Firepower FXOSアプライアンスでのsyslogの設定

内容

概要

このドキュメントでは、Firepower eXtensible Operating System(FXOS)アプライアンスでSyslogを設定、確認、およびトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに特有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いています。

- FXOSソフトウェアバージョン2.2(1.70)が稼働するFPR4120 X 1
- ASAソフトウェアバージョン9.9が稼働するFPR2110 X 1
- FTDソフトウェアバージョン6.2.3が稼働するFPR2110 X 1
- 1x Syslogサーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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

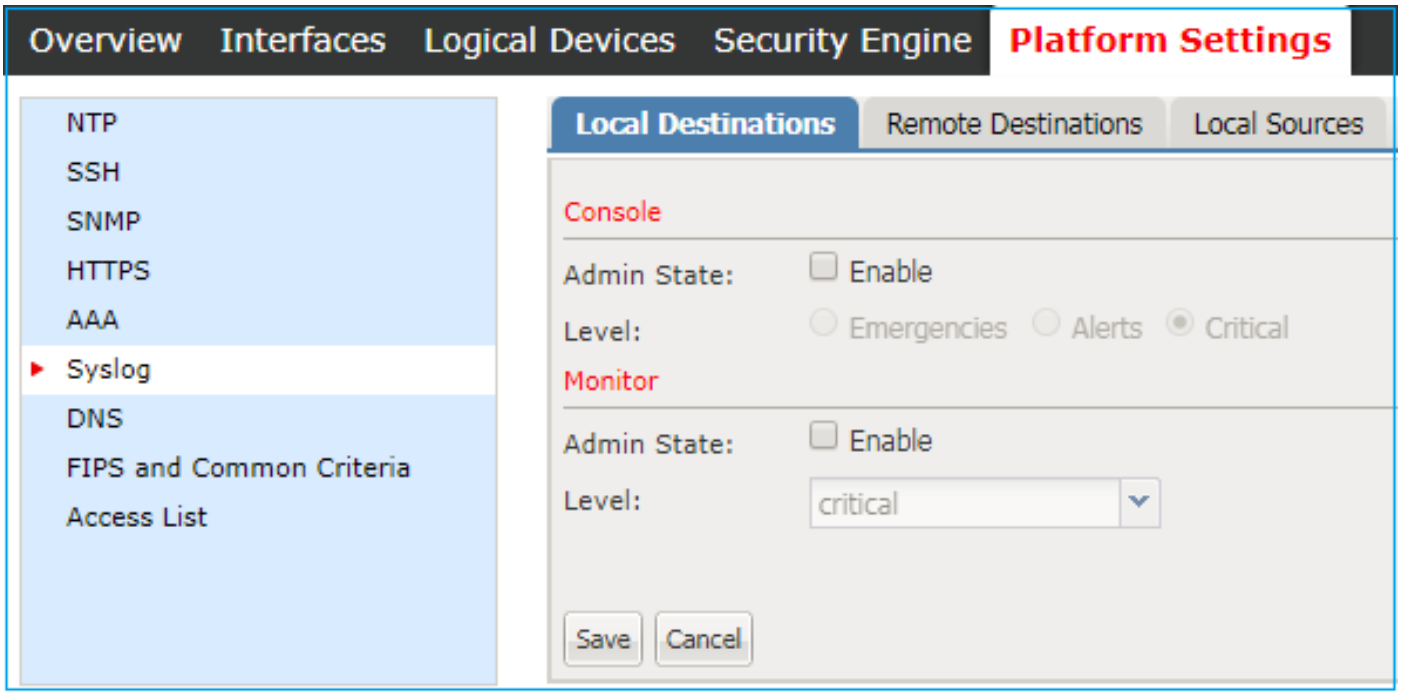
。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

