Firepower FXOS アプライアンスの設定 Syslog

目次

概要

この資料に Firepower 拡張可能なオペレーティング システム（FXOS）アプライアンスの Syslog を設定し、確認し解決する方法を記述されています。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- FXOS ソフトウェア バージョン 2.2(1.70) との 1x FPR4120
- ASA ソフトウェア バージョンとの 1x FPR2110 9.9(2)
- FTD ソフトウェア バージョン 6.2.3 との 1x FPR2110
- 1x Syslog サーバ

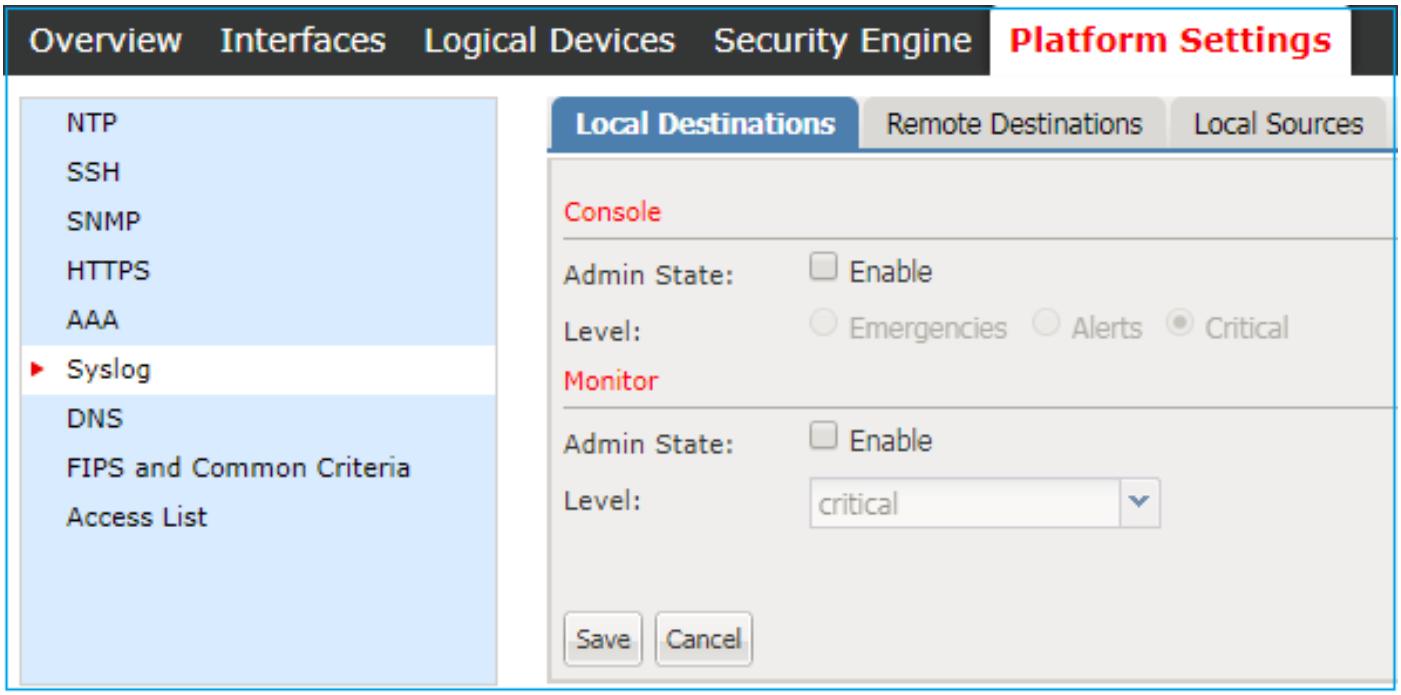
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

