تكوين Syslog على أجهزة FirePOWER FXOS

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين Syslog والتحقق من صحته واستكشاف أخطائه وإصلاحها على أجهزة نظام التشغيل القابل للتشغيل (FXOS) FirePOWER.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- 1x FPR4120 مع برنامج FXOS، الإصدار 2.2(1.70)
- 1x FPR2110 مع برنامج ASA، الإصدار 9.9(2)
- 1x FPR2110 مع برنامج FTD، الإصدار 6.2.3
- خادم Syslog 1x

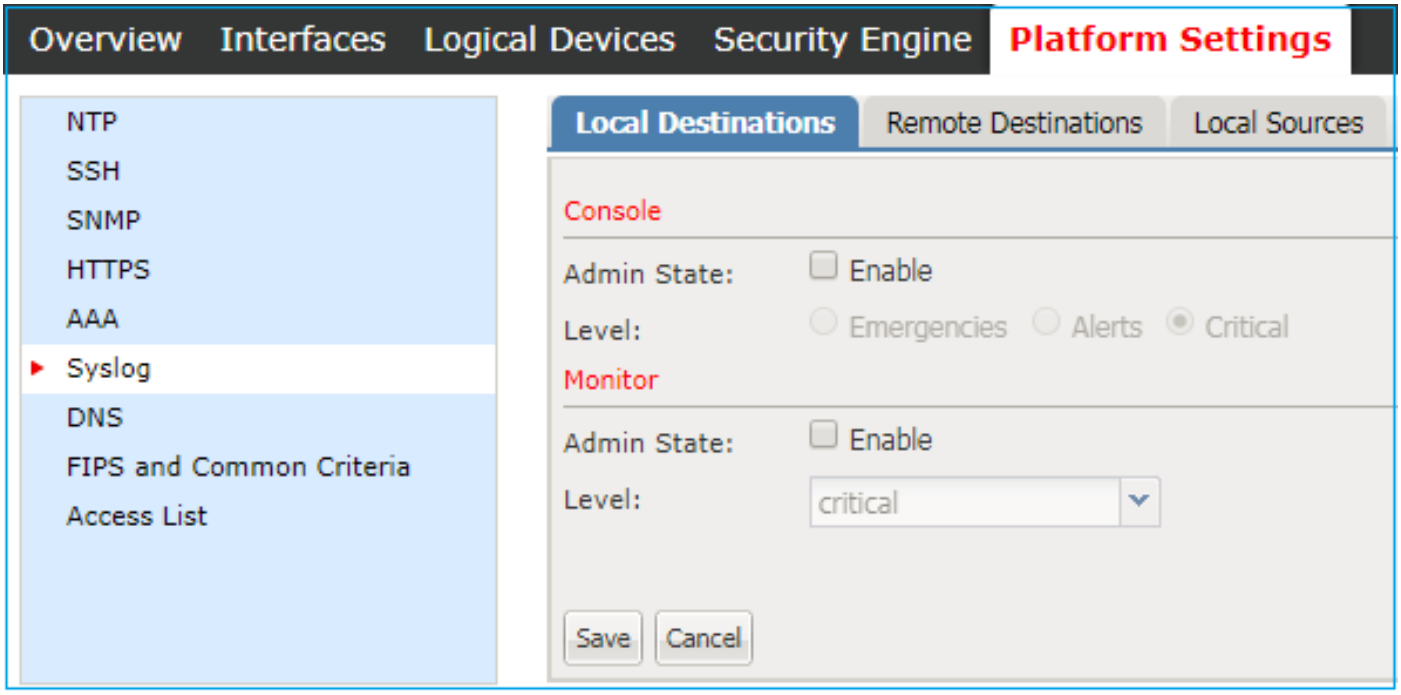
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

