

在Firepower FXOS设备上配置系统日志

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[从FXOS用户界面\(FPR4100/FPR9300\)配置系统日志](#)

[从FXOS CLI配置系统日志\(FPR4100/FPR9300\)](#)

[通过CLI验证配置](#)

[验证系统日志消息是否显示在终端监控器下](#)

[验证所配置远程主机的服务](#)

[验证本地日志文件是否正确从FXOS记录](#)

[生成测试系统日志消息](#)

[Firepower 2100设备中的FXOS系统日志](#)

[FPR2100中的ASA逻辑设备](#)

[FPR2100中的FTD逻辑设备](#)

[常见问题](#)

[相关信息](#)

简介

本文档介绍如何在Firepower可扩展操作系统(FXOS)设备上配置、验证系统日志并对其进行故障排除。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件版本：

- 1x FPR4120，带FXOS软件版本2.2(1.70)
- 1x FPR2110，带ASA软件版本9.9(2)
- 1x FPR2110，带FTD软件版本6.2.3
- 1个系统日志服务器

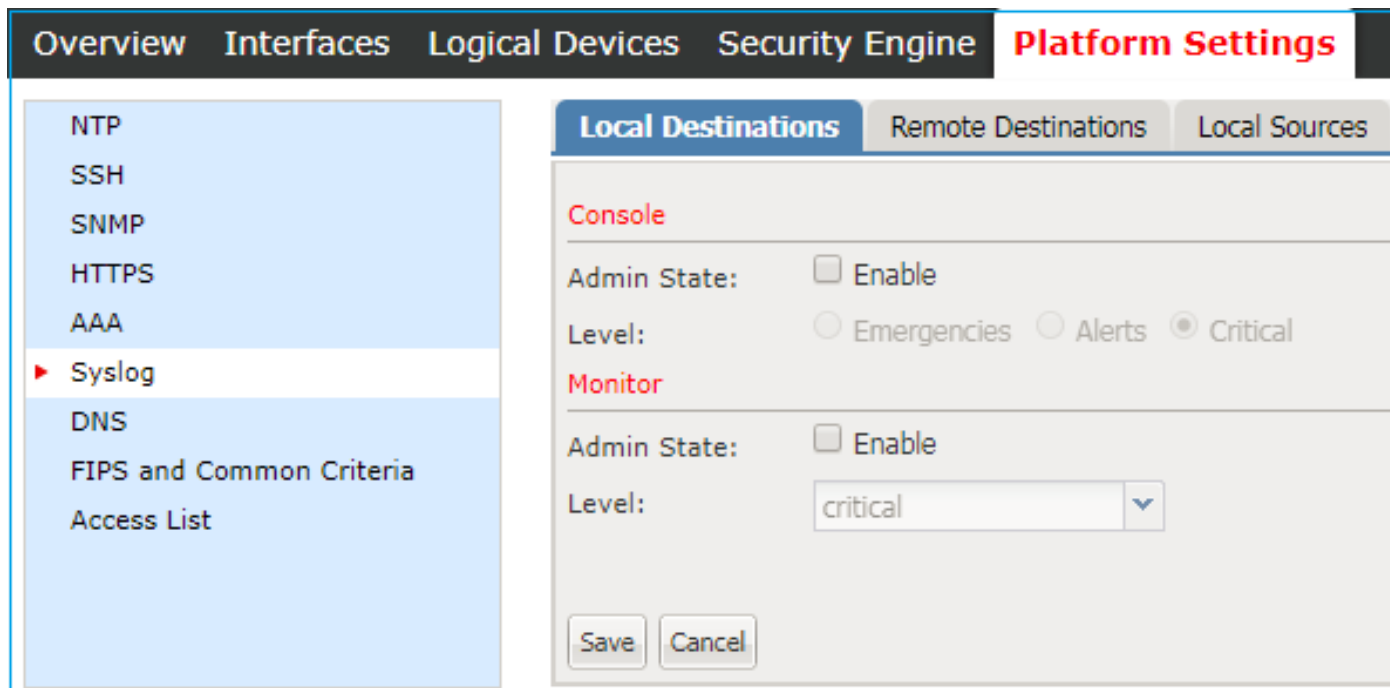
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