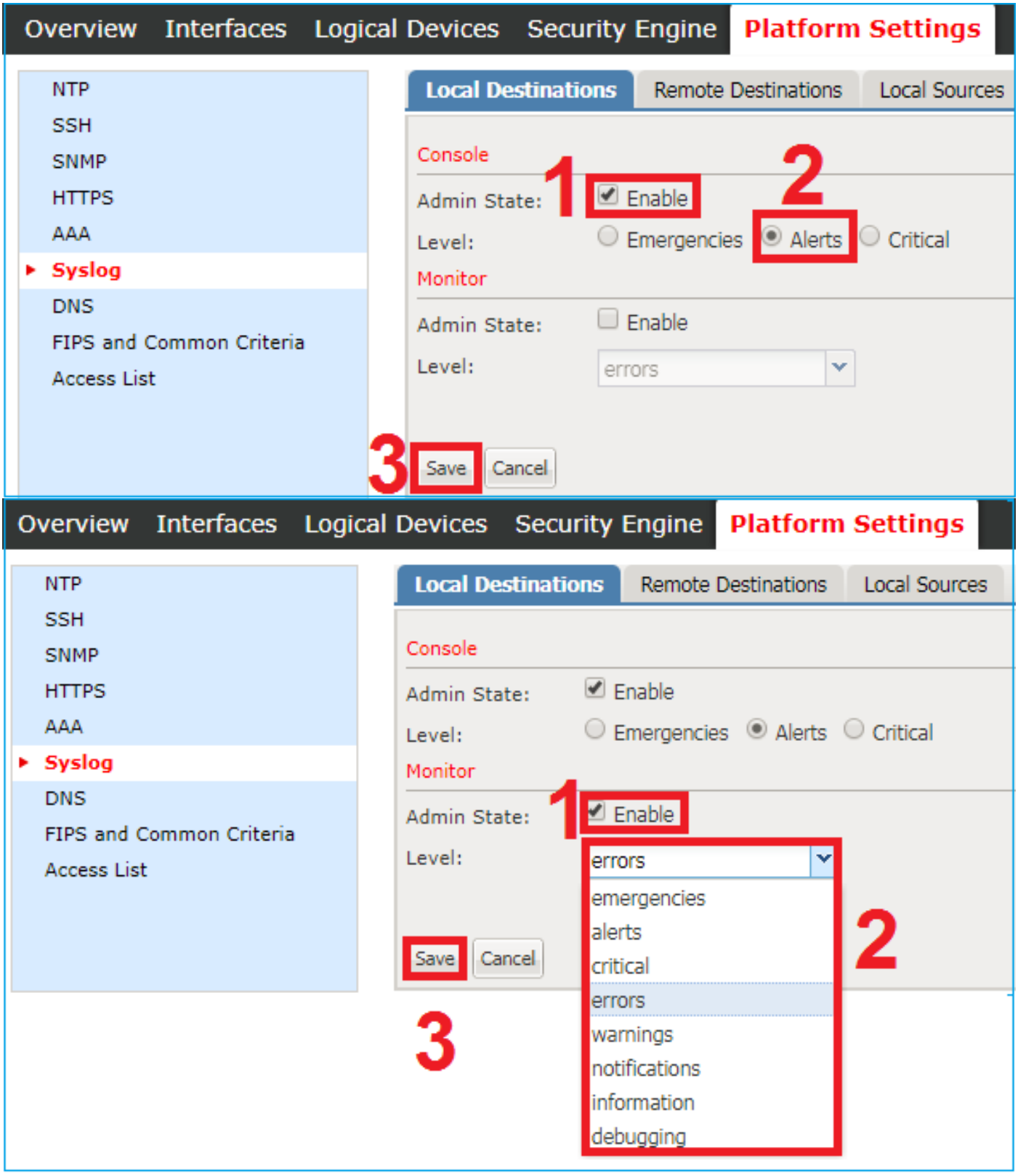
FXOSユーザインターフェイス(FPR4100/FPR9300)からのsyslogの設定