設定

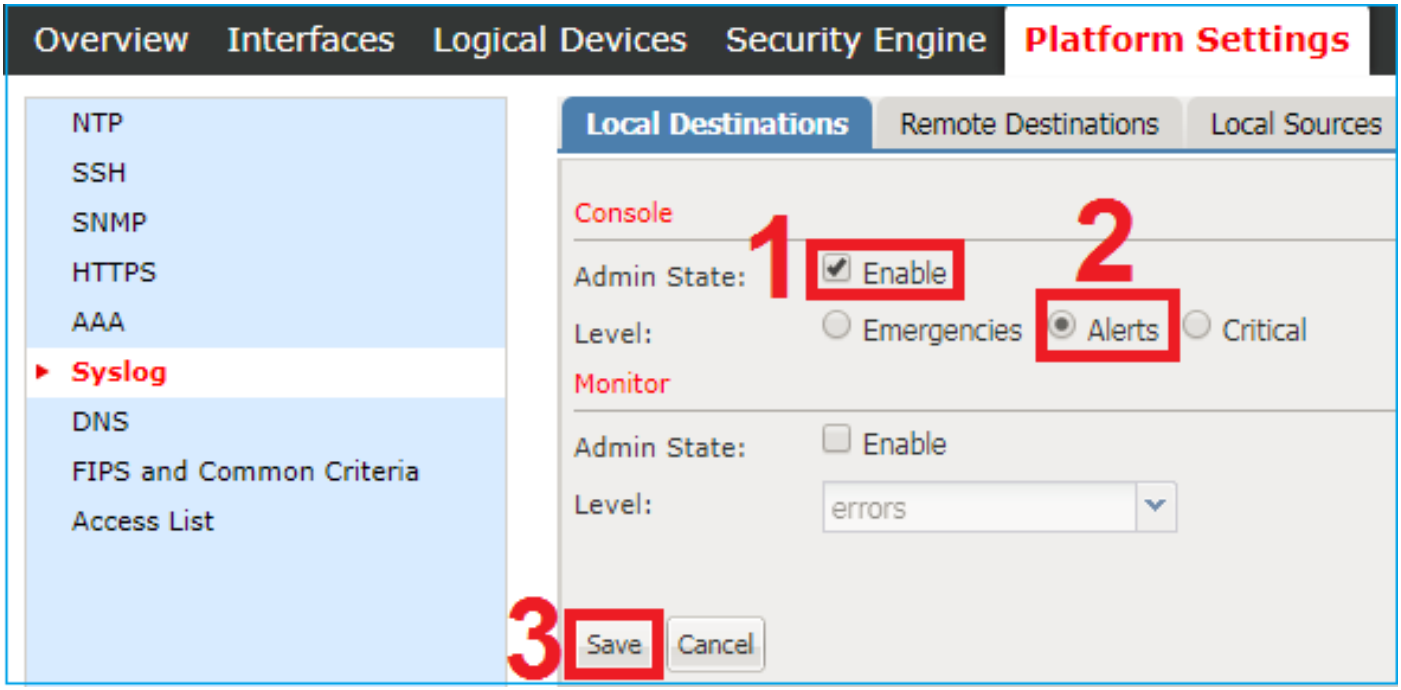
FXOS ユーザインターフェイス（FPR4100/FPR9300）からの設定 Syslog

