配置在Firepower FXO工具上的Syslog

Contents

Introduction

本文描述如何配置，验证和排除在Firepower可扩展操作系统的(FXO)工具上的Syslog故障。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于以下软件版本：

- 与FXO软件版本2.2(1.70)的1x FPR4120
- 与ASA软件版本的1x FPR2110 9.9(2)
- 与FTD软件版本6.2.3的1x FPR2110
- 1x系统日志服务器

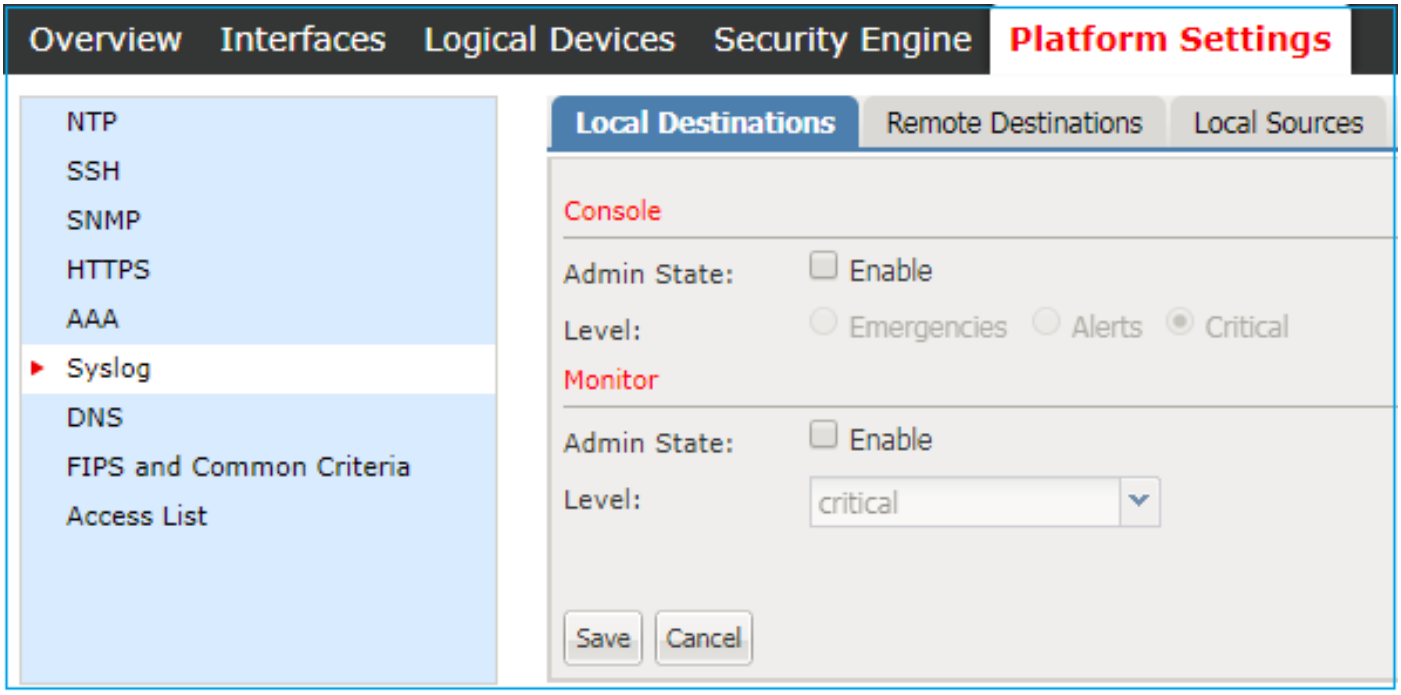
The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.如果您的网络实际，请保证您了解所有命令的潜在影响。

