Configuración de Syslog en Dispositivos Firepower FXOS

Contenido

Introducción

Este documento describe cómo configurar, verificar y resolver problemas de Syslog en dispositivos FirePOWER Xtensible Operating System (FXOS).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- 1 FPR4120 con software FXOS versión 2.2(1.70)
- 1 FPR2110 con software ASA versión 9.9(2)
- 1x FPR2110 con software FTD versión 6.2.3
- 1 servidor Syslog

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. Si tiene una red

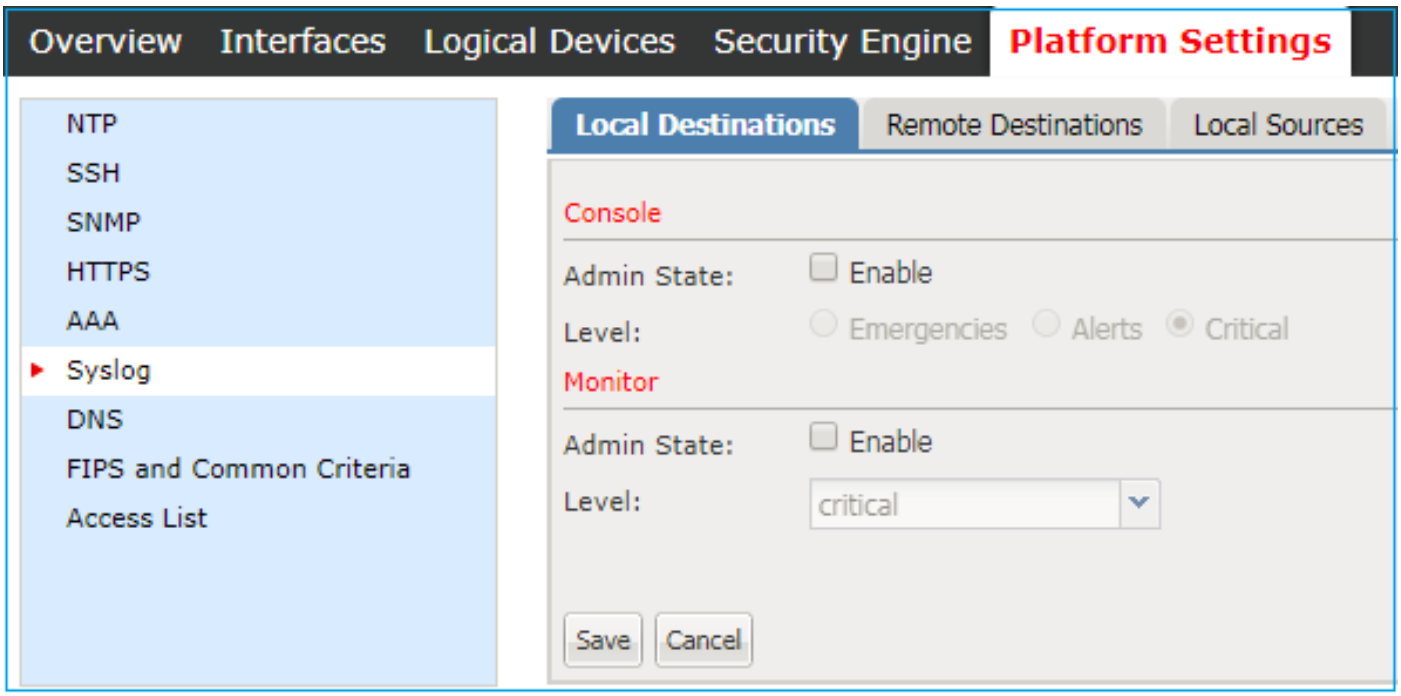
en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