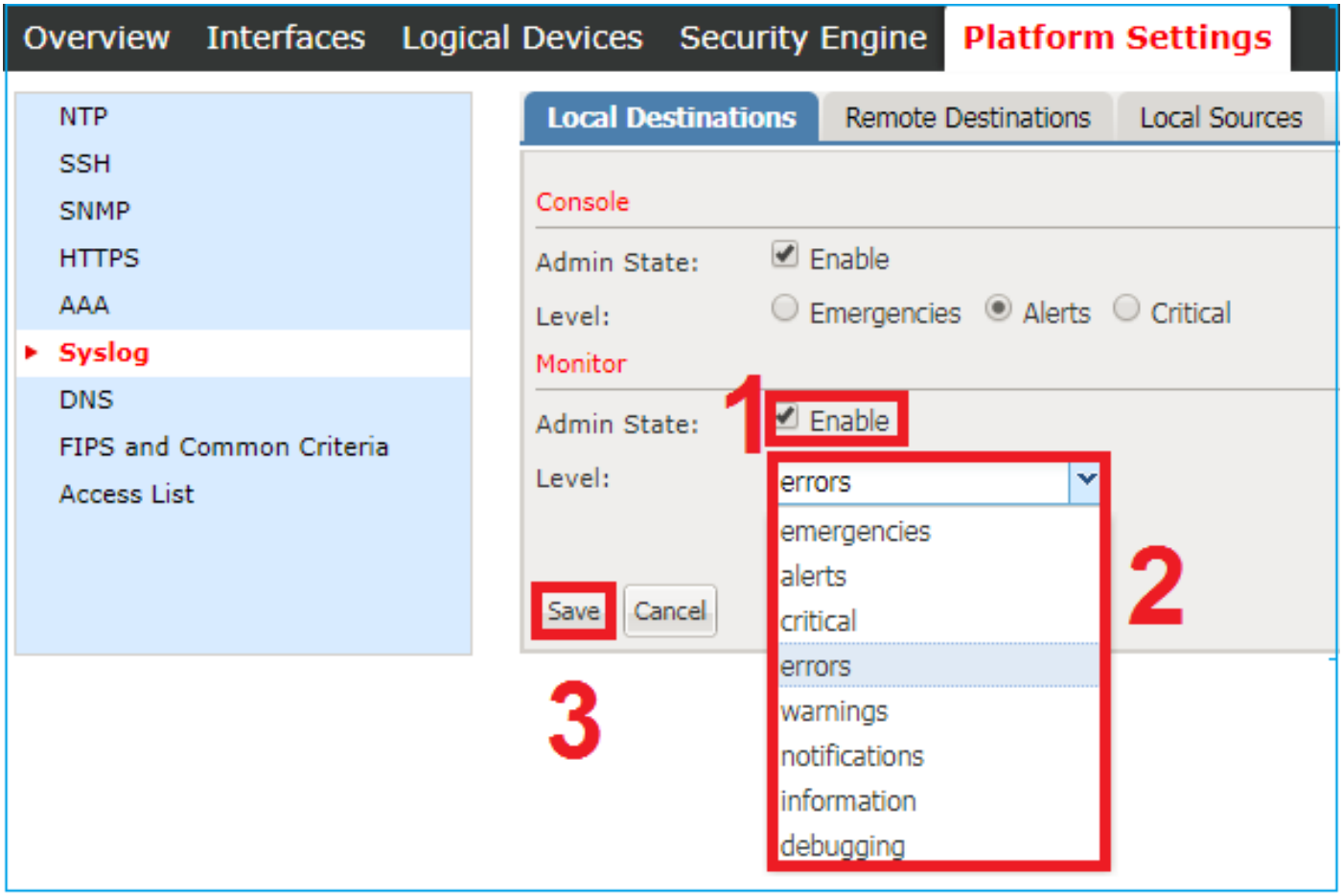
FXOS に Firepower シャーシ マネージャ（FCM）から有効に なり、設定することができる Syslog メッセージの自身のセットがあります。