Configure

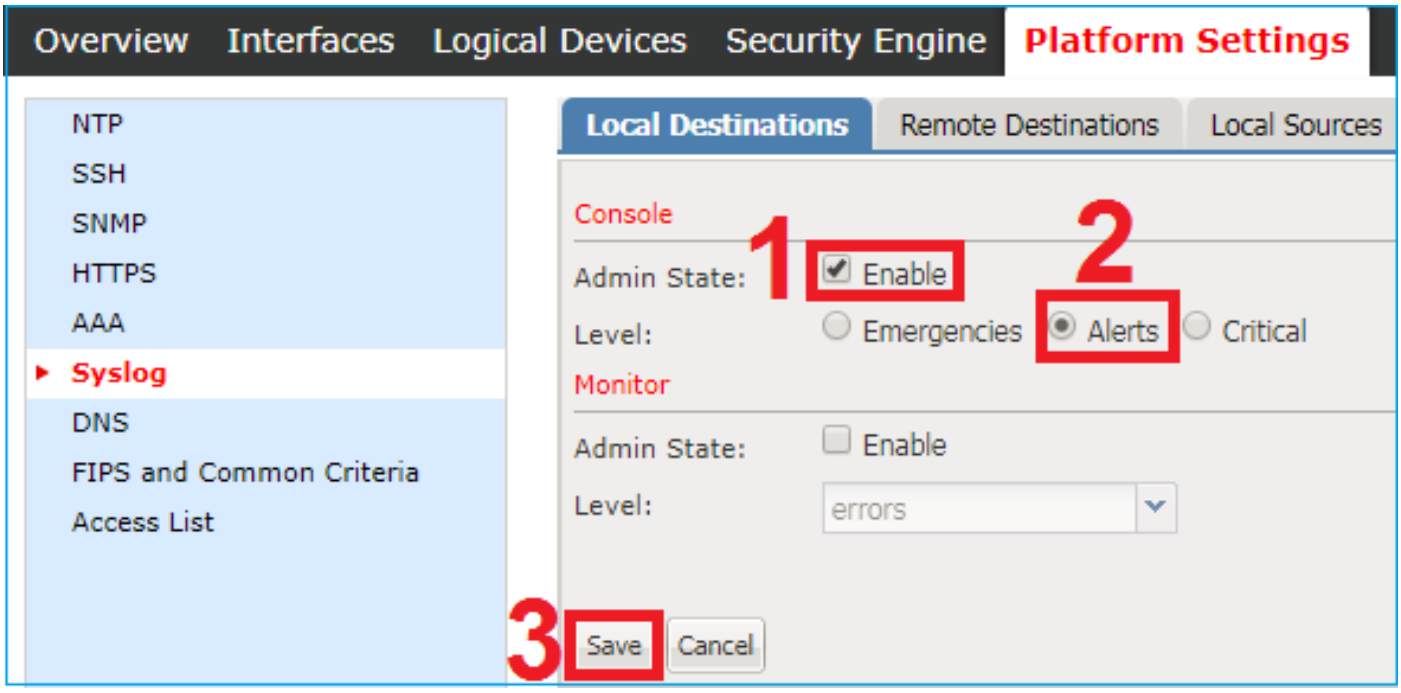
配置从FXO用户界面(FPR4100/FPR9300)的Syslog