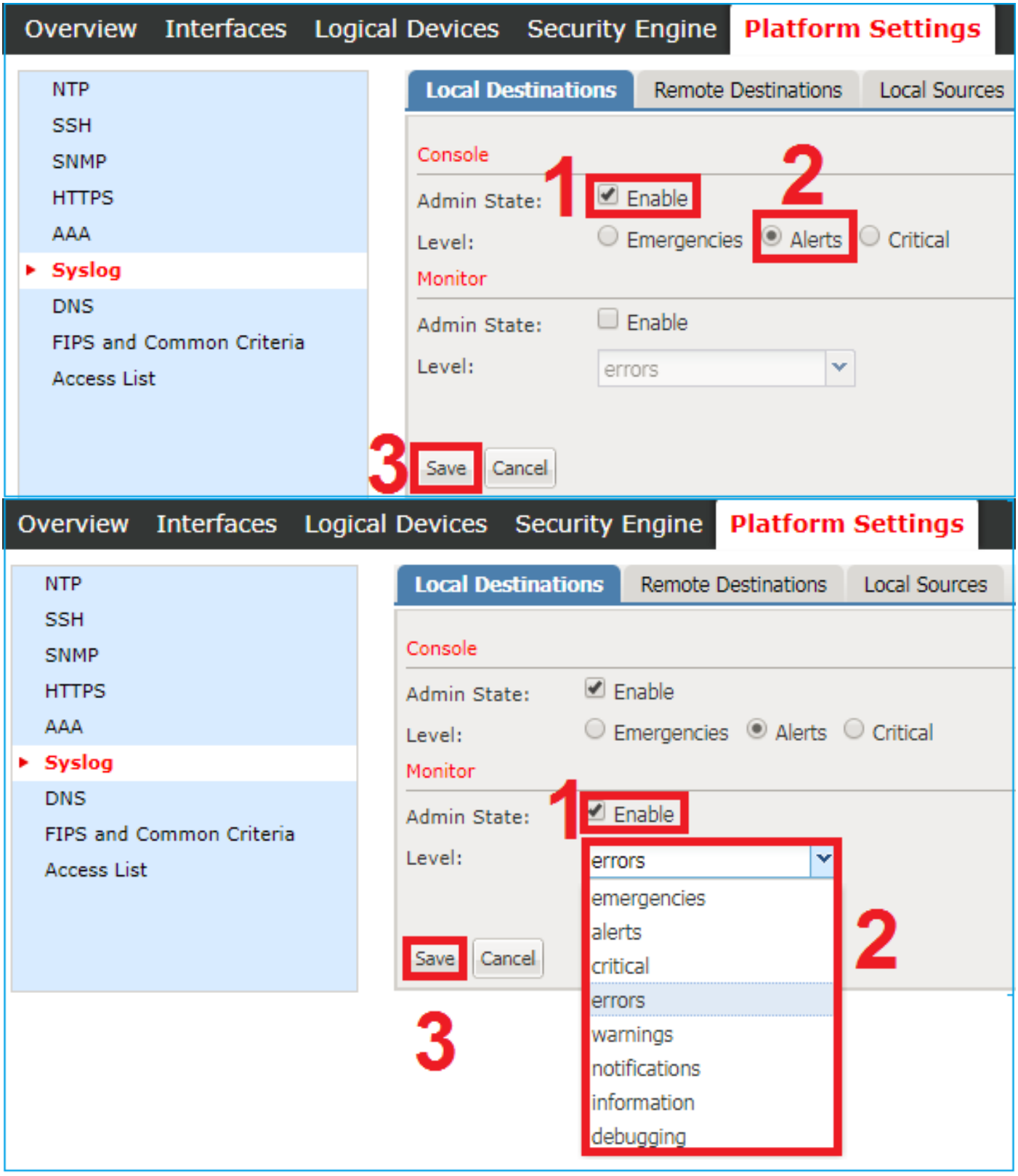
Configuración de Syslog desde la Interfaz de Usuario FXOS (FPR4100/FPR9300)

FXOS tiene su propio conjunto de mensajes Syslog que se pueden habilitar y configurar desde el Administrador de chasis de Firepower (FCM).

