Configurazione di Syslog su appliance Firepower FXOS

Sommario

Introduzione

In questo documento viene descritto come configurare, verificare e risolvere i problemi relativi a Syslog su appliance Firepower eXtensible Operating System (FXOS).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

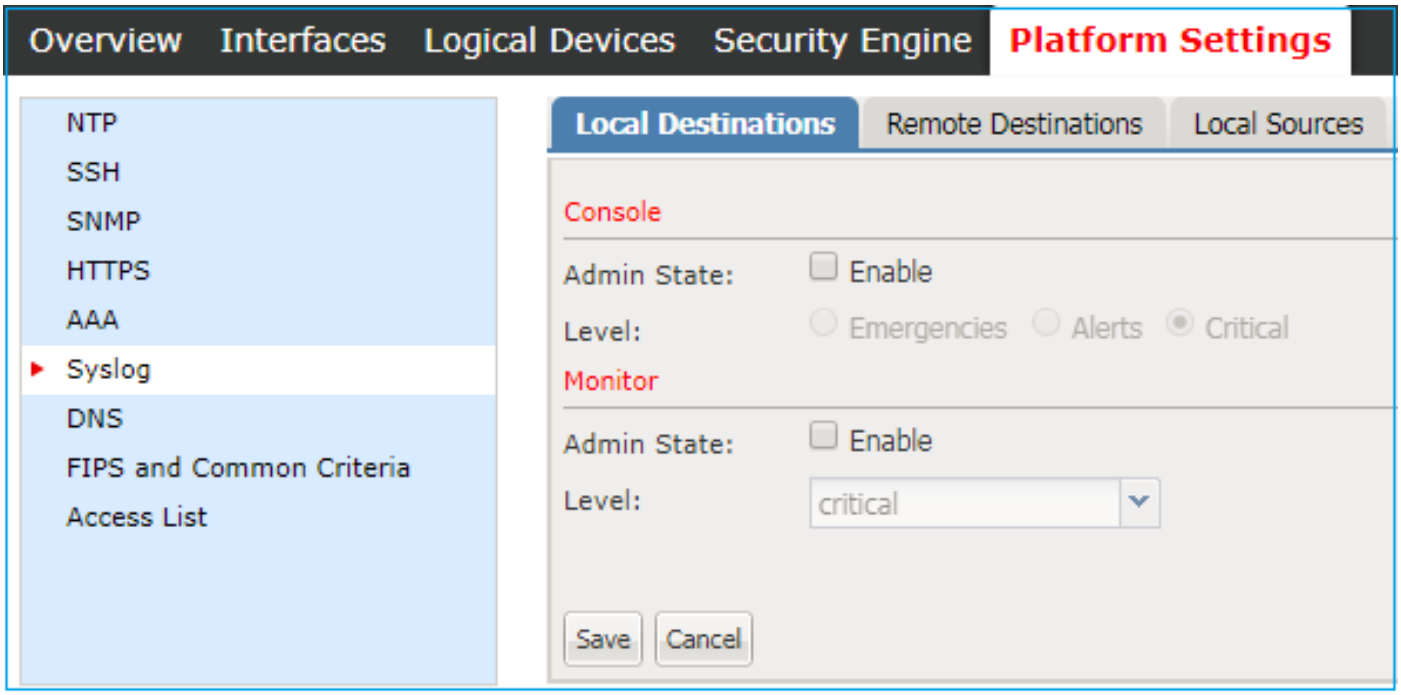
ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