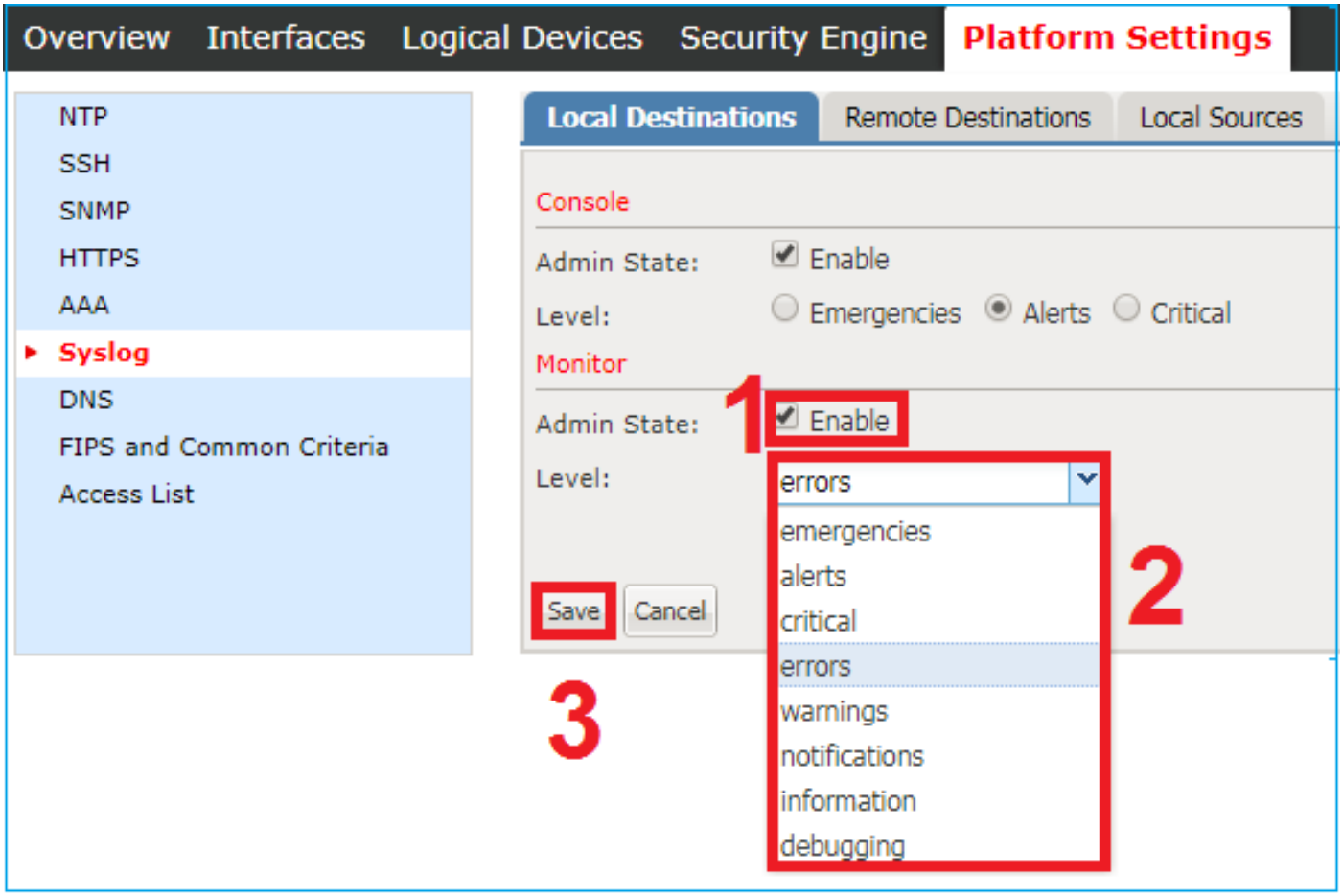
FXO有可以是启用和配置从Firepower机箱管理器的其自己的套系统消息(FCM)。