ステップ 1.**プラットフォーム設定 > Syslog** へのナビゲート。

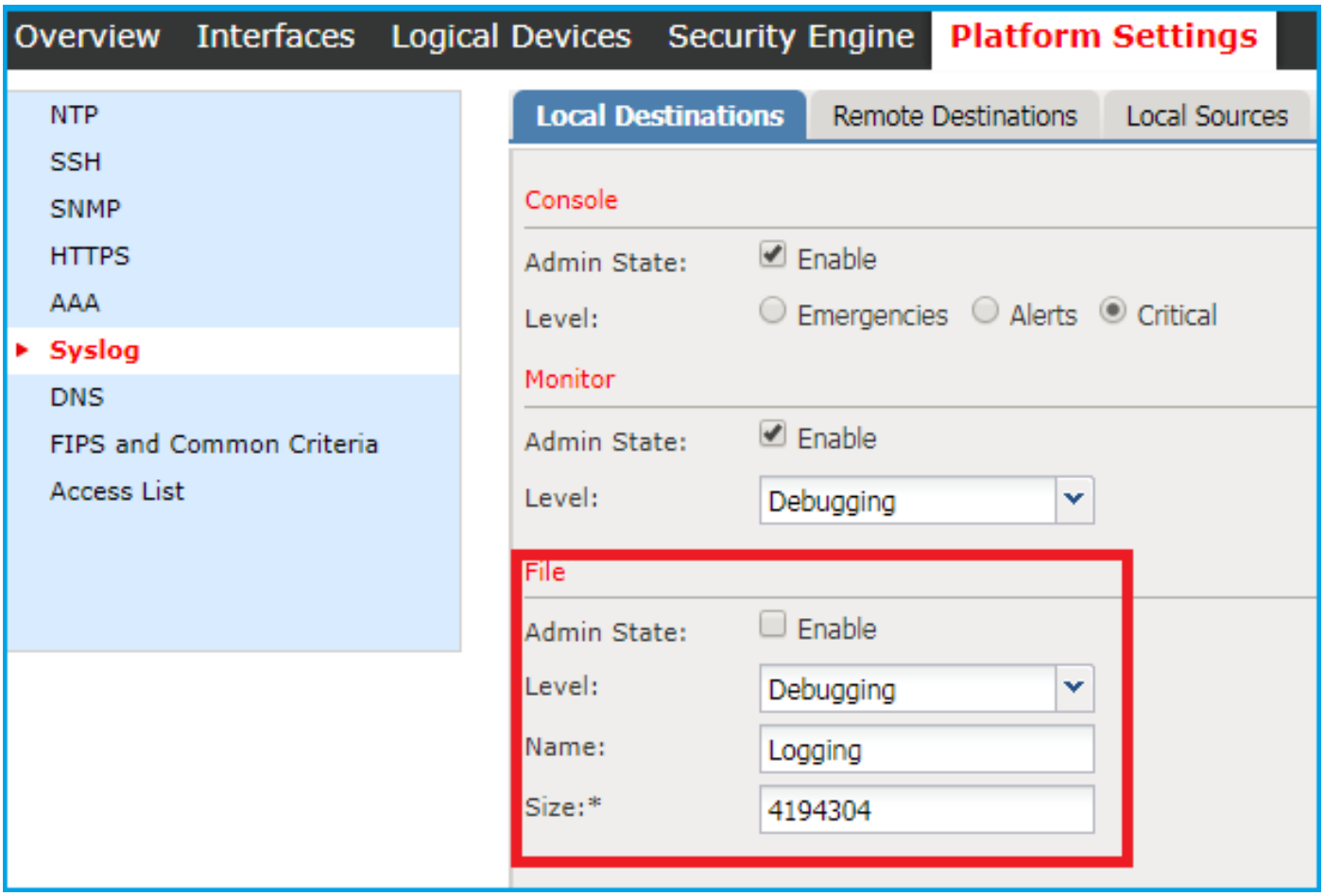


呼び出します。 **ローカル宛先**の下で、ローカルで保存されるあらゆるレベルのための Syslog の 0-2 またはローカル モニタリング レベルのためのコンソールの Syslog メッセージを有効に することができます。 また選択される両方のメソッドのためにものの上のすべての重大度が表示すると考慮して下さい: コンソールおよびモニタ。