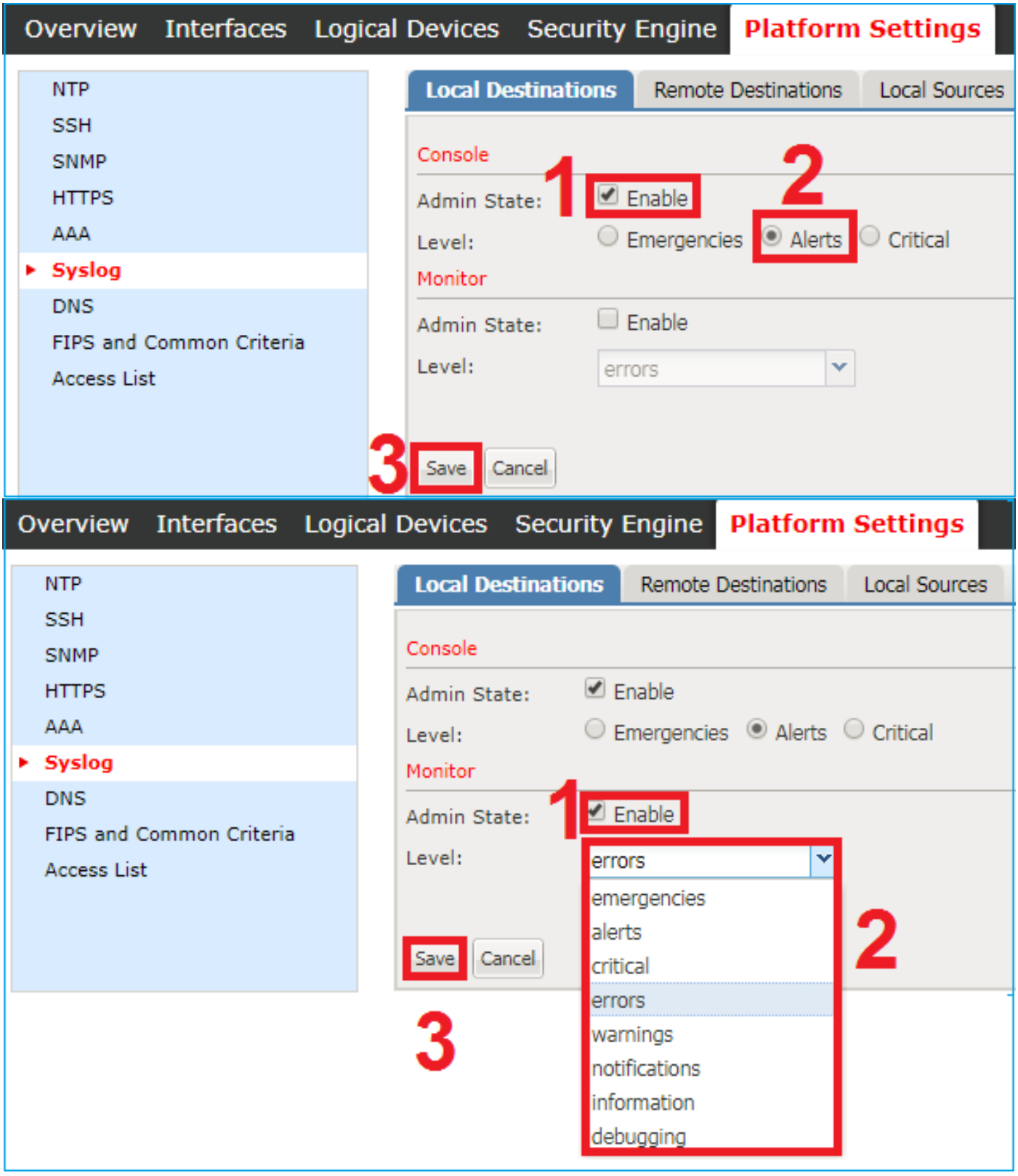
Configurazione di Syslog dall'interfaccia utente di FXOS (FPR4100/FPR9300)

FXOS dispone di un proprio set di messaggi Syslog che possono essere abilitati e configurati da Firepower Chassis Manager (FCM).