步骤1.连接对**平台设置> Syslog。**

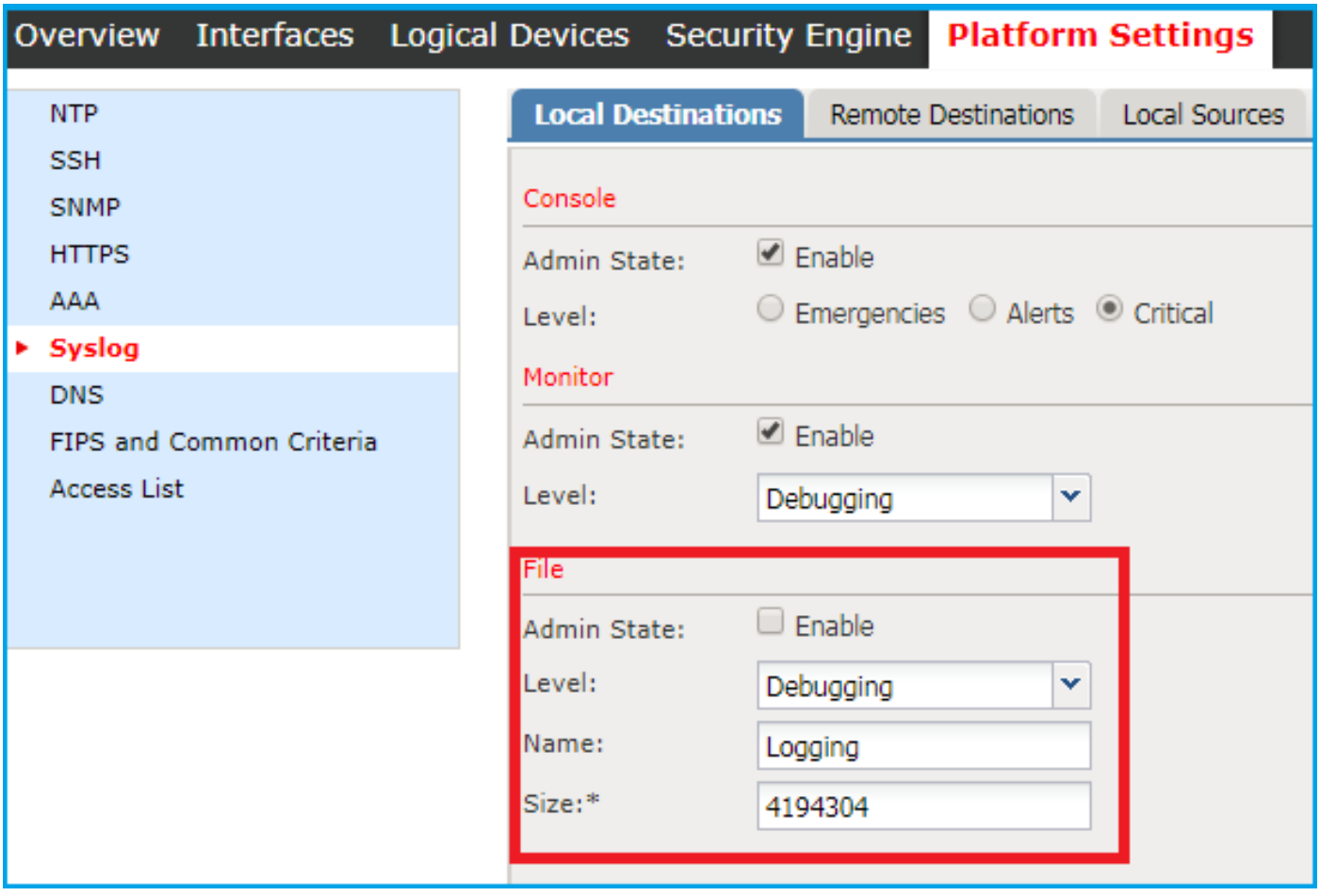


Step 2.在**本地目的地**，您下能在控制台的enable (event)系统消息级别的0-2或Syslog本地监控存储的所有级别的本地。考虑在也所选的那个上的所有告警级别为两个方法显示：控制台和监控程序。