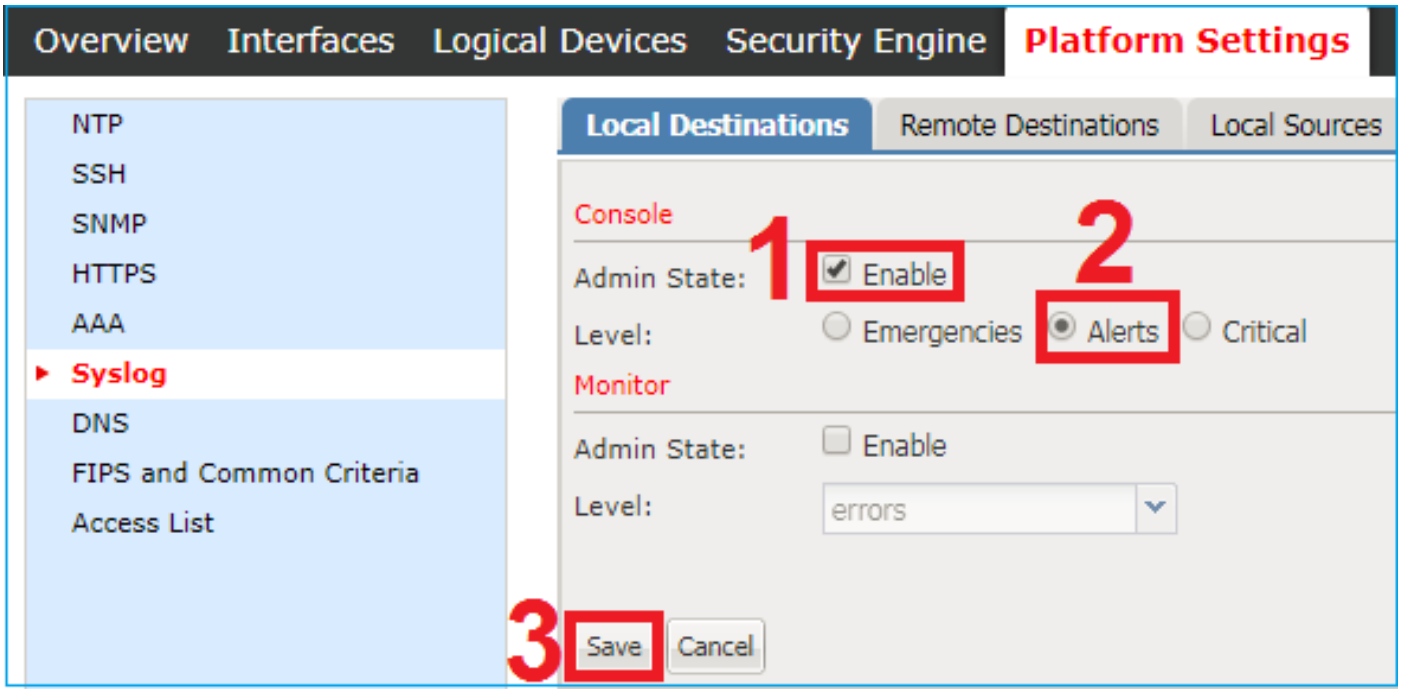
تكوين syslog من واجهة مستخدم FXOS (FPR4100/FPR9300)

