在Firepower FXOS裝置上配置系統日誌

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[從FXOS使用者介面配置系統日誌\(FPR4100/FPR9300\)](#)

[從FXOS CLI配置系統日誌\(FPR4100/FPR9300\)](#)

[通過CLI驗證配置](#)

[驗證終端監控器下是否顯示系統日誌消息](#)

[驗證已配置的遠端主機的服務](#)

[驗證本地日誌檔案是否正確從FXOS記錄](#)

[生成測試系統日誌消息](#)

[Firepower 2100裝置中的FXOS系統日誌](#)

[FPR2100中的ASA邏輯裝置](#)

[FPR2100中的FTD邏輯裝置](#)

[常見問題](#)

[相關資訊](#)

簡介

本檔案介紹如何在Firepower可擴展作業系統(FXOS)裝置上配置、驗證系統日誌和對其進行故障排除。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 1個FPR4120，帶FXOS軟體版本2.2(1.70)
- 1個FPR2110，帶ASA軟體版本9.9(2)
- 1個FPR2110，帶FTD軟體版本6.2.3
- 1台系統日誌伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

從FXOS使用者介面配置系統日誌(FPR4100/FPR9300)

FXOS具有一組可從Firepower機箱管理器(FCM)啟用和配置的系統日誌消息。

步驟1.導覽至Platform Settings > Syslog。

The screenshot shows the 'Platform Settings' page with the 'Syslog' menu item selected in the left sidebar. The 'Local Destinations' tab is active, showing the configuration for 'Console' and 'Monitor'. The 'Console' section has 'Admin State' set to 'Disable' and 'Level' set to 'Critical'. The 'Monitor' section has 'Admin State' set to 'Disable' and 'Level' set to 'critical'. 'Save' and 'Cancel' buttons are visible at the bottom.

步驟2.在Local Destinations下，可以在控制檯上啟用級別0-2的系統日誌消息，或者對本地儲存的任何級別的系統日誌進行本地監控。請考慮同時顯示這兩種方法的所有選定嚴重性級別：控制檯和監控器。

The screenshot shows the same 'Platform Settings' page as in step 1, but with annotations. A red '1' points to the 'Enable' checkbox in the 'Console' 'Admin State' field, which is now checked. A red '2' points to the 'Alerts' radio button in the 'Console' 'Level' field, which is now selected. A red '3' points to the 'Save' button at the bottom of the configuration area.

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
AAA
▶ **Syslog**
DNS
FIPS and Common Criteria
Access List

Local Destinations Remote Destinations Local Sources

Console
Admin State: Enable
Level: Emergencies Alerts Critical

Monitor
Admin State: Enable
Level: errors
emergencies
alerts
critical
errors
warnings
notifications
information
debugging

Save Cancel

1 2 3

從FXOS版本2.3.1，您還可以通過GUI為系統日誌消息配置本地檔案目標：

- NTP
- SSH
- SNMP
- HTTPS
- AAA
- ▶ **Syslog**
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- Resource Profiles
- Network Control Policy
- Chassis URL

Local Destinations
Remote Destinations
Local Sources

Console

Admin State: Enable

Level: Emergencies Alerts Critical

Monitor

Admin State: Enable

Level: ▾

File

Admin State: Enable

Level: ▾

Name:

Size: *

附註： 檔案大小的大小只能介於4096和4194304位元組之間。

附註： 在2.3.1版之前的FXOS版本中，檔案配置只能通過CLI提供。

您還可以通過遠端目標頁籤配置最多3台遠端系統日誌伺服器。可以將每台伺服器定義為不同系統日誌嚴重級別消息的目標，並使用不同的本地設施進行標籤。

- NTP
- SSH
- SNMP
- HTTPS
- AAA
- ▶ **Syslog**
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- Resource Profiles
- Network Control Policy
- Chassis URL