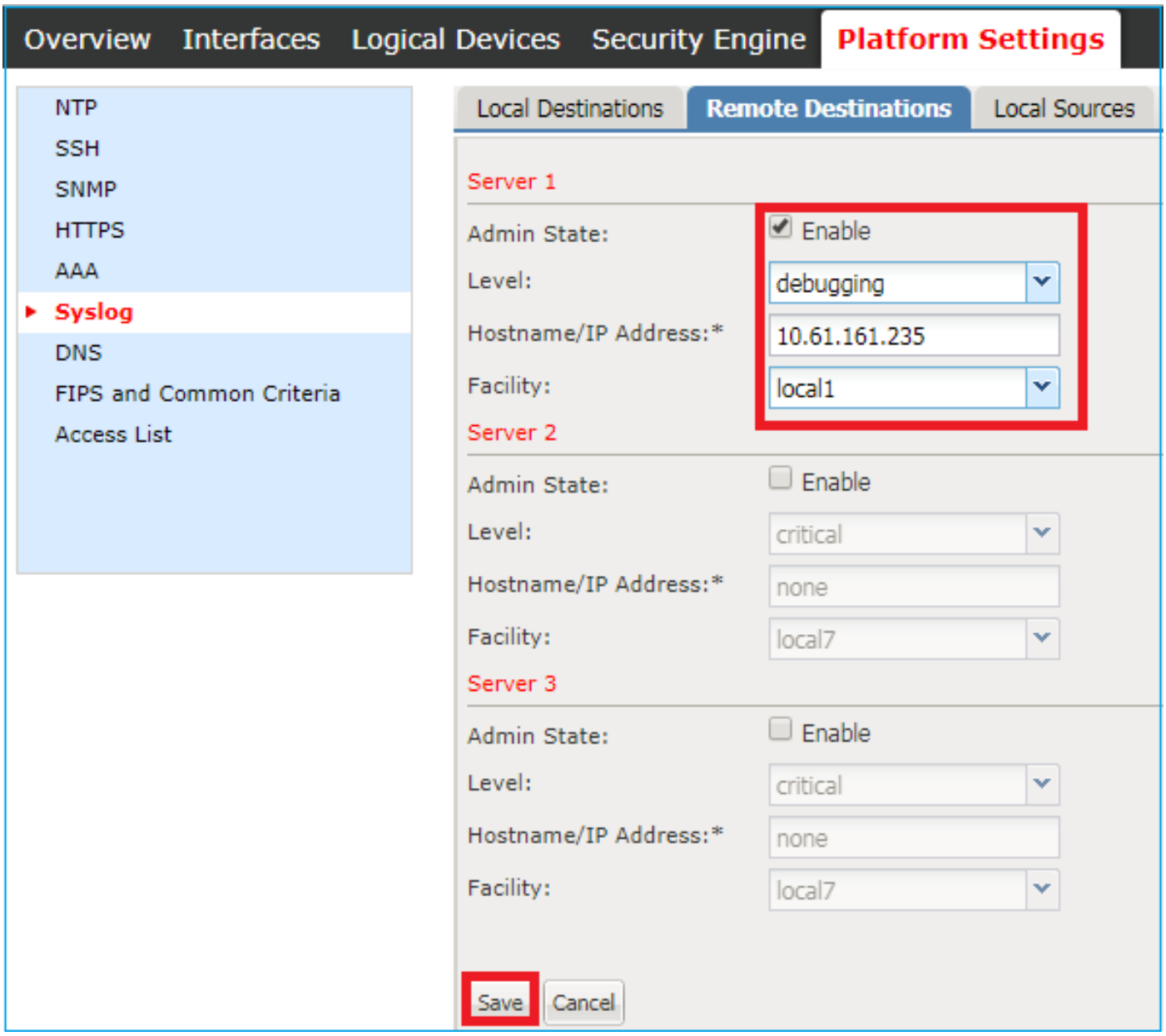
从FXO版本2.3.1您能通过GUI也配置系统消息的一个本地文件目的地：



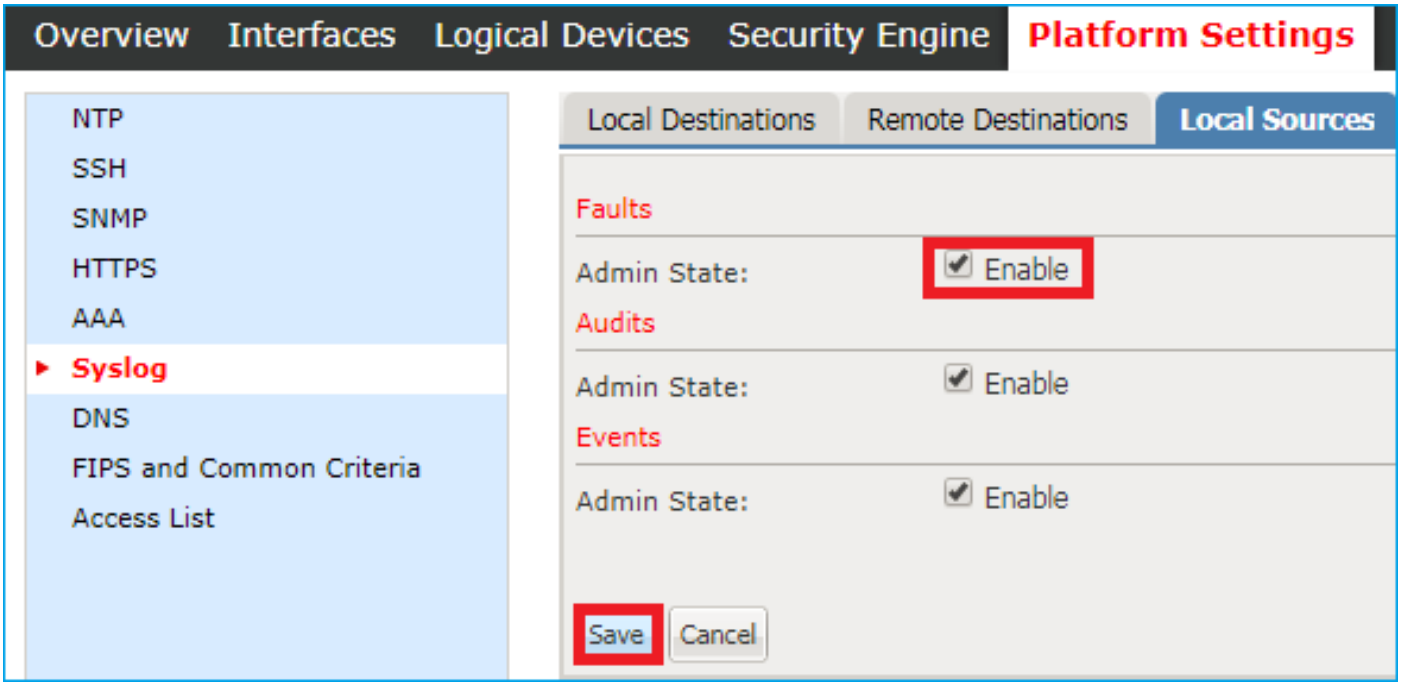
Note:文件大小能只有在4096个和4194304个字节之间的大小。

Note:在pre-2.3.1 FXO版本中文件配置通过CLI是仅可用的。

您能也配置从**远端目的地**选项的3个远程系统日志服务器。每个服务器可以被定义作为不同的系统日志严重性级别级别消息的一个目的地和标记与不同的本地设备。



步骤3.最后，系统消息的挑选另外的**本地来源**。FXO能使用作为Syslog来源故障，审计消息和事件。



配置从FXO CLI (FPR4100/FPR9300)的Syslog

通过CLI配置部分**本地目的地**等同：

```
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 debugging
FP4120-A /monitoring* # commit-buffer
```

通过CLI配置部分**远端目的地**等同：

```
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 debugging
FP4120-A /monitoring* # set syslog remote-destination server-1 hostname 10.61.161.235
FP4120-A /monitoring* # commit-buffer
```

通过CLI配置部分**本地来源**等同：

```
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
```

另外，您能enable (event)一个本地文件作为Syslog目的地。使用show logging命令或**show logging logfile**，这些系统消息可以**显示**：

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

Note: 此文件的默认大小最大(4194304个字节)

通过CLI验证配置

配置可以从范围**监控**被验证和被配置：

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

console
    state: Enabled
    level: Critical

monitor
    state: Enabled
    level: Debugging

file
    state: Enabled
    level: Debugging
    name:  Logging
    size:  4194304

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

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

并且，您能从FXO CLI得到更多完整输出用**show logging命令**：

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

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: notifications)
Logging fex:            enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 enabled
{10.61.161.235}
        server severity:        debugging
        server facility:        local1
        server VRF:             management
Logging logfile:                enabled
        Name - Logging: Severity - debugging 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
mrib	5	7

```
msp                   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: Testing-Syslog - ucssh[18553]
```

验证系统消息出现在终端监视器下

当Syslog监控程序是启用的时，您应该看到系统消息在FXO CLI下，当监控程序终端是启用的时。

```
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]
```

验证被配置的远端主机的服务

验证消息在系统日志服务器收到。

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

捕获在FXO CLI的数据流以Ethanalyzer工具确认生成的并且是FXO传送系统消息。

在本例中、匹配本地系统日志服务器(10.61.161.235)的消息的目的地，设备标志位(Local1)和消息(6)的严重性：

```
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]
```