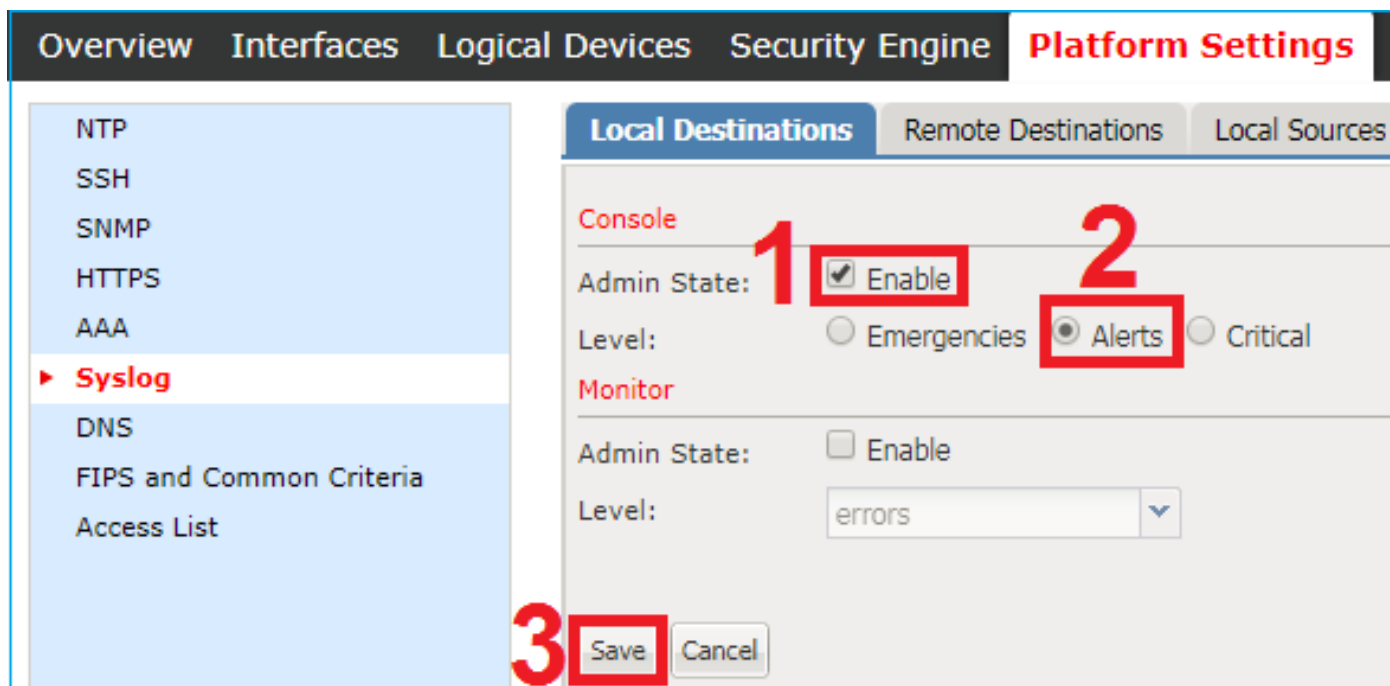
从FXOS用户界面(FPR4100/FPR9300)配置系统日志

FXOS有自己的一组系统日志消息，可从Firepower机箱管理器(FCM)启用和配置。

步骤1.导航至Platform Settings > Syslog。

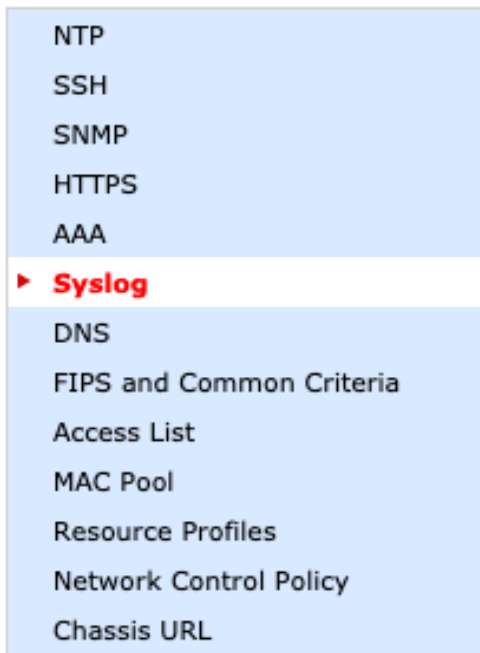


步骤2.在Local Destinations下，可以在控制台上为0-2级启用Syslog消息，或为本地存储的任何级别启用Syslog的本地监控。请考虑，为这两种方法选择的所有严重性级别也会显示：控制台和监控器。