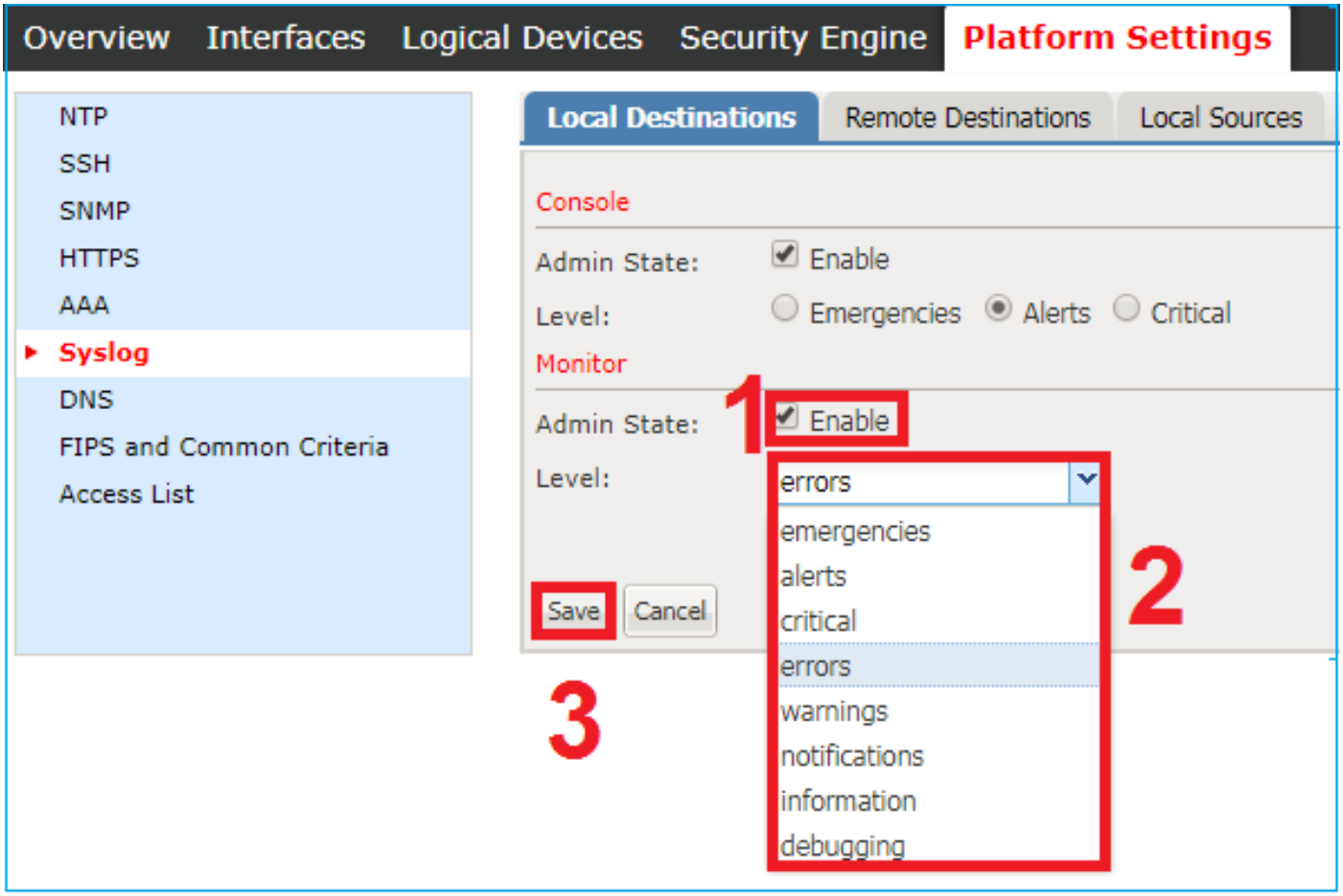
يحتوي FXOS على مجموعة رسائل Syslog الخاصة به التي يمكن تمكينها وتكوينها من مدير هيكل FirePOWER (FCM).

الخطوة 1. انتقل إلى **إعدادات النظام الأساسي** > **Syslog**.