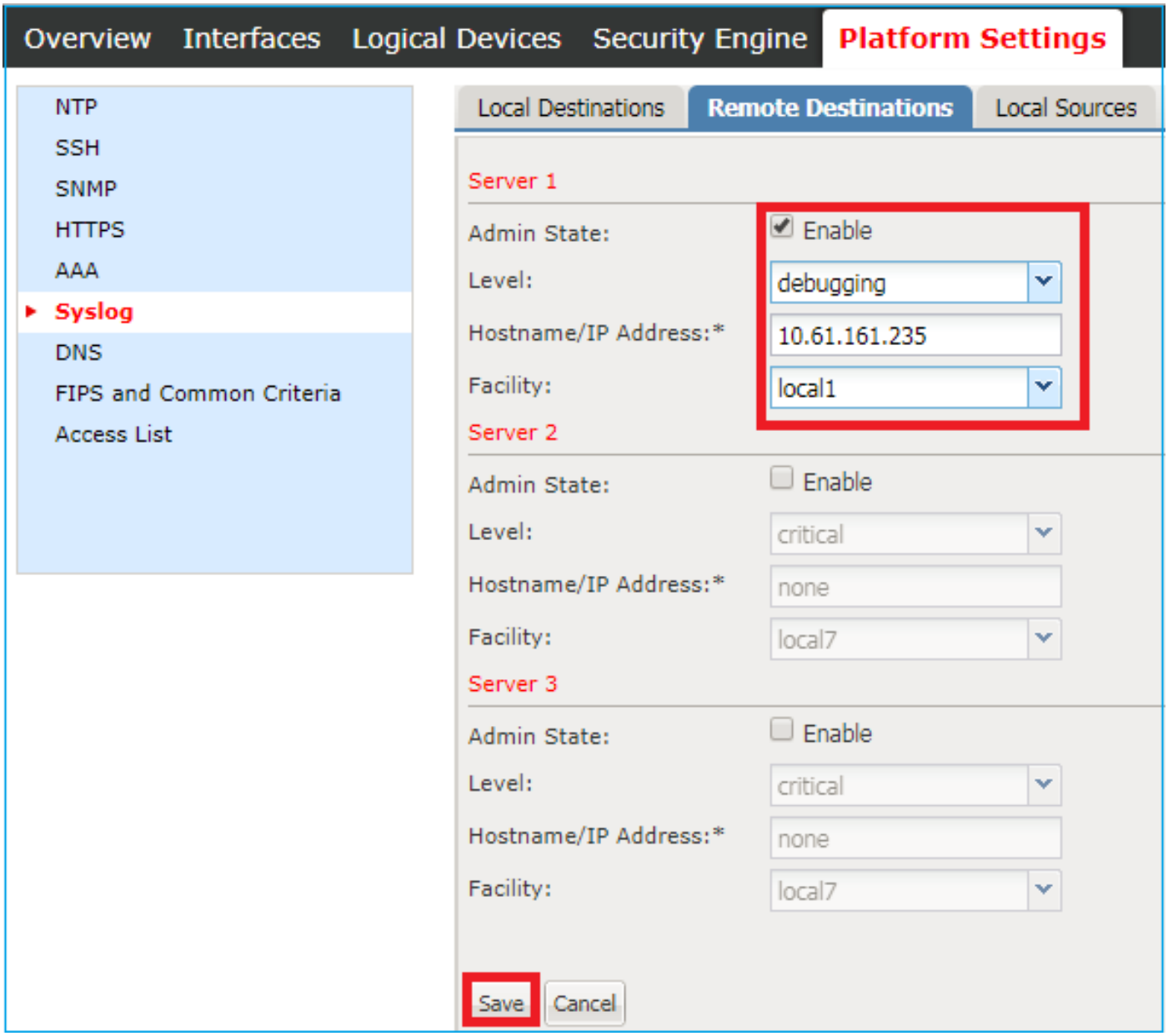
FXOS バージョン 2.3.1 からまた GUI によって Syslog メッセージのためのローカルファイル 宛先を設定できます:



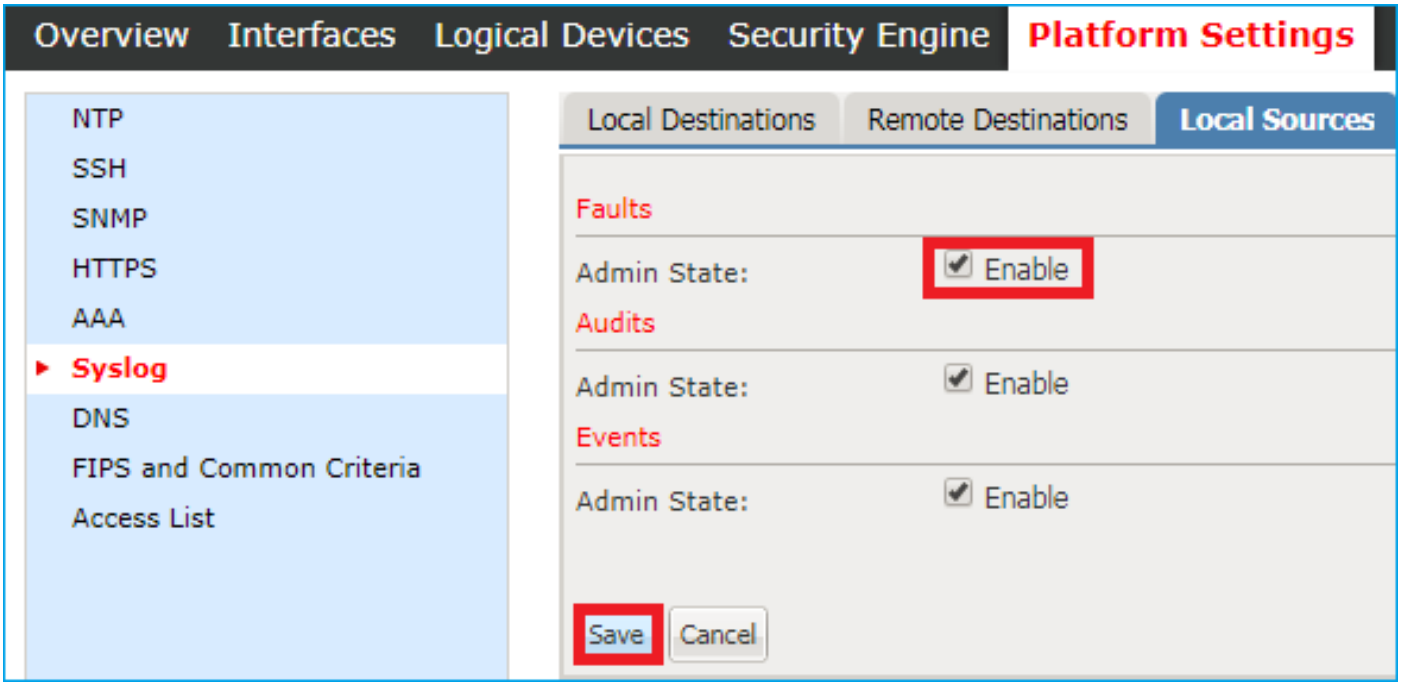
注: ファイルサイズは 4096 のおよび 4194304 バイト間のサイズがあるただ場合があります。

注: pre-2.3.1 FXOS バージョンでファイル設定は CLI だけによって利用できます。

また**リモート宛先**タブからの 3 つまでのリモート syslog サーバを設定できます。 各サーバは異なる Syslog 重大度 レベル メッセージのための宛先と定義され、別の地域 施設とフラグを付けることができます。



ステップ 3.最後に、Syslog メッセージにおける選定された追加**ローカル出典**。 FXOS は Syslog 出典エラー、監査 メッセージやイベントとして使用できます。