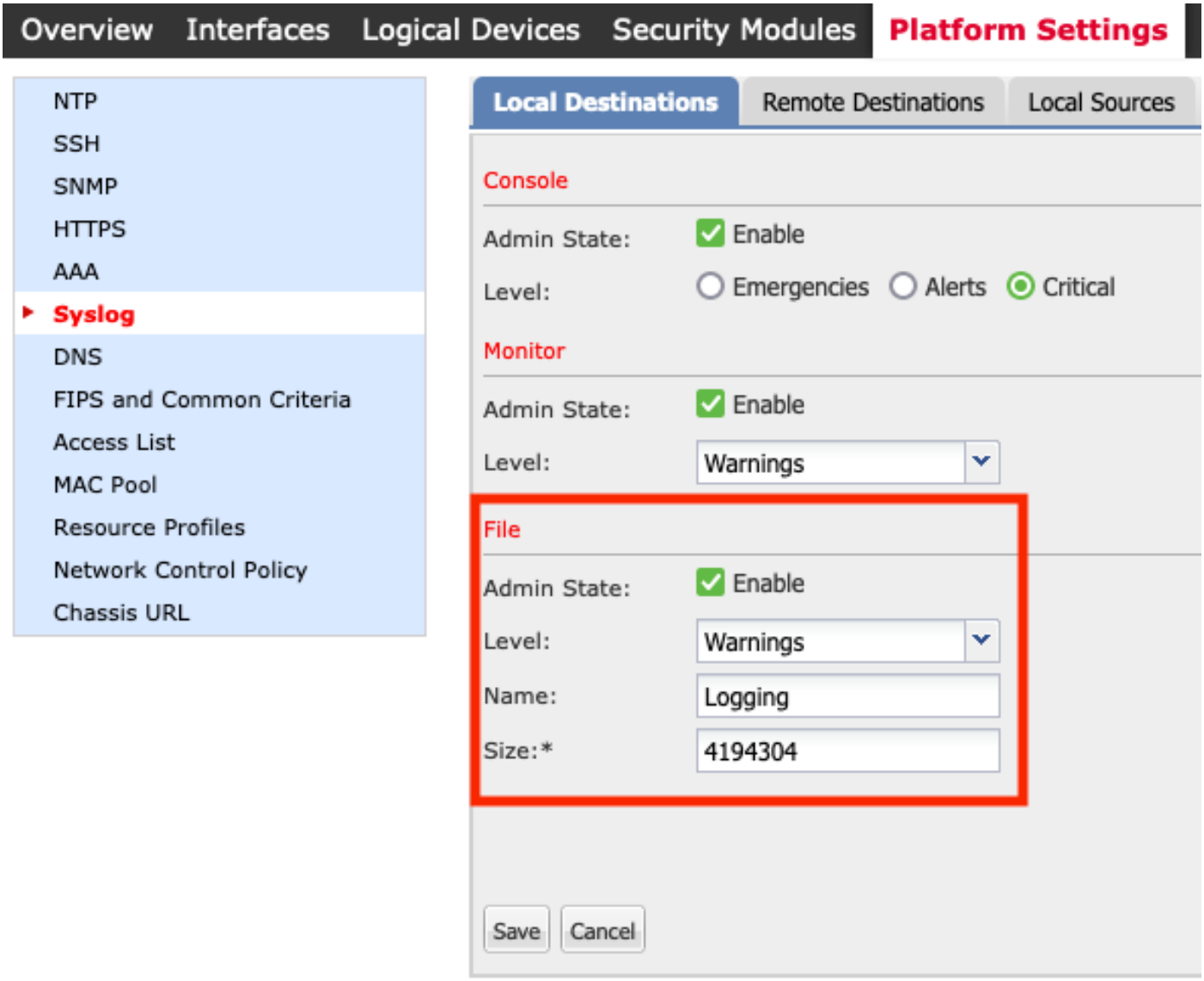
Paso 1. Vaya a **Configuración de plataforma > Syslog.**



Paso 2. En **Destinos locales**, puede habilitar los mensajes Syslog en la consola para los niveles 0-2 o la supervisión local de Syslog para cualquier nivel almacenado localmente. Tenga en cuenta que todos los niveles de gravedad seleccionados también se muestran para ambos métodos: consola y monitor.