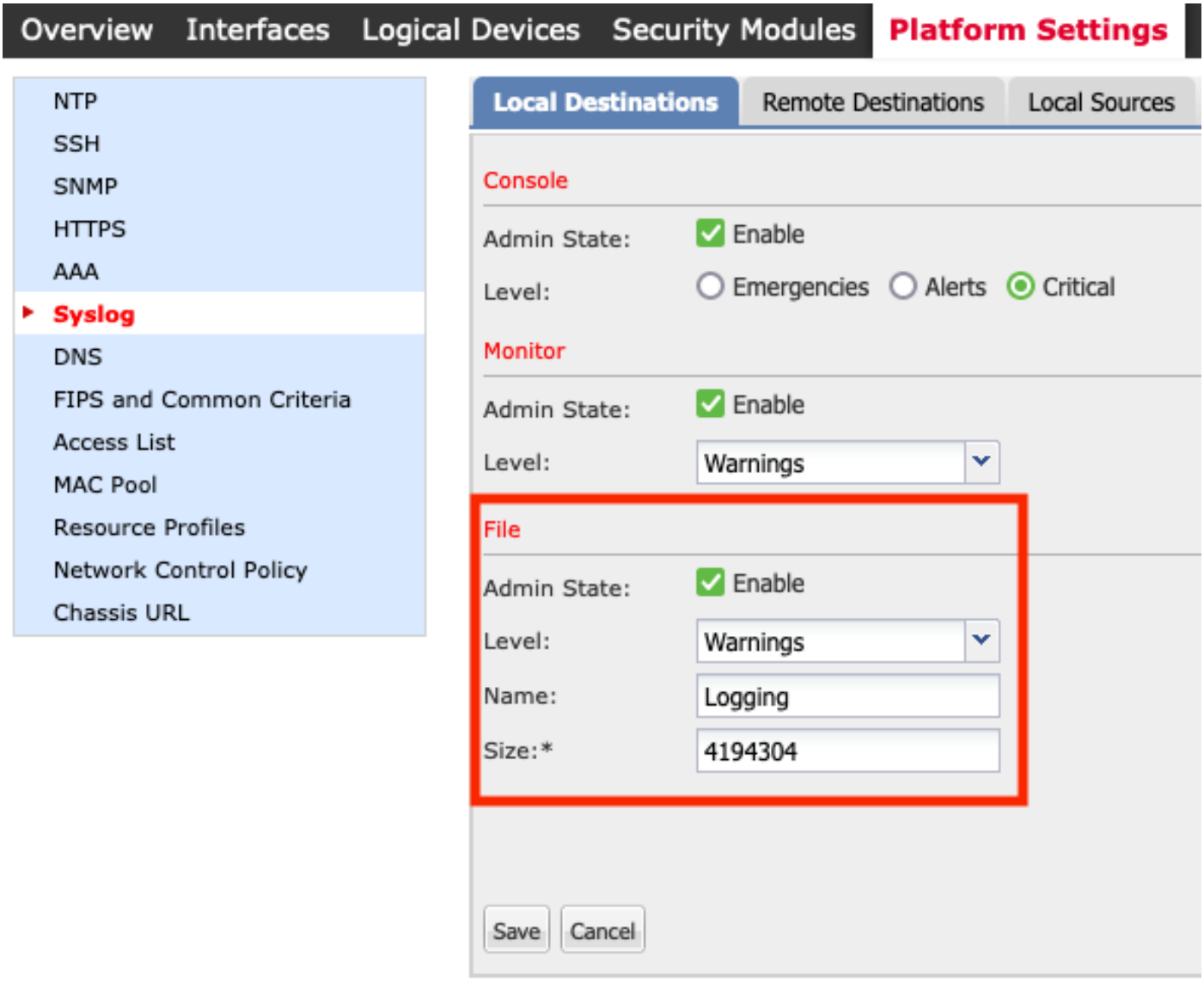


الخطوة 2. ضمن **الوجهات المحلية**، يمكنك تمكين رسائل syslog على وحدة التحكم للمستويات 0-2 أو المراقبة المحلية ل syslog أي مستوى يتم تخزينه محليا. تذكر أنه يتم عرض جميع مستويات الخطورة المحددة أيضا لكل من الطريقتين: وحدة التحكم والمراقبة.