Local Destinations
Remote Destinations
Local Sources

Server 1

Admin State: Enable

Level: Warnings ▼

Hostname/IP Address:* 10.61.161.235

Facility: Local1 ▼

Server 2

Admin State: Enable

Level: Critical ▼

Hostname/IP Address:* none

Facility: Local7 ▼

Server 3

Admin State: Enable

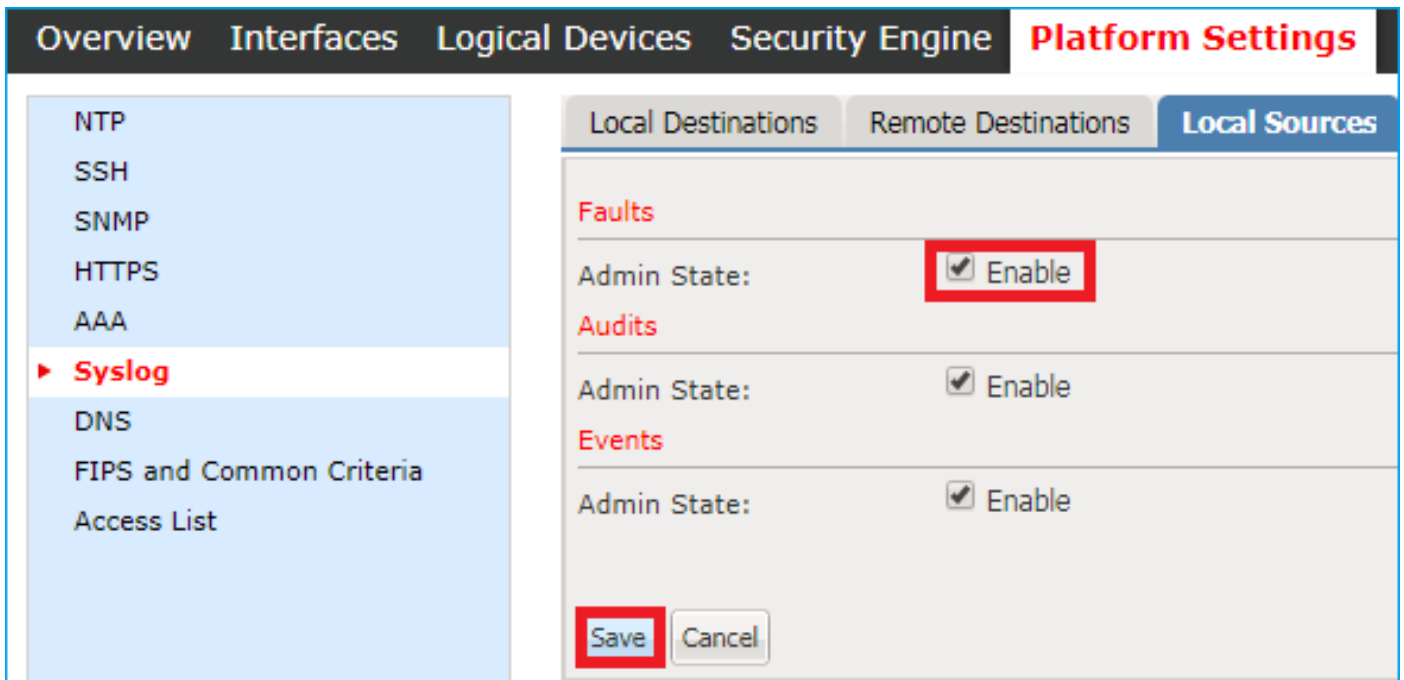
Level: Critical ▼

Hostname/IP Address:* none

Facility: Local7 ▼

Save
Cancel

步驟3.最後，為系統日誌消息選擇其他Local Sources。FXOS可用作系統日誌源故障、審計消息和/或事件。



從FXOS CLI配置系統日誌(FPR4100/FPR9300)

通過CLI配置與本地目標：

```
FP4120-A /monitoring # enable syslog console
FP4120-A /monitoring* # set syslog console level critical
FP4120-A /monitoring* # enable syslog monitor
FP4120-A /monitoring* # set syslog monitor level warning
FP4120-A /monitoring* # commit-buffer
```

通過CLI配置等效於遠端目標部分：

```
FP4120-A /monitoring # enable syslog remote-destination server-1
FP4120-A /monitoring* # set syslog remote-destination server-1 facility local1
FP4120-A /monitoring* # set syslog remote-destination server-1 level warning
FP4120-A /monitoring* # set syslog remote-destination server-1 hostname 10.61.161.235
FP4120-A /monitoring* # commit-buffer
```

通過CLI配置等效於Local Sources一節：

```
FP4120-A /monitoring # enable syslog source audits
FP4120-A /monitoring* # enable syslog source events
FP4120-A /monitoring* # enable syslog source faults
FP4120-A /monitoring* # commit-buffer
```

此外，您還可以啟用本地檔案作為系統日誌目標。可以使用命令show logging或show logging logfile顯示以下系統日誌消息：

```
FP4120-A /monitoring # enable syslog file
FP4120-A /monitoring* # set syslog file level warning
FP4120-A /monitoring* # set syslog file name Logging
FP4120-A /monitoring* # commit-buffer
```

附註：此檔案的預設大小為最大值(4194304位元組)。

通過CLI驗證配置

可以通過範圍監控驗證和配置配置：

```
FP4120-A# scope monitoring
FP4120-A /monitoring # show syslog
```

```
console
  state: Enabled
  level: Critical
```

```
monitor
  state: Enabled
  level: warning
```

```
file
  state: Enabled
  level: warning
  name: Logging
  size: 4194304
```

```
remote destinations
  Name      Hostname      State   Level      Facility
  -----
  Server 1  10.61.161.235 Enabled  warning    Local1
  Server 2  none          Disabled Critical    Local7
  Server 3  none          Disabled Critical    Local7
```