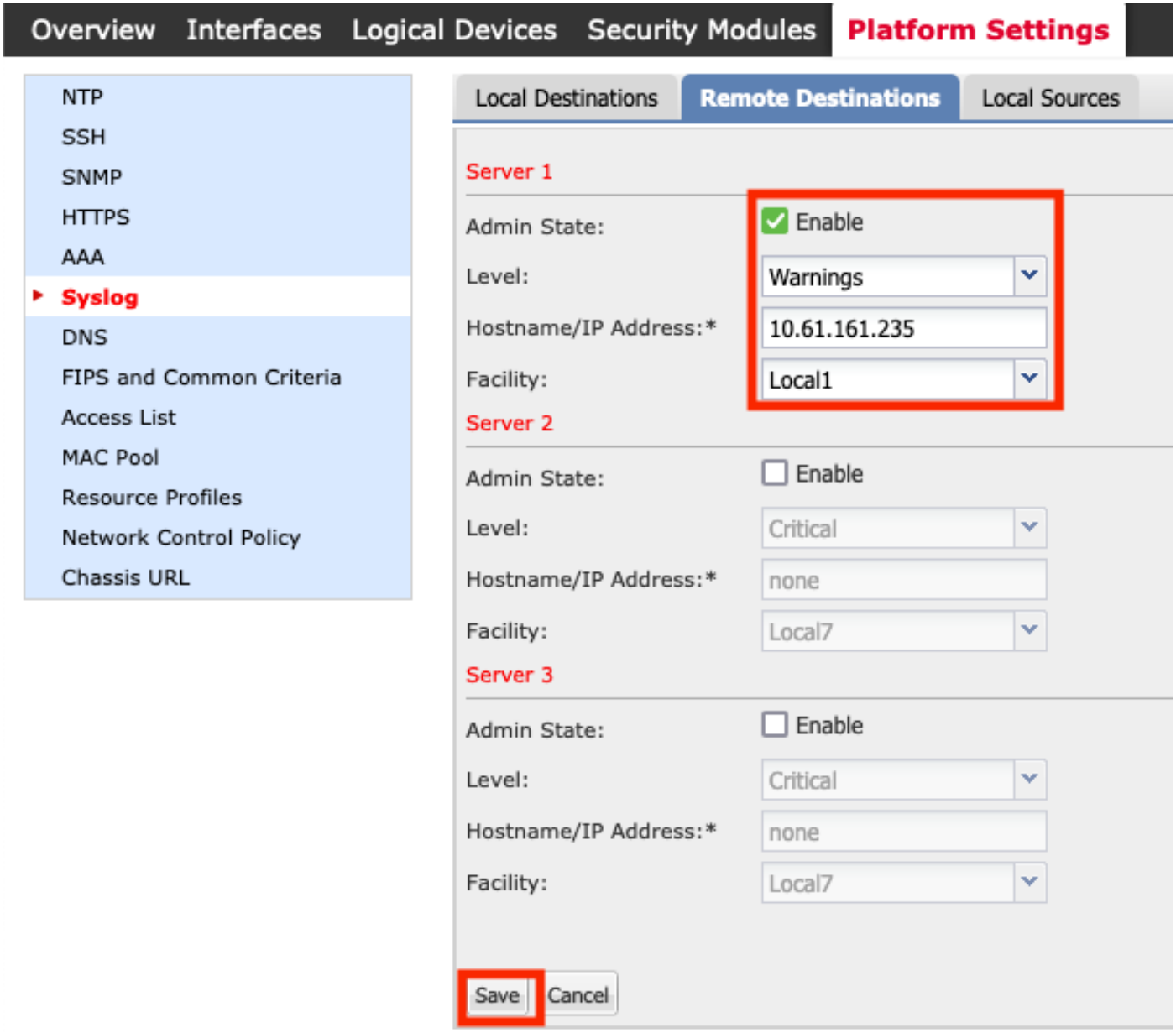
Desde FXOS versión 2.3.1 también puede configurar a través de la GUI un destino de archivo local para los mensajes Syslog:



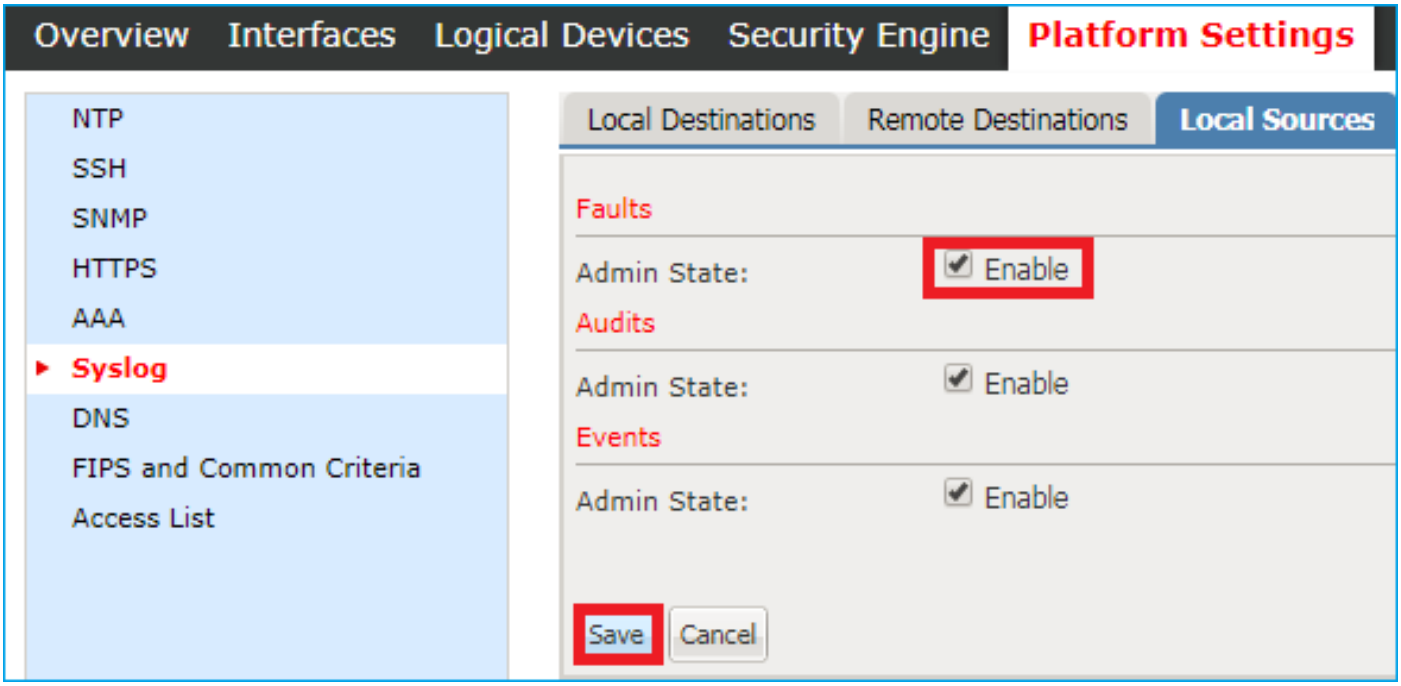
Nota: El tamaño del archivo sólo puede tener un tamaño entre 4096 y 4194304 bytes.

Nota: En la versión anterior a 2.3.1 FXOS, la configuración de archivo está disponible sólo a través de CLI.

También puede configurar hasta 3 servidores Syslog remotos desde la pestaña **Destinos Remotos**. Cada servidor se puede definir como destino para diferentes mensajes de nivel de gravedad de Syslog y marcar con una función local diferente.