FXOSには、Firepower Chassis Manager(FCM)からイネーブルおよび設定できる独自のsyslogメッセージのセットがあります。

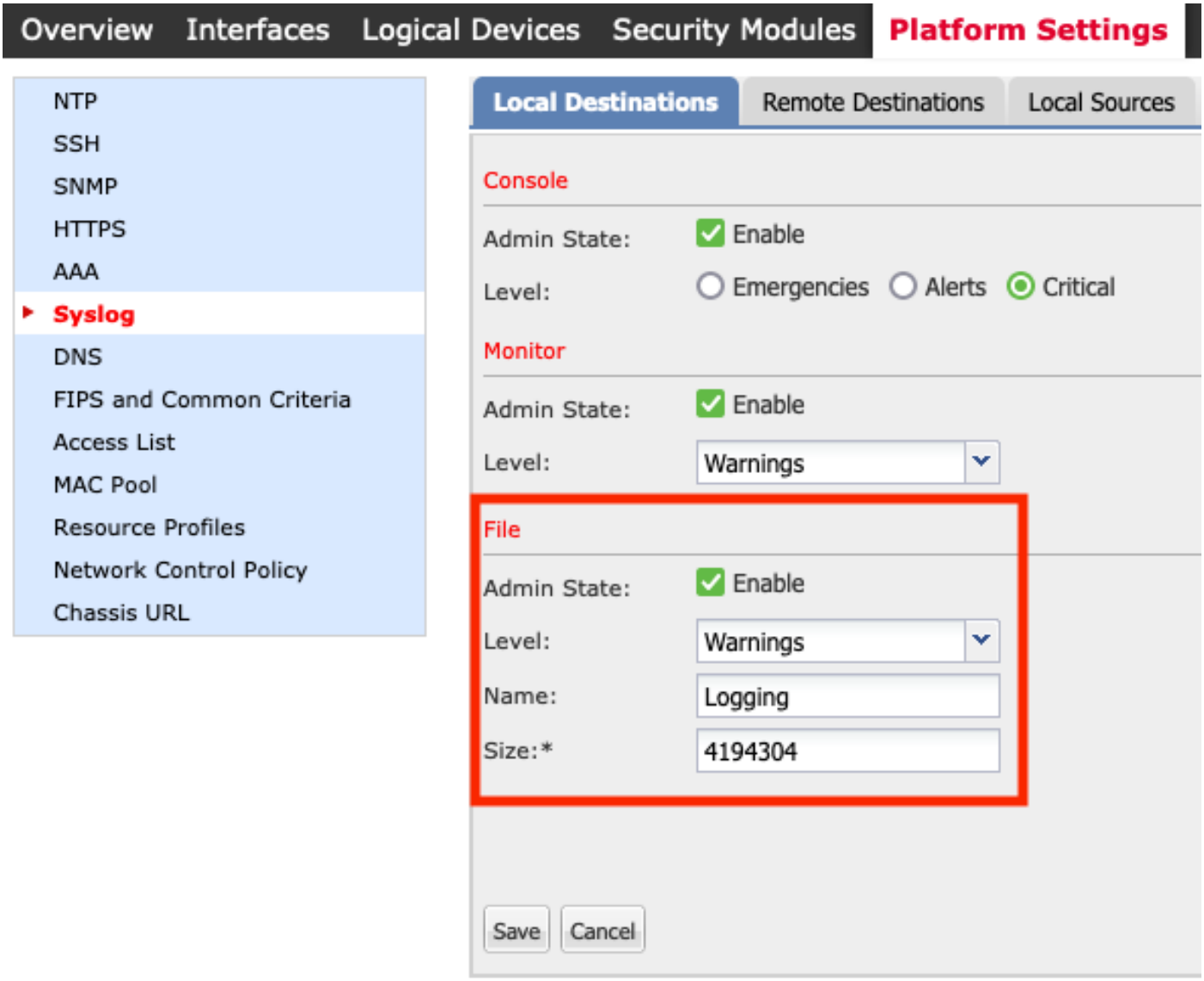
ステップ1:[Platform Settings] > [**Syslog]に移動します。**