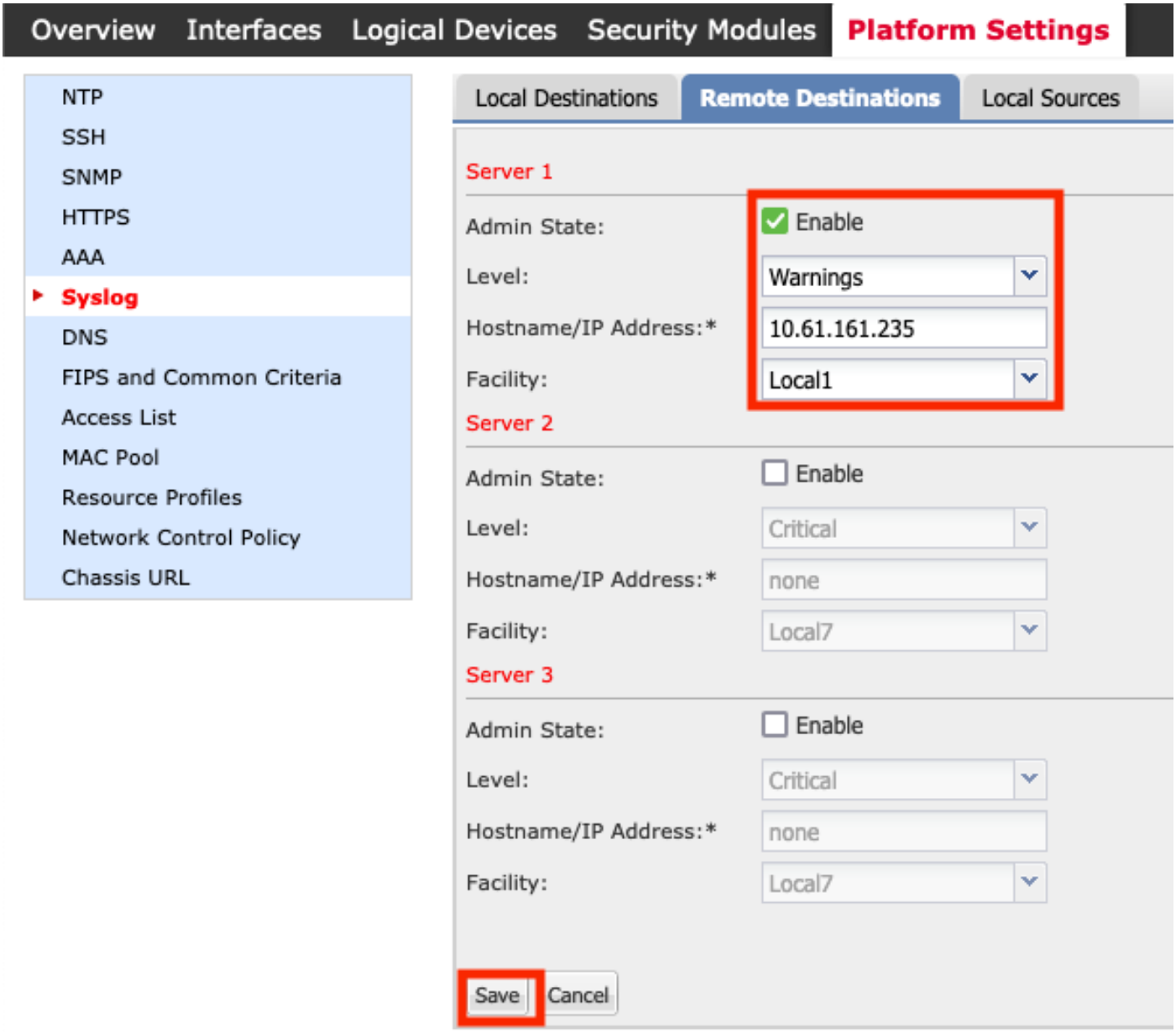
يمكنك أيضا تكوين مخزن مؤقت محلي ل syslog من FXOS صيغة 2.3.1 عن طريق gui عايشة مبرد من رسالة:



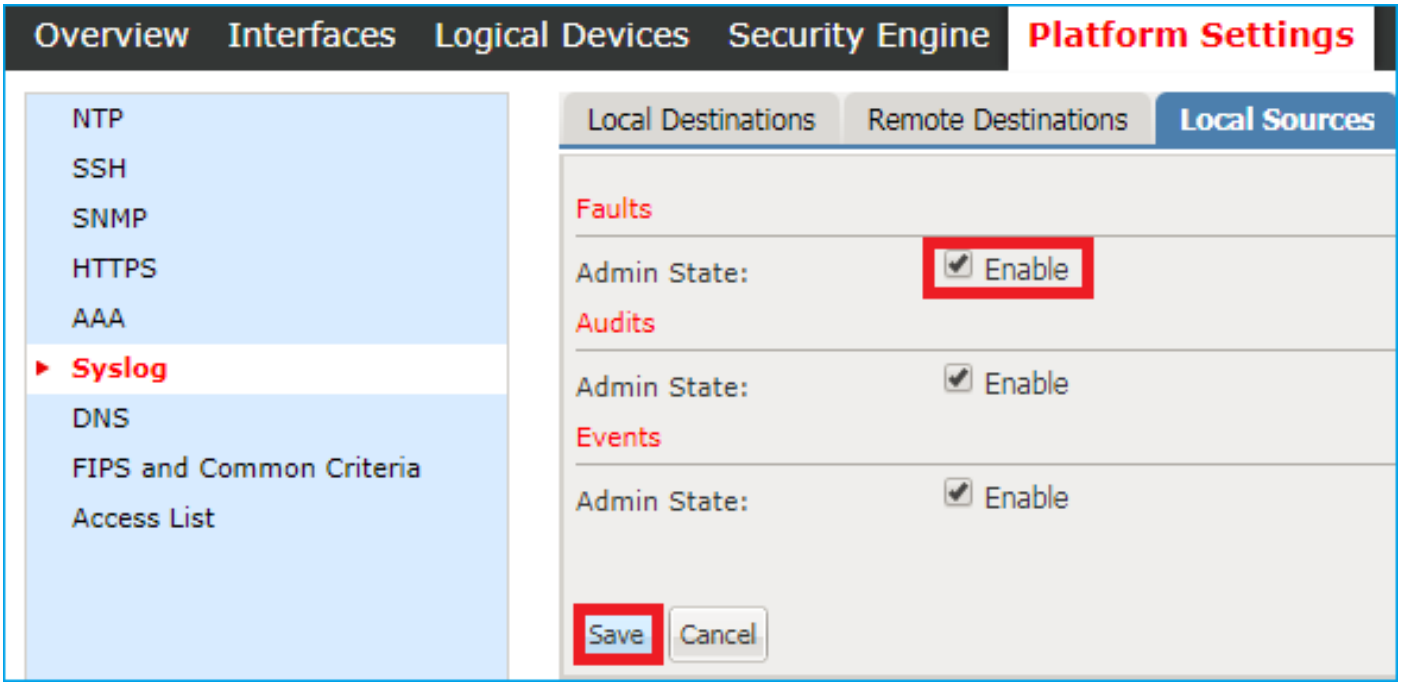
ملاحظة: يمكن أن يتراوح حجم الملف بين 4096 و 4194304 بايت فقط.

ملاحظة: في إصدار FXOS pre-2.3.1، يتوفر تكوين الملف عبر CLI فقط.

يمكنك أيضا تكوين ما يصل إلى 3 خوادم Syslog عن بعد من علامة التبويب **الوجهات البعيدة**. يمكن تعريف كل خادم كوجهة لرسائل مستوى خطورة Syslog المختلفة ووضع علامة عليها باستخدام مرفق محلي مختلف.



الخطوة 3. أخيرا، حدد **مصادر محلية** إضافية لرسائل syslog. يمكن أن يستخدم FXOS كأخطاء مصدر Syslog ورسائل التدقيق و/أو الأحداث.



