

# 以前に設定した（レガシー）Syslogサーバにログを送信するファイアウォールのトラブルシューティング

## 内容

---

---

## お問い合わせ内容

ファイアウォールは、以前に設定された（レガシー）syslogサーバ（IPアドレス198.51.100.100）にsyslogメッセージを送信します。このIPアドレスは、ファイアウォール設定には存在しません。

## 環境

該当するプラットフォームは、プラットフォームモードでASAを実行するFirepower 2100です。

## 解決策

ステップ 1 : syslogメッセージの送信元IPアドレスを見つけます。

レガシーsyslogサーバで受信したメッセージの分析に基づくと、発信元IPアドレスはFirepowerシャーシの管理IPアドレスです。

Firepower eXtensible Operating System(FXOS)で設定されたIPアドレスは192.0.2.100です。

<#root>

192.0.2.100

```
Apr 27 09:22:49 firepower FPRM: <<%FPRM-3-NTP_CONFIG_FAILED>> [F1329][major][ntp-config-failed][syslog]
2026-04-27 15:22:54 User.Error
```

192.0.2.100

```
Apr 27 09:22:54 firepower FPRM: <<%FPRM-3-NTP_CONFIG_FAILED>> [F1329][cleared][ntp-config-failed][syslog]
```

ステップ 2 FXOSのsyslog設定を確認します。

- FXOSコマンドラインインターフェイス(CLI)設定に、レガシーsyslogサーバのアドレスが含まれていない。

```
<#root>
```

```
device #
```

```
scope monitoring
```

```
device /monitoring #
```

```
show configuration | i 198.51.100.100
```

```
device /monitoring #
```

```
show configuration all | i 198.51.100.100
```

- 同時に、監視スコープ内のshow syslogコマンドの出力には、サーバのIPアドレスが示されます。

```
<#root>
```

```
device #
```

```
scope monitoring
```

```
device /monitoring #
```

```
show syslog
```

```
console
state: Disabled
level: Critical
```

```
platform
state: Enabled
level: Information
```

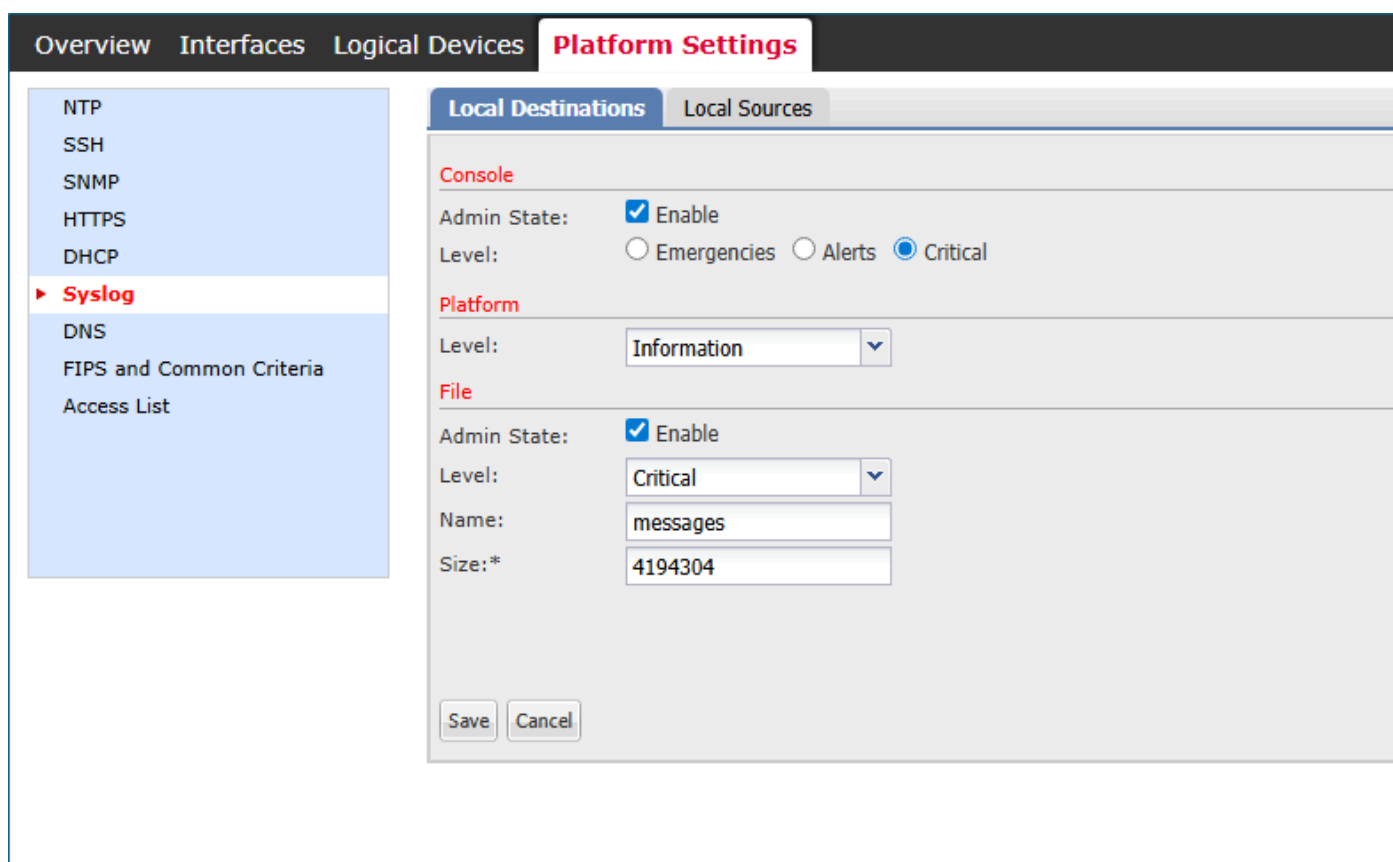
| Name     | Hostname      | State   | Level    | Facility |
|----------|---------------|---------|----------|----------|
| Server 1 | 198.51.100.10 | Enabled | Warnings | Local7   |

```
Server 2 198.51.100.100      Enabled Warnings      Local7 <---- legacy server
```

```
Server 3 none                Disabled Critical      Local7
```

```
sources
faults: Enabled
audits: Enabled
events: Disabled
```