ステップ2:[Local Destinations] で、コンソールのSyslogメッセージをレベル0 ~ 2に対して有効にするか、またはローカルに保存されている任意のレベルに対してSyslogのローカルモニタリングを有効にできます。選択したすべての重大度レベルが両方の方法に対して表示されることを考慮してください。コンソールとモニタ。



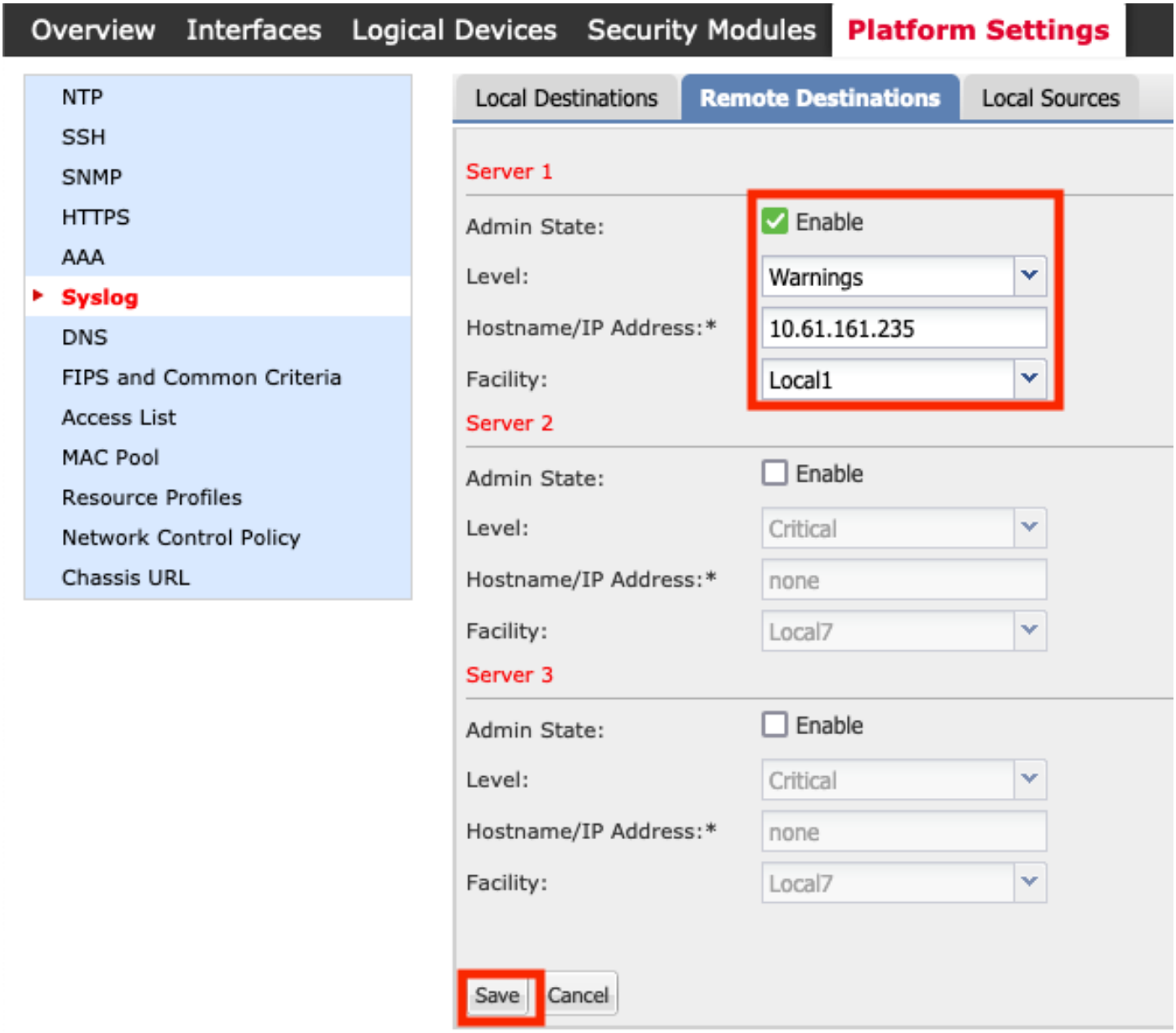
FXOSバージョン2.3.1から、GUIを使用してSyslogメッセージのローカルファイルの宛先を設定することもできます。