FXOS CLI（FPR4100/FPR9300）からの設定 Syslog

CLI によってセクション **ローカル宛先**の等量を設定して下さい:

```
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
```

CLI によってセクション **リモート宛先**の等量を設定して下さい:

```
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
```

CLI によってセクション **ローカル出典**の等量を設定して下さい:

```
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
```

さらに、Syslog 宛先としてローカルファイルを有効に することができます。 これらの Syslog メッセージはコマンド **show logging** か **show logging ログファイル**を使用して表示することができます:

```
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
```

注: このファイルのデフォルト サイズは最大です（4194304 バイト）

CLI によって設定を確認して下さい

設定はスコープ **モニタリング**から確認され、設定することができます:

```
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
```

また、**show logging コマンド**で FXOS CLI からより多くの完全な出力が表示されることができます:

```
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]
```

Syslog メッセージが Terminal monitor の下で現れることを確認して下さい

Syslog モニタが有効に なるとき、FXOS CLI の下でモニタ ターミナルが有効に なるとき Syslog メッセージが表示されるはずです。

```
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]
```

設定されるリモートホストのためのサービスを確認して下さい

メッセージが Syslog サーバで受け取られていることを確認して下さい。

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

Syslog メッセージが FXOS によって生成されて、送信 されて いることを確認するために Ethanalyzer ツールの FXOS CLI のトラフィックをキャプチャ して下さい。

この例では、ローカル Syslog サーバと一致するメッセージの宛先（10.61.161.235）、ファシリティ フラグ（Local1）およびメッセージ（6）の重大度:

```
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]
```

ローカル ログファイルが FXOS から正しく記録 して いることを確認して下さい

```
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
```

Syslog メッセージをテストすることを生成して下さい

また CLI によってあらゆる重大度の Syslog メッセージをオンデマンド式でテストの目的で生成するオプションがあります。 非常にアクティブな Syslog サーバのこの方法、Syslog メッセージが正しく送信 されて いることを確認するために助けるようにより多くの特定のフィルタを定義できます:

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

このメッセージは Syslog あらゆる宛先に転送され、仕様 Syslog 出典のフィルタリングが実行不可能であるシナリオで有用である場合もあります:

```
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]

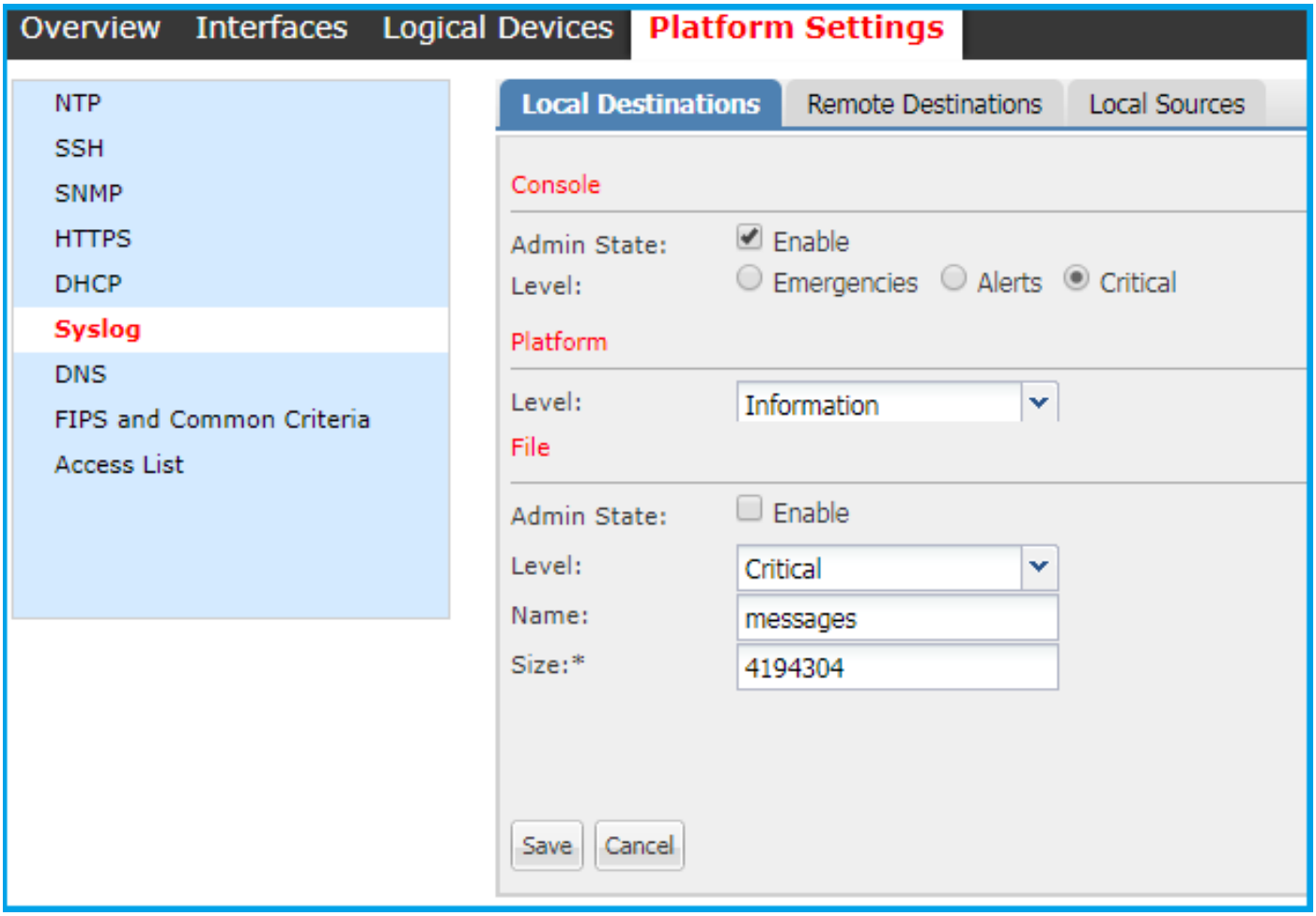
Firepower の FXOS Syslog 2100 のアプライアンス

FPR2100 の ASA 論理デバイス

Firepower 4100/9300 および Firepower のための Syslog 設定間に 2 つの主な違いが ASA ソフトウェアの 2100 のアプライアンスあります。

1. Firepower 2100 でプラットフォーム ロギングはデフォルトで有効に なり、無効に なることができません。

2. モニタ ターミナルが FP2100 プラットフォームにないというファクトによるモニタロギングがありません。



両方とも、**リモート宛先**および**ローカル 出典**セクションは他のプラットフォームと同一です。

ログファイルおよびプラットフォーム ライブ ログは CLI コマンドによってアクセスが不可能です。

FPR2100 の FTD 論理デバイス

FTD アプライアンスがインストールされている FPR2100 で他のトポロジーと比較される 2 つの主な違いがあります:

1. ソース IP アドレスは論理デバイス Syslog メッセージのために使用した同じです。

2. すべての FXOS メッセージは Syslog ID のために ASA 199013-199019 の一般的 なプロセスのためのメッセージ使用されます

```
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
```

この例では、インターフェイスが Syslog メッセージをシャットダウンするのを表示できます。

FAQ

Syslog によって使用されるデフォルトポートはどれですか。

デフォルトで、Syslog 使用 UDP ポート 514

TCP によって Syslog を設定できますか。

TCP による Syslog はだけ FXOS Syslog が ASA メッセージと統合 FTD アプライアンスとの FPR2100 のためにサポートされます

関連情報

- FXOS CLI コンフィギュレーション ガイド
- テクニカル サポートとドキュメント – Cisco Systems