- Firepower Chassis Manager(FCM)User Interface(UI)> Platform Settings > Syslogでsyslogサーバ設定が表示されません。



fcm\_syslogs\_configuration.png (すべてのバージョンのインストール)

ステップ 3syslogサーバの変更または削除を試みます。

```
<#root>
device#

scope monitoring

device /monitoring #

delete

<---
snmp-trap  SNMP trap hostname or IP address
snmp-user  SNMPv3 User

device /monitoring #

set syslog

<---
console  Console
file     File
platform Platform

device /monitoring #

set syslog platform

<---
level  Level
```

結論として、FXOS CLIもFCM UIも、198.51.100.100を含むsyslogサーバを作成、変更、または削除する方法を提供していません。

## 原因

次の3つのソフトウェア不具合を検討してください。

Cisco Bug ID CSCvn19025

この不具合の修正が適用されたソフトウェアバージョンでは、CLIまたはFCM UIでFXOSリモー

トsyslog設定を行うことができません。

Cisco Bug ID CSCvt85766

この不具合を修正すると、FXOSのshow syslogコマンドの出力から「リモート接続先」セクションが削除されます。

修正のないバージョン：

```
<#root>
```

```
device#
```

```
scope monitoring
```

```
device /monitoring #
```

```
show syslog
```

```
console
```

```
state: Enabled  
level: Critical
```

```
platform
```

```
state: Enabled  
level: Information
```

```
file
```

```
state: Enabled  
level: Critical  
name: messages  
size: 4194304
```

```
remote destinations <-----
```

| Name     | Hostname  | State    | Level       | Facility |
|----------|-----------|----------|-------------|----------|
| Server 1 | 192.0.2.1 | Enabled  | Information | Local7   |
| Server 2 | 192.0.2.2 | Enabled  | Information | Local7   |
| Server 3 | none      | Disabled | Critical    | Local7   |

```
sources
```

```
faults: Enabled  
audits: Enabled  
events: Disabled
```

修正済みのバージョンには、「リモート接続先」セクションがありません。

```
<#root>
```

```
device #
```

```
scope monitoring
```

```
device /monitoring #
```

```
show syslog
```

```
console
```

```
state: Enabled  
level: Critical
```

```
platform
```

```
state: Enabled  
level: Information
```

| Name     | Hostname  | State    | Level       | Facility |
|----------|-----------|----------|-------------|----------|
| Server 1 | 192.0.2.1 | Enabled  | Information | Local7   |
| Server 2 | 192.0.2.2 | Enabled  | Information | Local7   |
| Server 3 | none      | Disabled | Critical    | Local7   |

```
sources
```

```
faults: Enabled  
audits: Enabled  
events: Disabled
```

「リモート接続先」セクションが欠落しているにもかかわらず、「プラットフォーム」セクションにsyslogサーバが表示されます。

Cisco Bug ID CSCwu12470

Cisco Bug ID [CSCvn19025](#)の修正でバージョンをソフトウェアにアップグレードすると、リモートsyslogサーバの作成、変更、または削除をFXOS CLIまたはFCM UIで管理できなくなります。この制限は、アップグレード前に設定されたサーバにも適用されます。それにもかかわらず、ソフトウェアのアップグレード後、FXOSソフトウェアではshow syslogコマンド出力の「platform」セクションにsyslogサーバが表示され、これらのサーバにsyslogメッセージが送信されます。ユーザは、既存のFXOSリモートsyslog設定を管理できません。この問題は、Cisco Bug ID [CSCwu12470](#)で追跡されています。

## 関連コンテンツ

- Cisco Bug ID [CSCvn19025](#)
- Cisco Bug ID [CSCvt85766](#)
- Cisco Bug ID [CSCwu12470](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。