تكوين Syslog من FXOS CLI (FPR4100/FPR9300)

شكلت عبر CLI ال يماثل من قسم **محلي غاية**:

```
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
```

شكلت عبر CLI ال يماثل قسم **غاية بعيد**:

```
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
```

شكلت عبر CLI ال يماثل من قسم **مصدر محلي**:

```
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
```

وبالإضافة إلى ذلك، يمكنك تمكين ملف محلي كوجهة syslog. يمكن عرض رسائل syslog هذه باستخدام الأوامر **show logging** أو **show logging log 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
```

ملاحظة: الحجم الافتراضي لهذا الملف هو الحد الأقصى (4194304 بايت).

دقة التشكيل عبر CLI

يمكن التحقق من التكوين وتكوينه من **مراقبة** النطاق:

```
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
```

أيضا، يمكنك الحصول على إخراج أكثر اكتمالا من واجهة سطر الأوامر (CLI) ل **show logging** باستخدام الأمر:

```
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]
```

التحقق من ظهور رسائل syslog ضمن جهاز العرض الطرفي

عندما syslog مكنت مدرب، syslog رسالة تحت FXOS CLI عندما مدرب انتهائية مكنت.

```
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]
```

التحقق من خدمة الأجهزة المضيفة البعيدة التي تم تكوينها

تحقق من تلقي الرسائل على خادم 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

التقط حركة مرور البيانات على CLI ل FXOS باستخدام أداة EtherAlyzer لتأكيد إنشاء رسائل syslog وإرسالها بواسطة FXOS.

في هذا المثال، تطابق وجهة الرسالة خادم syslog المحلي (10.61.161.235)، وعلامة المرفق (محلي 1) وقسوة الرسالة (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]
```

التحقق من تسجيل ملف السجل المحلي بشكل صحيح من 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
```

إنشاء رسائل إختبار syslog

هناك أيضا خيار إنشاء رسائل syslog من أي خطوة على الطلب لأغراض الاختبار عبر CLI (واجهة سطر الأوامر). بهذه الطريقة، يمكنك في خوادم syslog النشطة جدا تحديد عامل تصفية أكثر تحديدا لمساعدتك في تأكيد إرسال رسائل syslog بشكل صحيح:

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

تتم إعادة توجيه هذه الرسالة إلى أي وجهة Syslog ويمكن أن تكون مفيدة في السيناريوهات التي لا تكون فيها تصفية مصدر Syslog محددة ممكنة:

```
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]