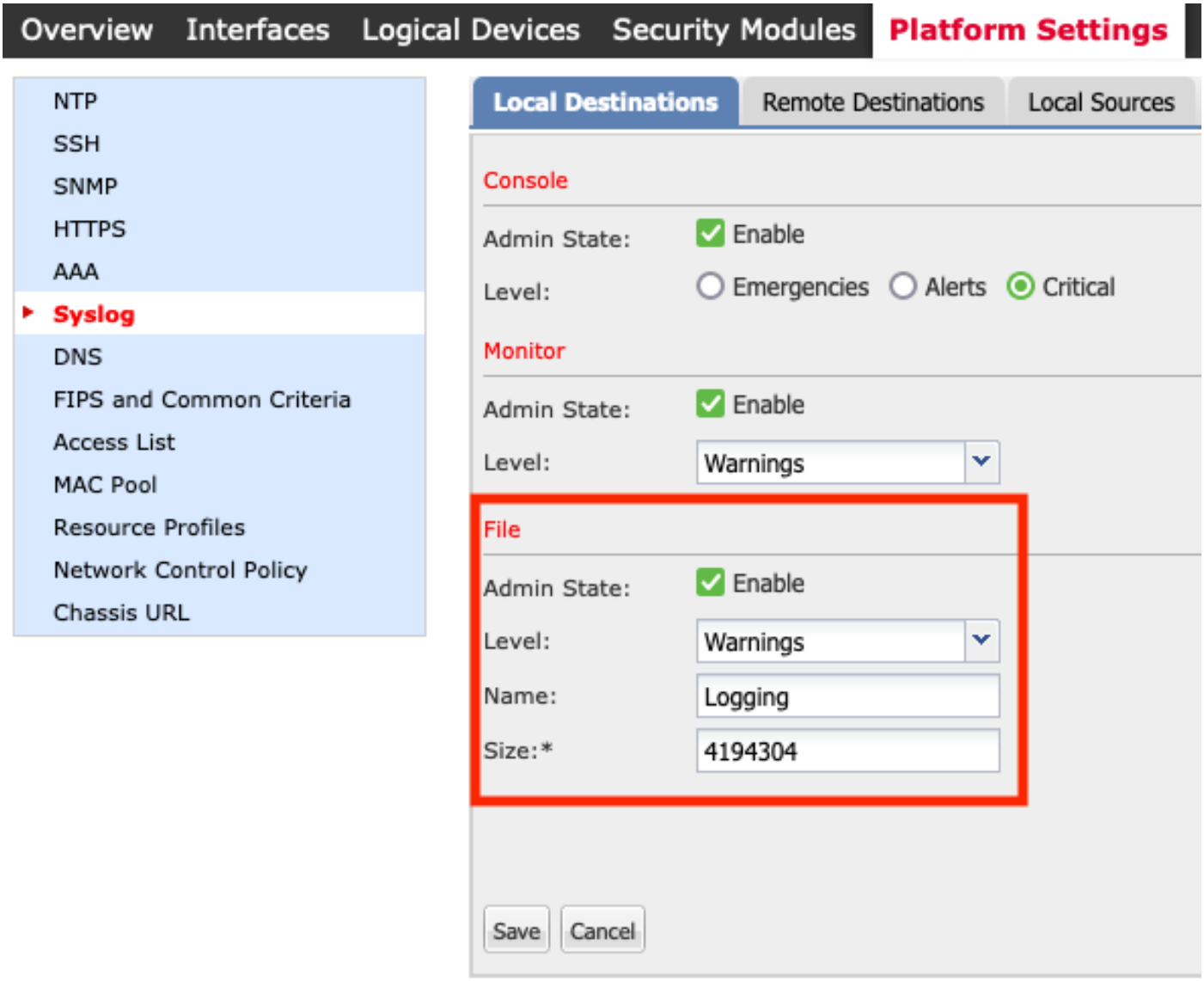
Passaggio 1. Passare a **Impostazioni piattaforma > Syslog.**



Passaggio 2. In **Destinazioni locali**, è possibile abilitare i messaggi Syslog sulla console per i livelli 0-2 o il monitoraggio locale di Syslog per qualsiasi livello archiviato localmente. Tenere presente che tutti i livelli di gravità selezionati vengono visualizzati anche per entrambi i metodi: console e monitor.