Paso 3. Por último, seleccione **Orígenes locales** adicionales para los mensajes de Syslog. FXOS puede utilizarse como fallas de origen de Syslog, mensajes de auditoría y/o eventos.



Configuración de Syslog desde FXOS CLI (FPR4100/FPR9300)

Configure mediante CLI el equivalente de la sección **Destinos locales:**

```
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
```

Configure mediante CLI el equivalente de la sección **Destinos remotos**:

```
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
```

Configure mediante CLI el equivalente de la sección **Orígenes locales**:

```
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
```

Además, puede habilitar un archivo local como destino de Syslog. Estos mensajes de Syslog se pueden mostrar con el uso de los comandos **show logging** o **show logging logfile**:

```
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
```

Nota: El tamaño predeterminado de este archivo es el máximo (4194304 bytes).

Verifique la configuración mediante CLI

La configuración se puede verificar y configurar desde el **monitoreo** de alcance:

```
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
```

Además, puede obtener un resultado más completo de FXOS CLI con el comando **show logging**:

```
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
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: Test-Syslog - ucssh[18553]
```

Verifique que los Mensajes de Syslog Aparezcan en el Monitor de Terminal

Cuando el monitor Syslog está habilitado, los mensajes de Syslog se encuentran en FXOS CLI

cuando el terminal monitor está habilitado.

```
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]
```

Verificar el servicio para los hosts remotos configurados

Verifique que los mensajes se reciban en el servidor Syslog.

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

Capture el tráfico en FXOS CLI con la herramienta Ethanalyzer para confirmar que los mensajes Syslog son generados y enviados por FXOS.

En este ejemplo, el destino del mensaje coincide con el servidor Syslog local (10.61.161.235), el indicador del recurso (Local1) y la gravedad del mensaje (6):

```
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 -> 10.61.161.235Syslog 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]
```

Verifique que el archivo de registro local esté registrando correctamente desde FXOS

```
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
```

Generar mensajes Syslog de prueba

También existe la opción de generar mensajes de Syslog de cualquier gravedad a petición para fines de prueba a través de CLI. De esta manera, en servidores Syslog muy activos, puede definir un filtro más específico para ayudarle a confirmar que los mensajes de Syslog se envían correctamente:

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

Este mensaje se reenvía a cualquier destino de Syslog y puede ser útil en escenarios donde el filtrado de un origen específico de Syslog no es factible:

```
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]

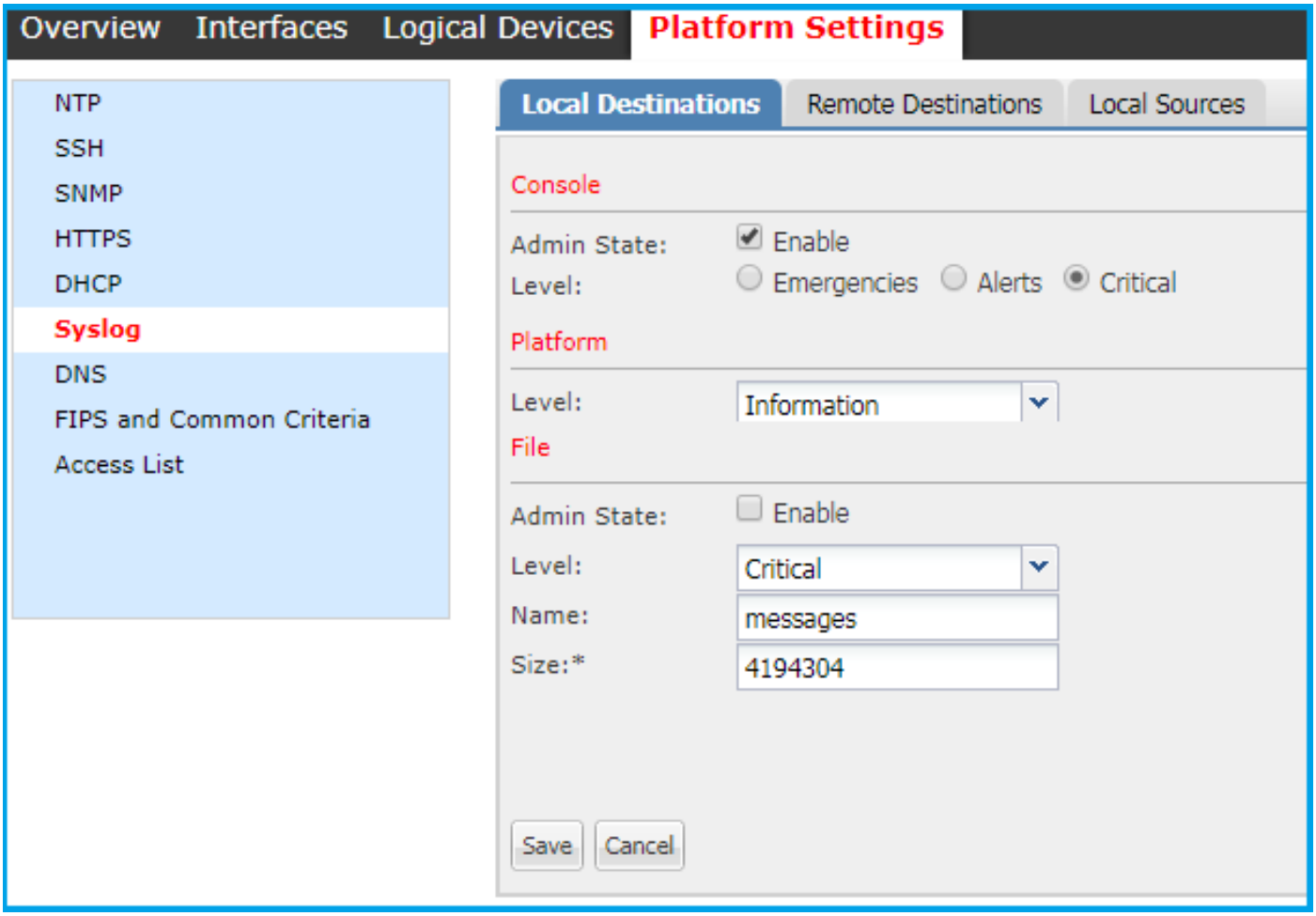
Registro del sistema FXOS en dispositivos Firepower 2100

Dispositivo lógico ASA en FPR2100

Hay dos diferencias principales entre la configuración de Syslog para los appliances Firepower 4100/9300 y Firepower 2100 con el software ASA.

1. En Firepower 2100, el registro de la plataforma se habilita de forma predeterminada y no se puede inhabilitar.

2. No hay registro del monitor debido al hecho de que el terminal del monitor no existe en las plataformas FP2100.



Ambas secciones, **Destinos Remotos** y **Orígenes Locales** son idénticas a las otras plataformas.

No se puede acceder al archivo de registro ni a los registros en vivo de la plataforma mediante comandos CLI.

Dispositivo lógico FTD en FPR2100

En FPR2100, donde se instala el dispositivo FTD, hay dos diferencias principales en comparación con las otras topologías:

1. La dirección IP de origen es la misma que se utiliza para los mensajes Syslog del dispositivo lógico.

2. Todos los mensajes FXOS se utilizan para Syslog ID el mensaje para los procesos genéricos de ASA 199013-199019

```
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
```

En este ejemplo, está la interfaz shutdown Syslog messages.

Preguntas frecuentes

¿Cuál es el puerto predeterminado utilizado por Syslog?

De forma predeterminada, Syslog utiliza el puerto UDP 514

¿Puede configurar Syslog a través de TCP?

Syslog vía TCP sólo es compatible con FPR2100 con dispositivos FTD donde los Syslogs FXOS se integran con los mensajes ASA

Información Relacionada

- Guía de Configuración de CLI de FXOS
- Soporte Técnico y Documentación - Cisco Systems