验证本地日志文件从FXO正确地记录

```
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
```

测试系统消息的Generate

根据要求为了便于测试也有生成所有严重性系统消息的选项通过CLI。此方式，在非常活动系统日志服务器您能定义一台更加特定的过滤器协助解决您确认正确地传送系统消息：

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

此消息转发到所有Syslog目的地，并且可以是有用的在过滤一个特定Syslog来源不是可行的方案：

```
FP4120-A(fxos)# show logging logfile
2017 Nov 26 16:49:19 FP4120-5-A %$ VDC-1 %$ %LOCAL0-2-SYSTEM_MSG: Testing-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]

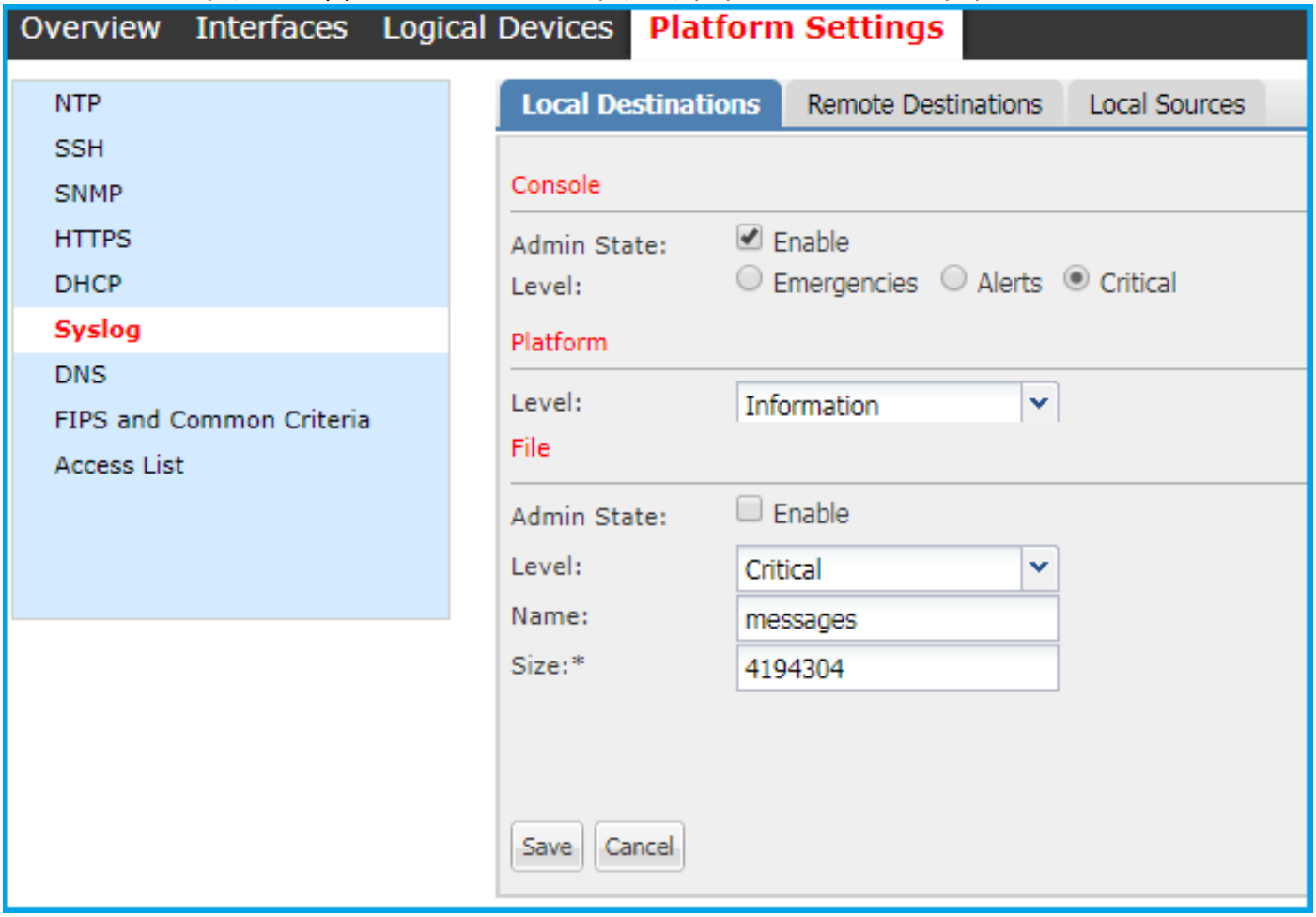
在Firepower的FXO Syslog 2100种工具

在FPR2100的ASA逻辑设备

有Syslog配置之间的两个主要区别的Firepower 4100/9300和Firepower与ASA软件的2100种工具。

1. 默认情况下在Firepower 2100平台记录被启用并且不可以是失效的。

2. 没有监控程序记录由于这样的事实监控程序终端不于FP2100平台存在。



两个，**远端目的地**和**本地来源**部分与其他平台是相同的。

日志文件和平台实际日志通过CLI命令不是可访问的。

在FPR2100的FTD逻辑设备

在FTD工具安装的FPR2100中有2个主要区别比较其他拓扑：

1. IP原地址是使用逻辑设备系统消息的相同的。

2. 所有FXO消息使用Syslog ID ASA 199013-199019的通用的进程的消息

```
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
```

在本例中，您能看到接口关闭系统消息。

FAQ

Syslog使用的默认端口是哪些？

默认情况下， Syslog使用UDP端口514

能否通过TCP配置Syslog ？

Syslog通过TCP为与FXO Syslog集成ASA消息的FTD工具的FPR2100只支持

Related Information

- FXO CLI配置指南
- Technical Support & Documentation - Cisco Systems