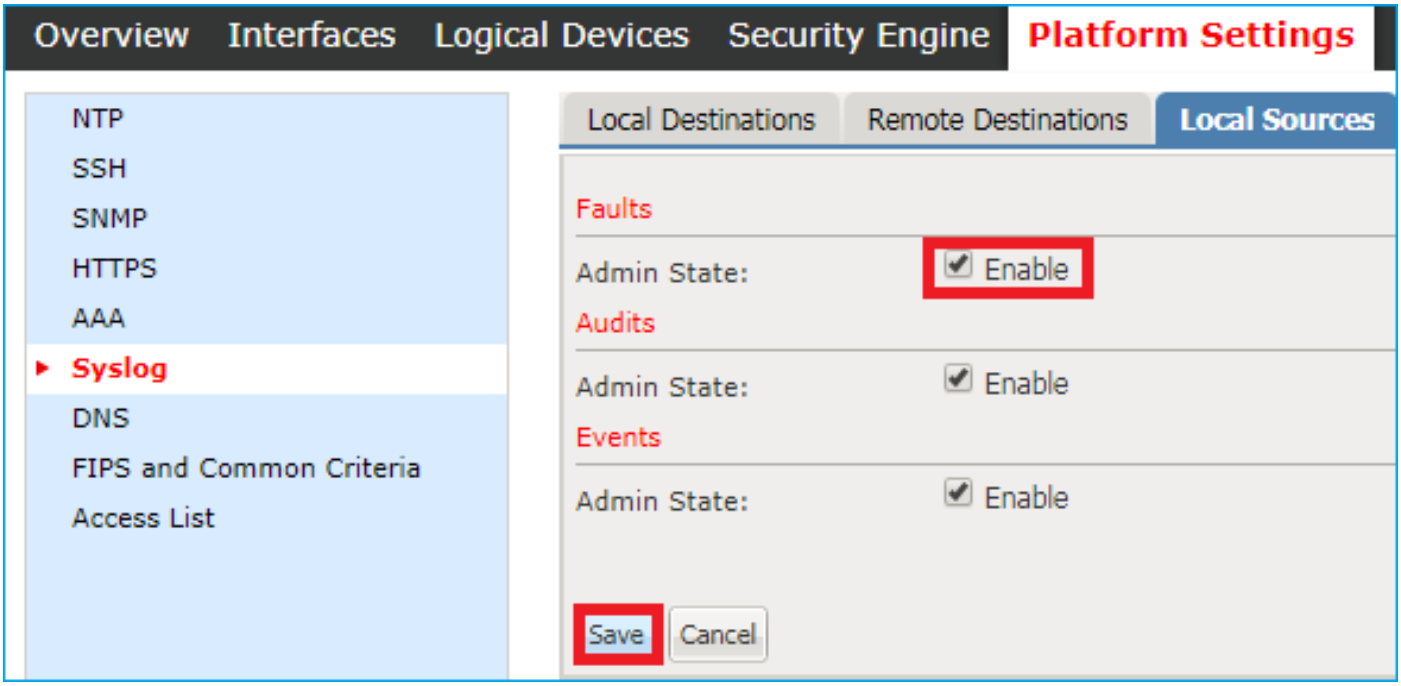
注：ファイルサイズのサイズは4096 ~ 4194304バイトまでです。

注：2.3.1より前のFXOSバージョンでは、ファイルの設定はCLIでのみ使用できます。

[リモート接続先(Remote Destinations)]タブから最大3台のリモート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宛先として定義でき、異なるローカルファシリティでフラグを付けることができます。