在FXOS版本2.3.1中，您还可以通过GUI配置系统日志消息的本地文件目标：



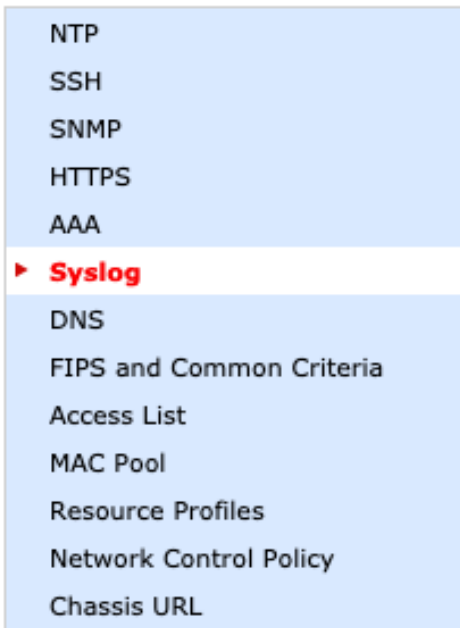
The Syslog configuration interface is shown with three tabs: Local Destinations (selected), Remote Destinations, and Local Sources. The 'Local Destinations' tab contains three sections: Console, Monitor, and File. The 'File' section is highlighted with a red border. At the bottom are 'Save' and 'Cancel' buttons.

Section	Admin State	Level	Name	Size
Console	<input checked="" type="checkbox"/> Enable	<input type="radio"/> Emergencies <input type="radio"/> Alerts <input checked="" type="radio"/> Critical		
Monitor	<input checked="" type="checkbox"/> Enable	Warnings		
File	<input checked="" type="checkbox"/> Enable	Warnings	Logging	4194304

注意：文件大小的大小只能介于4096和4194304字节之间。

注意：在2.3.1之前的FXOS版本中，文件配置仅通过CLI提供。

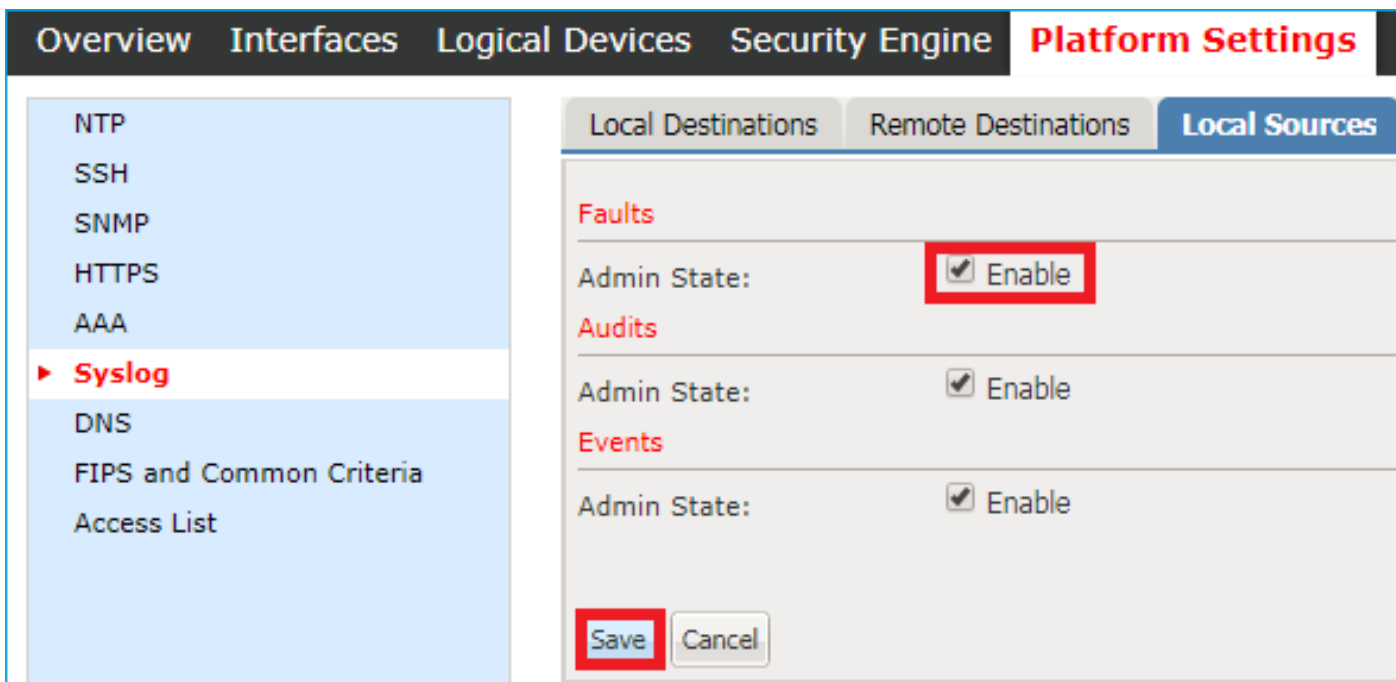
您还可以从Remote Destinations选项卡配置最多3个远程系统日志服务器。每台服务器都可以定义为不同系统日志严重性级别消息的目标，并使用不同的本地设施进行标记。



The main configuration area for Syslog Remote Destinations. It has three tabs: Local Destinations, Remote Destinations (selected), and Local Sources. There are three server configuration sections: Server 1, Server 2, and Server 3. Each section has fields for Admin State, Level, Hostname/IP Address, and Facility. Server 1 is enabled with level 'Warnings' and IP '10.61.161.235'. Server 2 is disabled with level 'Critical' and IP 'none'. Server 3 is disabled with level 'Critical' and IP 'none'. A 'Save' button is highlighted with a red box at the bottom left.