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

此外，您還可以使用show logging命令從FXOS CLI獲取更完整的輸出：

```
FP4120-A(fxos)# show logging
```

```
Logging console:          enabled (Severity: critical)
Logging monitor:         enabled (Severity: warning)
Logging linecard:        enabled (Severity: notifications)
Logging fex:              enabled (Severity: notifications)
Logging timestamp:       Seconds
Logging server:           enabled
{10.61.161.235}
  server severity:        warning
  server facility:        local1
  server VRF:             management
Logging logfile:         enabled
  Name - Logging: Severity - warning Size - 4194304
```

```
Facility      Default Severity      Current Session Severity
-----
aaa            3                      7
acllog        2                      7
```

aclmgr	3	7
afm	3	7
assoc_mgr	7	7
auth	0	7
authpriv	3	7
bcm_usd	3	7
bootvar	5	7
callhome	2	7
capability	2	7
capability	2	7
cdp	2	7
cert_enroll	2	7
cfs	3	7
clis	7	7
confcheck	2	7
copp	2	7
cron	3	7
daemon	3	7
device-alias	3	7
epp	5	7
eth_port_channel	5	7
eth_port_sec	2	7
ethpc	2	7
ethpm	5	7
evmc	5	7
fabric_start_cfg_mgr	2	7
fc2d	2	7
fcdomain	3	7
fcns	2	7
fcpc	2	7
fcs	2	7
fdmi	2	7
feature-mgr	2	7
fex	5	7
flogi	2	7
fspf	3	7
ftp	3	7
fwm	6	7
ifmgr	5	7
igmp_1	5	7
ip	3	7
ipqosmgr	4	7
ipv6	3	7
kern	3	7
l3vm	5	7
lacp	2	7
ldap	2	7
ldap	2	7
licmgr	6	7
lldp	2	7
local0	3	7
local1	3	7
local2	3	7
local3	3	7
local4	3	7
local5	3	7
local6	3	7
local7	3	7
lpr	3	7
m2rib	2	7
mail	3	7
mcm	2	7
monitor	3	7
mrrib	5	7

msh	5	7
mvsh	2	7
news	3	7
nfp	2	7
nohms	2	7
nsmgr	5	7
ntp	2	7
otm	3	7
pfstat	2	7
pim	5	5
platform	5	7
plugin	2	7
port	5	7
port-channel	5	7
port-profile	2	7
port-resources	5	7
private-vlan	3	7
qd	2	7
radius	3	7
rdl	2	7
res_mgr	5	7
rib	2	7
rlir	2	7
rpm	5	7
rscn	2	7
sal	2	7
scsi-target	2	7
securityd	3	7
smm	4	7
snmpd	2	7
span	3	7
stp	3	7
syslog	3	7
sysmgr	3	7
tacacs	3	7
u6rib	5	7
udld	5	7
urib	5	7
user	3	7
uucp	3	7
vdc_mgr	6	7
vim	5	7
vlan_mgr	2	7
vmm	5	7
vms	5	7
vntag_mgr	6	7
vsan	2	7
vshd	5	7
wwn	3	7
xmlma	3	7
zone	2	7
zschk	2	7

0(emergencies) 1(alerts) 2(critical)
3(errors) 4(warnings) 5(notifications)
6(information) 7(debugging)

2017 Nov 26 16:49:19 FP4120-5-A %\$ VDC-1 %\$ %LOCAL0-2-SYSTEM_MSG: Test-Syslog - ucssh[18553]

驗證終端監控器下是否顯示系統日誌消息

啟用系統日誌監控器後，當啟用監控終端時，系統日誌消息位於FXOS CLI下。

```

FP4120-A(fxos)# terminal monitor
2017 Nov 26 16:39:35 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1910369168]
[client 127.0.0.1:34975] AH01964: Connection to child 40 established (server 10.62.148.187:443)
- httpd[23982]
2017 Nov 26 16:39:36 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1908272016]
[client 127.0.0.1:34977] AH01964: Connection to child 42 established (server 10.62.148.187:443)
- httpd[23982]
2017 Nov 26 16:39:36 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1911417744]
(70014)End of file found: [client 127.0.0.1:34972] AH01991: SSL input filter read failed. -
httpd[23982]

```

驗證已配置的遠端主機的服務

驗證系統日誌伺服器上是否收到消息。

Date	Time	Priority	Hostname	Message
11-26-2017	16:03:03	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:46 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid
11-26-2017	16:03:03	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:46 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid
11-26-2017	16:03:01	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:44 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid

使用Ethanalyzer工具捕獲FXOS CLI上的流量，以確認Syslog消息是由FXOS生成和傳送的。

在本示例中，消息的目的地與本地Syslog伺服器(10.61.161.235)、設施標誌(Local1)和消息的嚴重性(6)匹配：

```

FP4120-A(fxos)# ethanalyzer local interface mgmt capture-filter "host 10.61.161.235 && udp port 514"
Capturing on eth0
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
2017-11-26 16:01:38.881829 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1799220112] (70014)End of file
found: [client 127.0.0.1:51015] AH01991: SSL input filter read failed. - httpd[23982]
2017-11-26 16:01:38.882574 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: Nov 26 16:01:37 %KERN-6-SYSTEM_MSG: [363494.943876] device eth0 entered
promiscuous mode - kernel
2017-11-26 16:01:38.883333 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1782442896] (70014)End of file
found: [client 127.0.0.1:51018] AH01991: SSL input filter read failed. - httpd[23982]

```

驗證本地日誌檔案是否正確從FXOS記錄

```

FP4120-A(fxos)# show logging logfile
2017 Nov 26 15:20:22 FP4120-5-A %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by
user
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: Semaphore lock success - aaad
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: accounting_sem_unlock Semaphore unlock
succeeded - aaad
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: Semaphore lock success - aaad

```

生成測試系統日誌消息

還可以通過CLI按需生成任何嚴重性的系統日誌消息，用於測試目的。這樣，在非常活躍的Syslog伺服器中，您可以定義更具體的過濾器，幫助您確認正確傳送了Syslog消息：

```
FP4120-A /monitoring # send-syslog critical Test-Syslog
```

此消息將轉發到任何系統日誌目標，在無法過濾特定系統日誌源的情況下可能有幫助：

```
FP4120-A(fxos)# show logging logfile
```

```
2017 Nov 26 16:49:19 FP4120-5-A %$ VDC-1 %$ %LOCAL0-2-SYSTEM_MSG: Test-Syslog - ucssh[18553]
```

Date	Time	Priority	Hostname	Message
11-26-2017	17:11:36	Local1.Critical	10.62.148.187	: 2017 Nov 26 16:49:19 UTC: %LOCAL0-2-SYSTEM_MSG: Testing-Syslog - ucssh[18553]

Firepower 2100裝置中的FXOS系統日誌

FPR2100中的ASA邏輯裝置

Firepower 4100/9300和帶ASA軟體的Firepower 2100裝置的系統日誌配置有兩個主要區別。

1. 在Firepower 2100中，平台日誌記錄預設啟用，無法禁用。
2. 由於FP2100平台中不存在監控終端，因此沒有監控記錄。

The screenshot shows the 'Platform Settings' configuration page for a Firepower 2100 device. The 'Local Destinations' tab is selected. On the left, a navigation menu lists various services, with 'Syslog' highlighted. The main configuration area is divided into three sections: 'Console', 'Platform', and 'File'.
- **Console:** Admin State is checked (Enable). Level is set to 'Critical' (radio buttons for Emergencies, Alerts, and Critical).
- **Platform:** Level is set to 'Information' (dropdown menu).
- **File:** Admin State is unchecked (Disable). Level is set to 'Critical' (dropdown menu). Name is 'messages' and Size is '4194304'.
At the bottom, there are 'Save' and 'Cancel' buttons.

Remote Destinations和Local Sources這兩個部分與其他平台相同。

無法通過CLI命令訪問日誌檔案和平台即時日誌。

FPR2100中的FTD邏輯裝置

在安裝了FTD裝置的FPR2100中，與其他拓撲相比，主要有2個區別：

1. 源IP地址與邏輯裝置Syslog消息所用的地址相同。
2. 所有FXOS消息均用於系統日誌ID和ASA 199013-199019通用進程的消息

```
firepower# show logging | include 1990
%ASA-6-199018: May 11 18:10:55 fp2100a port-manager: Informational: Ethernet1/12: admin state changed to down
%ASA-7-199019: May 11 18:10:55 fp2100a port-manager: LINK STATE CHANGE: port 50, new state 0/0/0
%ASA-2-199014: May 11 18:10:56 fp2100a port-manager: Alert: Ethernet1/12 link changed to DOWN
%ASA-6-199018: May 11 18:10:56 fp2100a port-manager: Informational: Ethernet1/12 speed changed to Unknown
```

在此範例中，存在介面關閉Syslog訊息。

常見問題

Syslog使用哪個預設埠？

預設情況下，系統日誌使用UDP埠514

是否可通過TCP配置系統日誌？

只有FPR2100和FTD裝置支援通過TCP的系統日誌，其中FXOS系統日誌與ASA消息整合

相關資訊

- [FXOS CLI配置指南](#)
- [技術支援與文件 - Cisco Systems](#)