ステップ3：最後に、Syslogメッセージに追加**のローカルソ**ースを選択します。FXOSは、syslogソース障害、監査メッセージ、イベントとして使用できます。



FXOS CLIからのsyslogの設定(FPR4100/FPR9300)

CLIを使用して、「ローカル宛先」セクションに相当する**設定を行います。**

```
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
```

CLIを使用して、「リモート接続先」セクションと同じ**ことを設定します。**

```
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
```

CLIを使用して、「ローカルソース」セクションに相当する**項目を設定します。**

```
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
```

また、ローカルファイルをSyslogの宛先として有効にすることもできます。次のSyslogメッセージは、**show logging**または**show logging logfile**コマンドを使用して表示できます。

```
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
```

注：このファイルのデフォルトサイズは最大(4194304バイト)です。

CLIによる設定の確認

設定は、スコープの監視から確認および設定できます。

```
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
```

また、show loggingコマンドを使用すると、FXOS CLIからより完全な出力を取得できます。

```
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]
```

Syslogメッセージがターミナルモニタに表示されることを確認する

Syslogモニタが有効な場合、モニタターミナルが有効な場合、SyslogメッセージはFXOS CLIの下

にあります。

```
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]
```

設定されたリモートホストのサービスの確認

メッセージがSyslogサーバで受信されていることを確認します。

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

Ethanalyzerツールを使用してFXOS CLIでトラフィックをキャプチャし、Syslogメッセージが生成され、FXOSによって送信されることを確認します。

この例では、メッセージの宛先は、ローカルSyslogサーバ(10.61.161.235)、ファシリティフラグ(Local1)、およびメッセージの重大度(6)と一致します。

```
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]
```

ローカルログファイルがFXOSから正しくロギングされていることの確認

```
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
```

テストsyslogメッセージの生成

また、CLIを使用して、テスト目的でオンデマンドで重大度のsyslogメッセージを生成するオプションもあります。このように、非常にアクティブなSyslogサーバでは、より具体的なフィルタを定義して、Syslogメッセージが正しく送信されたことを確認できます。