Server	Admin State	Level	Hostname/IP Address	Facility
Server 1	<input checked="" type="checkbox"/> Enable	Warnings	10.61.161.235	Local1
Server 2	<input type="checkbox"/> Enable	Critical	none	Local7
Server 3	<input type="checkbox"/> Enable	Critical	none	Local7

步骤3.最后，为系统日志消息选择其他本地源。FXOS可用作系统日志源故障、审核消息和/或事件。



从FXOS CLI配置系统日志(FPR4100/FPR9300)

通过CLI配置与“本地目标：”一节等效的配置

```
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
```

通过CLI配置与“远程目标：”一节相同的内容

```
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
```

通过CLI配置与Local Sources部分相同的：

```
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，您可以将本地文件启用为系统日志目标。使用命令show logging或show logging logfile可以显示以下系统日志消息：

```
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
```

注意：此文件的默认大小是最大值(4194304字节)。

通过CLI验证配置

可以从范围监控验证和配置：

```
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，您还可以使用show logging命令从FXOS CLI获得更完整的输出：

```
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]

验证系统日志消息是否显示在终端监控器下

启用系统日志监控器后，当启用监控终端时，系统日志消息在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]

```

验证所配置远程主机的服务

验证系统日志服务器上是否收到消息。

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工具在FXOS CLI上捕获流量，以确认FXOS生成并发送系统日志消息。

在本示例中，消息的目标与本地系统日志服务器(10.61.161.235)、设施标志(Local1)和消息的严重性(6)匹配：

```

FP4120-A(fxos)# ethanalyzer local interface mgmt capture-filter "host 10.61.161.235 && udp port 514"
Capturing on eth0
wiresnark-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]

```

验证本地日志文件是否正确从FXOS记录

```

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

```

生成测试系统日志消息

此外，还可以选择通过CLI按需生成任何严重性的系统日志消息，以用于测试目的。这样，在非常活跃的系统日志服务器中，您可以定义一个更具体的过滤器，以帮助您确认系统日志消息已正确发送：

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

此消息将转发到任何系统日志目标，在无法过滤特定系统日志源的情况下非常有用：

```
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设备中的FXOS系统日志

FPR2100中的ASA逻辑设备

Firepower 4100/9300和Firepower 2100设备的系统日志配置与使用ASA软件的设备之间有两个主要区别。

1. 在Firepower 2100中，平台日志记录默认启用，无法禁用。
2. 由于FP2100平台中不存在监控终端，因此没有监控日志记录。

The screenshot shows the 'Platform Settings' configuration page. On the left, a navigation menu includes 'NTP', 'SSH', 'SNMP', 'HTTPS', 'DHCP', 'Syslog' (highlighted), 'DNS', 'FIPS and Common Criteria', and 'Access List'. The main area is divided into 'Local Destinations' and 'Remote Destinations' tabs. Under 'Local Destinations', there are three sections: 'Console', 'Platform', and 'File'. The 'Console' section has 'Admin State' checked and 'Level' set to 'Critical'. The 'Platform' section has 'Level' set to 'Information'. The 'File' section has 'Admin State' unchecked, 'Level' set to 'Critical', 'Name' set to 'messages', and 'Size' set to '4194304'. 'Save' and 'Cancel' buttons are at the bottom.

“远程目标”和“本地源”部分都与其他平台相同。

日志文件和平台实时日志无法通过CLI命令访问。

FPR2100中的FTD逻辑设备

在安装FTD设备的FPR2100中，与其他拓扑相比有2个主要区别：

1. 源IP地址与逻辑设备系统日志消息所用的地址相同。
2. 所有FXOS消息都用于ASA 199013-199019通用进程的系统日志ID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
```

在本例中，有接口关闭系统日志消息。

常见问题

系统日志使用哪个默认端口？

默认情况下，系统日志使用UDP端口514

您能否通过TCP配置系统日志？

FPR2100和FTD设备仅支持通过TCP的系统日志，其中FXOS系统日志与ASA消息集成

相关信息

- [FXOS CLI配置指南](#)
- [技术支持和文档 - Cisco Systems](#)