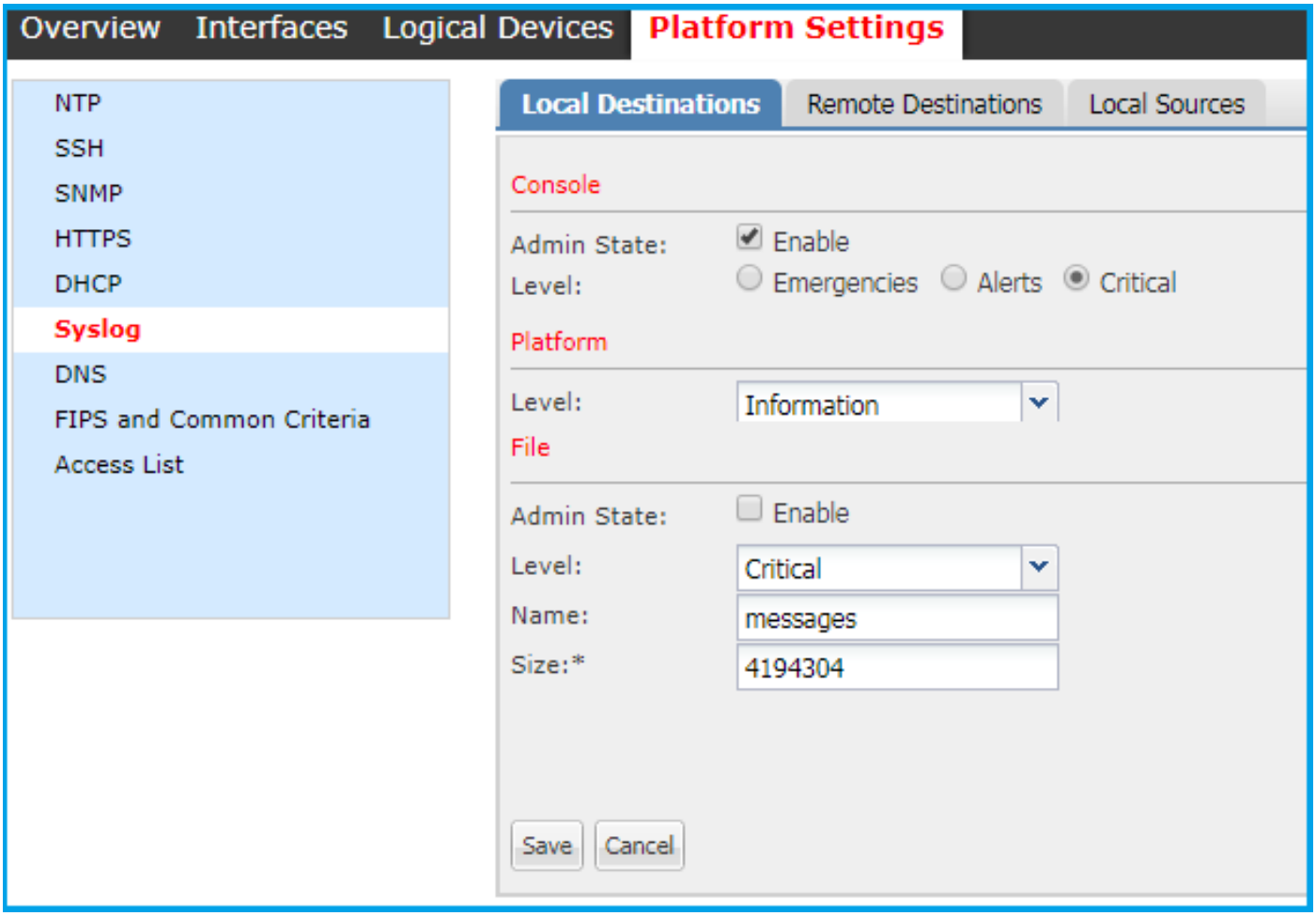
FXOS syslog في أجهزة FirePOWER 2100

جهاز ASA المنطقي في FPR2100

هناك إثنان فرق رئيسي بين syslog تشكيل ل FirePOWER 4100/9300 و FirePOWER 2100 أداة مع ASA برمجية.

1. في FirePOWER 2100 يتم تمكين تسجيل النظام الأساسي بشكل افتراضي ولا يمكن تعطيله.

2. لا يوجد تسجيل دخول للشاشة نظرا لحقيقة عدم وجود محطة المراقبة الطرفية في الأنظمة الأساسية FP2100.



كل، **الوجهات البعيدة والمصادر المحلية** متطابقة مع الأنظمة الأساسية الأخرى.

لا يمكن الوصول إلى ملف السجل وسجلات النظام الأساسي المباشرة عبر أوامر CLI.

الجهاز المنطقي FTD في FPR2100

في FPR2100 حيث يتم تثبيت جهاز FTD، يوجد اختلافان رئيسيان مقارنة بالطرازات الأخرى:

1. المصدر عنوان IP وهو نفسه الذي يستخدم لرسائل syslog للجهاز المنطقي.

2. يتم إستخدام جميع رسائل FXOS لمعرف syslog الرسالة للعمليات العامة ل 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
```

في هذا مثال، هناك القارن إيقاف عمل syslog رسالة.

أسئلة شائعة

ما هو المنفذ الافتراضي المستخدم من قبل Syslog؟

افتراضيا، يستعمل syslog UDP ميناء 514

هل يمكنك تكوين syslog عبر TCP؟

يتم دعم Syslog عبر TCP فقط لـ FPR2100 مع أجهزة FTD حيث يتم دمج أنظمة FXOS مع رسائل ASA

معلومات ذات صلة

- دليل تكوين واجهة سطر الأوامر (CLI) لـ FXOS
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).