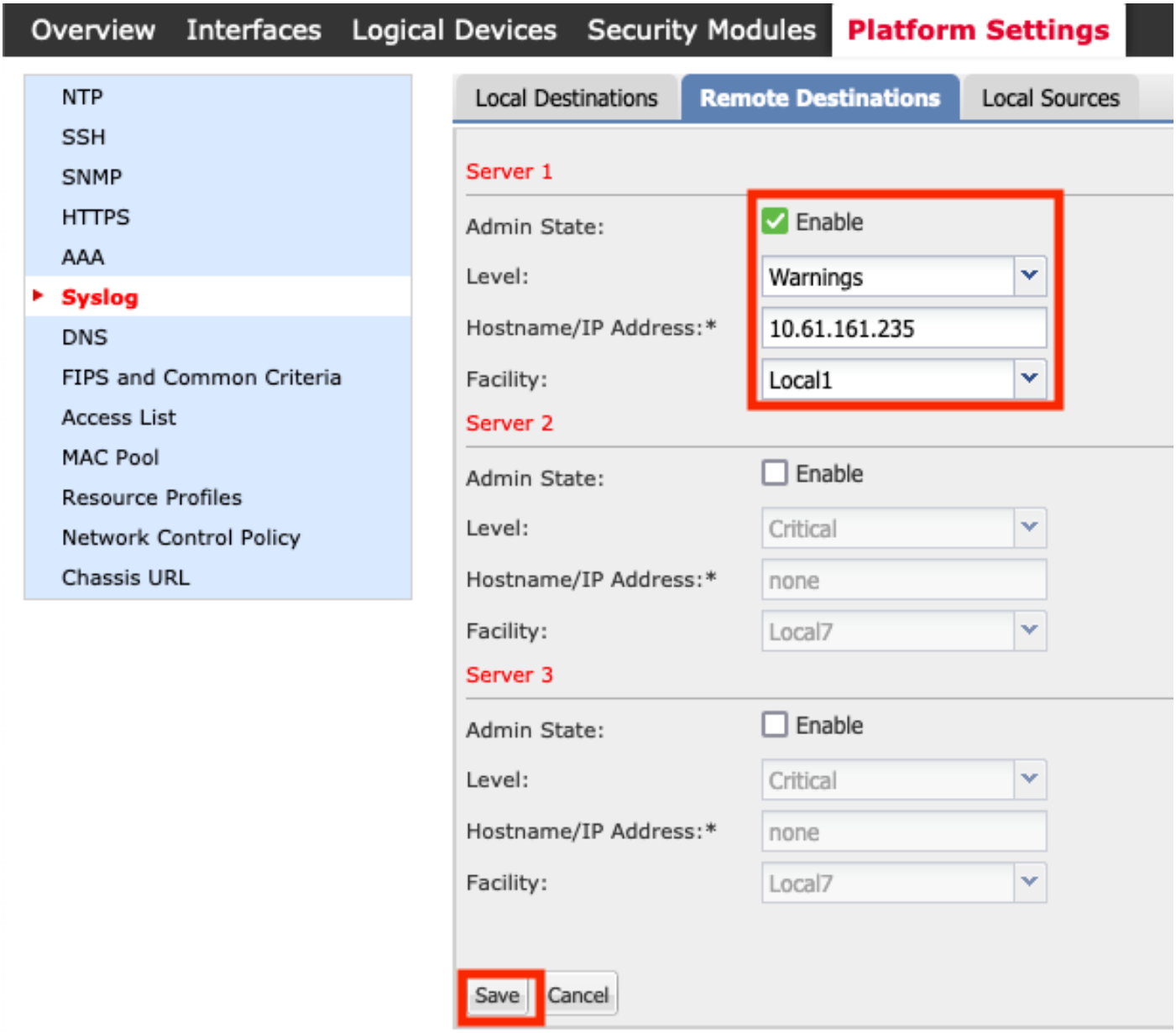
Da FXOS versione 2.3.1 è anche possibile configurare tramite GUI una destinazione locale per i messaggi Syslog:



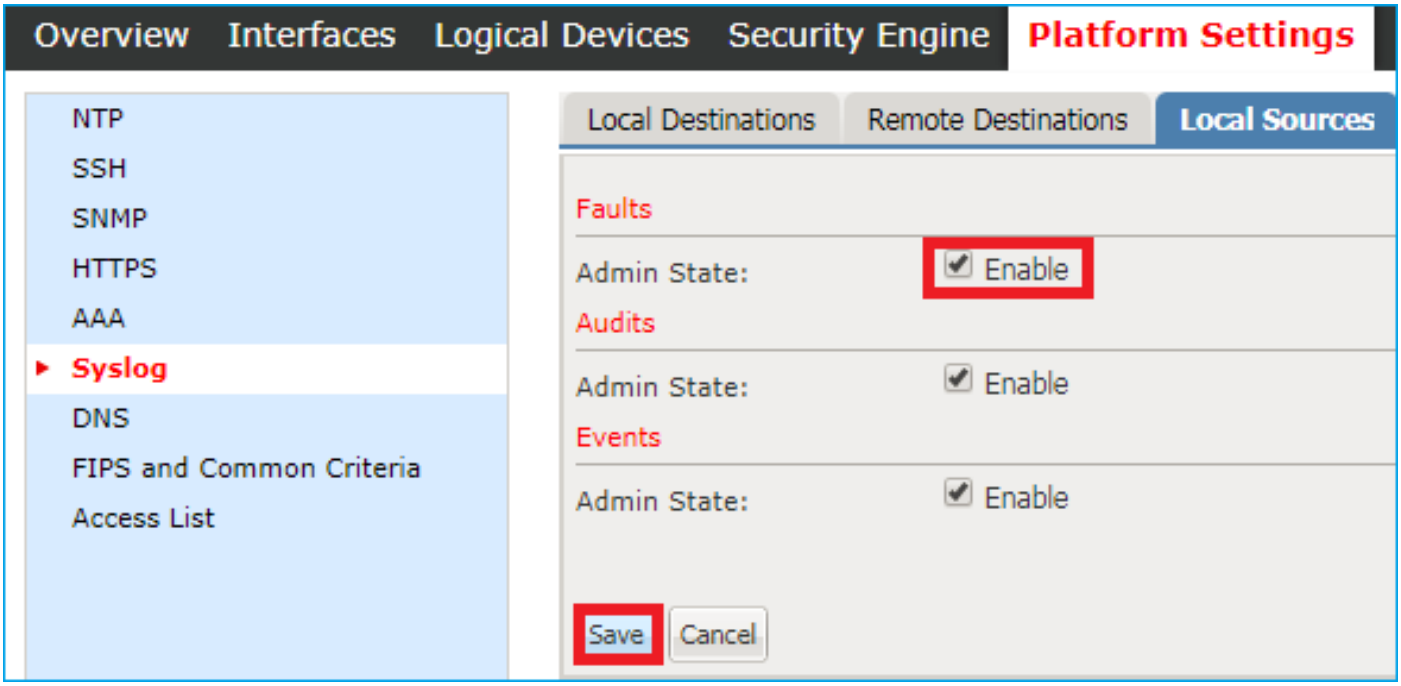
Nota: La dimensione del file può essere compresa solo tra 4096 e 4194304 byte.

Nota: Nella versione FXOS precedente alla 2.3.1, la configurazione dei file è disponibile solo dalla CLI.

Èinoltre possibile configurare fino a 3 server Syslog remoti dalla scheda **Destinazioni remote**. Ciascun server può essere definito come destinazione per messaggi con livelli di gravità diversi e contrassegnato con una struttura locale diversa.