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

このメッセージは任意のSyslog宛先に転送され、特定のSyslogソースのフィルタリングが不可能な場合に役立ちます。

```
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]

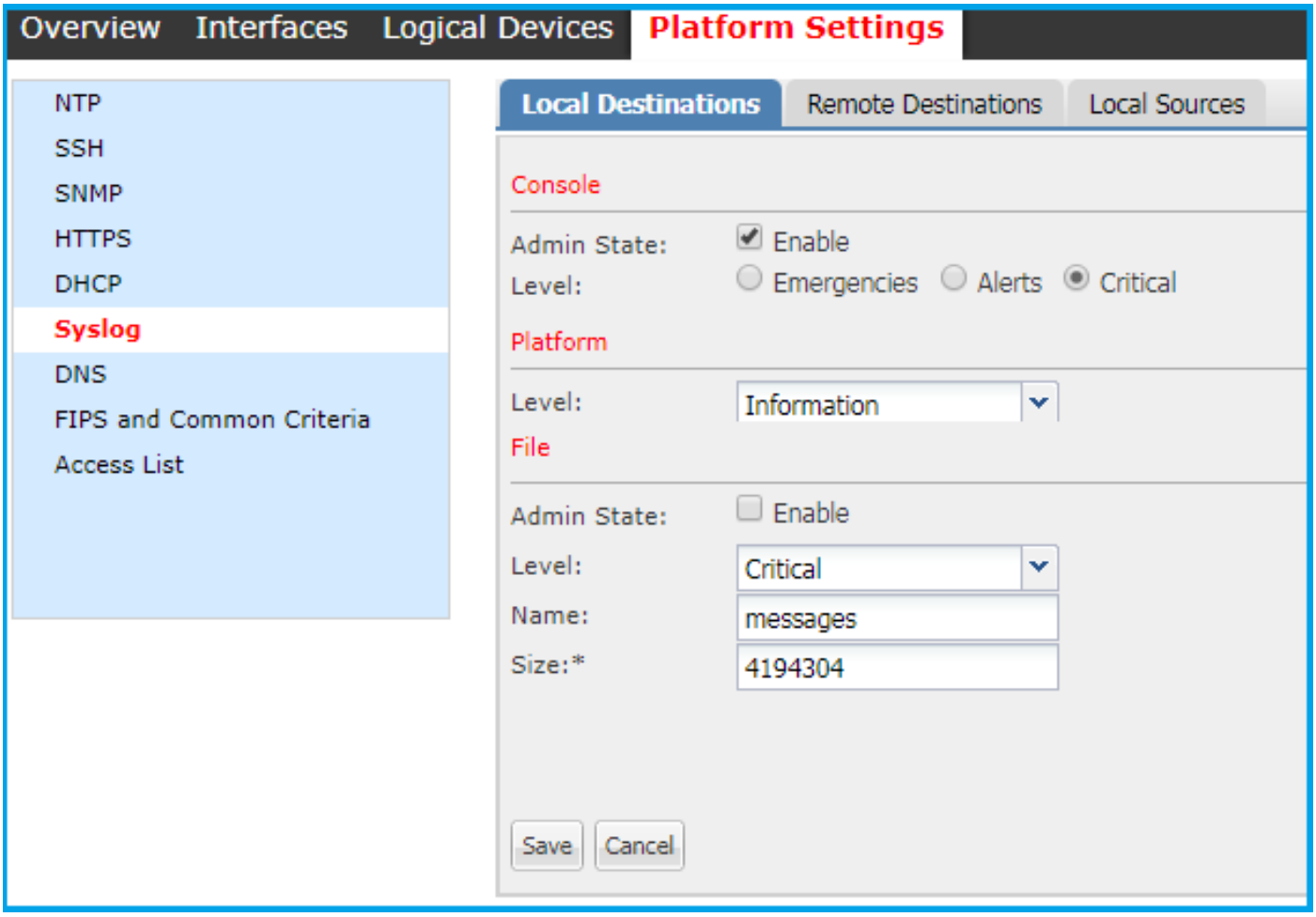
Firepower 2100アプライアンスのFXOS syslog

FPR2100のASA論理デバイス

ASAソフトウェアを使用するFirepower 4100/9300およびFirepower 2100アプライアンスのSyslog設定には、主に2つの違いがあります。

1. Firepower 2100では、プラットフォームロギングはデフォルトで有効になっており、無効にすることはできません。

2. モニタ端末がFP2100プラットフォームに存在しないため、モニタロギングはありません。



[Remote Destinations]セクションと[Local Sources]セクションの両方が他のプラットフォームと同じです。

ログファイルとプラットフォームのライブログには、CLIコマンドではアクセスできません。

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では、他のトポロジと比較して2つの大きな違いがあります。

1. 送信元IPアドレスは、論理デバイスのSyslogメッセージに使用されるものと同じです。

2. すべてのFXOSメッセージは、ASA 199013-199019の一般的なプロセスのメッセージであるSyslog IDに使用されます

```
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shutdown Syslogメッセージがあります。

FAQ

Syslogで使用されるデフォルトポートはどれか？

デフォルトでは、SyslogはUDPポート514を使用します

TCP経由でSyslogを設定できますか。

TCP経由のsyslogは、FXOS SyslogがASAメッセージに統合されているFTDアプライアンスを使用するFPR2100でのみサポートされます

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