Passaggio 3. Infine, selezionare altre **origini locali** per i messaggi Syslog. FXOS può utilizzare come origine Syslog errori, messaggi di controllo e/o eventi.



Configurazione di Syslog dalla CLI di FXOS (FPR4100/FPR9300)

Configurare tramite CLI l'equivalente della sezione **Destinazioni locali:**

```
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
```

Configurare tramite CLI l'equivalente della sezione **Destinazioni remote**:

```
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
```

Configurare tramite CLI l'equivalente della sezione **Origini locali**:

```
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
```

Inoltre, è possibile abilitare un file locale come destinazione Syslog. I messaggi Syslog possono essere visualizzati usando i comandi **show logging** o **show logging file**:

```
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: La dimensione predefinita del file è il massimo (4194304 byte).

Verifica della configurazione tramite CLI

La configurazione può essere verificata e configurata dal **monitoraggio** dell'ambito:

```
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
```

Inoltre, è possibile ottenere un output più completo dalla CLI di FXOS con il 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]
```

Verificare che i messaggi Syslog vengano visualizzati sotto il monitor del terminale

Quando il monitor Syslog è abilitato, i messaggi Syslog si trovano nella CLI di FXOS quando il terminale di monitoraggio è abilitato.

```
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]
```

Verifica servizio per gli host remoti configurati

Verificare che i messaggi vengano ricevuti sul server 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

Acquisire il traffico sulla CLI di FXOS con lo strumento Ethanalyzer per verificare che i messaggi Syslog siano generati e inviati da FXOS.

Nell'esempio, la destinazione del messaggio corrisponde al Syslog Server locale (10.61.161.235), al flag della funzionalità (Local1) e alla gravità del messaggio (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]
```

Verificare che il file di registro locale stia eseguendo correttamente la registrazione da 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
```

Genera messaggi syslog di prova

Èinoltre possibile generare messaggi Syslog di qualsiasi gravità su richiesta per scopi di test tramite CLI. In questo modo, nei server Syslog molto attivi è possibile definire un filtro più specifico per verificare che i messaggi Syslog siano stati inviati correttamente:

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

Questo messaggio viene inoltrato a qualsiasi destinazione Syslog e può essere utile in scenari in cui il filtro di una specifica origine Syslog non è possibile:

```
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]

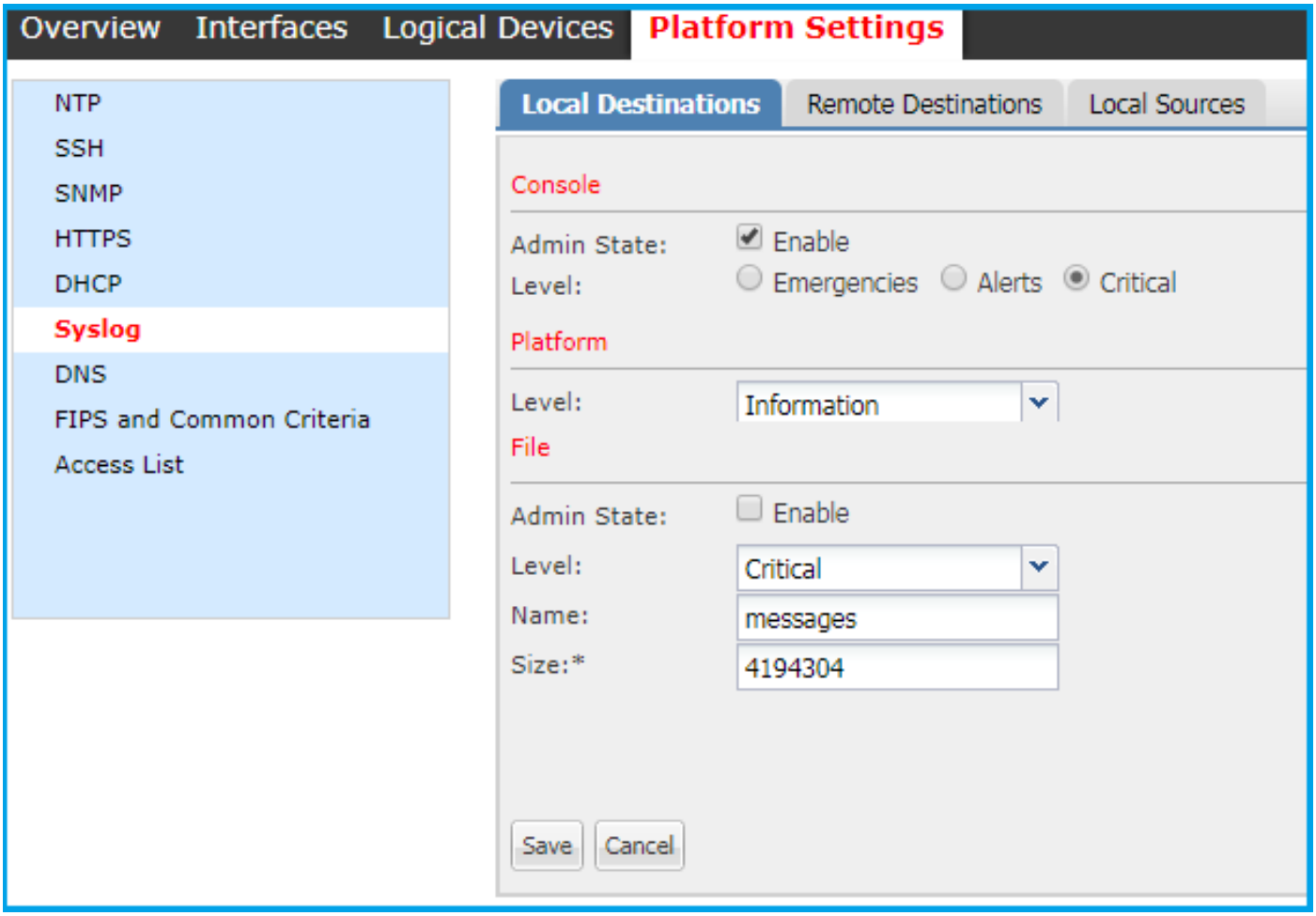
FXOS Syslog in appliance Firepower 2100

Dispositivo logico ASA in FPR2100

Esistono due differenze principali tra la configurazione Syslog per gli accessori Firepower 4100/9300 e Firepower 2100 con software ASA.

1. In Firepower 2100 la registrazione della piattaforma è attivata per impostazione predefinita e non può essere disattivata.

2. Non è disponibile la registrazione del monitor poiché il terminale monitor non esiste nelle piattaforme FP2100.



Le sezioni **Destinazioni remote** e **Origini locali** sono identiche alle altre piattaforme.

Il file di log e i log attivi della piattaforma non sono accessibili tramite i comandi CLI.

Dispositivo logico FTD in FPR2100

Nel modello FPR2100, in cui è installato l'accessorio FTD, esistono due differenze principali rispetto alle altre topologie:

1. L'indirizzo IP di origine è lo stesso utilizzato per i messaggi Syslog delle periferiche logiche.

2. Tutti i messaggi FXOS vengono utilizzati per l'ID syslog e per i processi generici di 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
```

In questo esempio vengono visualizzati i messaggi interface shutdown Syslog.

Domande frequenti

Qual è la porta predefinita utilizzata da Syslog?

Per impostazione predefinita, Syslog utilizza la porta UDP 514

Èpossibile configurare Syslog tramite TCP?

Syslog via TCP è supportato solo per FPR2100 con accessori FTD in cui i syslog FXOS sono integrati con i messaggi ASA

Informazioni correlate

- Guida alla configurazione della CLI di FXOS
- Documentazione e supporto tecnico – Cisco Systems