

SireSIGHT システムの光管理 (LOM) で問題を解決して下さい

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[LOM に接続できない](#)

[設定を確認して下さい](#)

[接続の確認](#)

[LOM インターフェイスへの接続がリブート中に解除される](#)

概要

光管理 (LOM) を設定する、およびそれらをステップバイステップで解決する方法をかもしれないときこの資料に現われるさまざまな現象をおよびエラーメッセージを提供されています。LOM はアプライアンスの Web インターフェイスにログインしないでリモートで監視するか、または管理しますアプライアンスを LAN (SOL) Management Connection 上のアウトオブバンドシリアルを使用することを可能にします。ビューのような限られたタスクを、シャーシシリアル番号行うかまたはファン速度および温度のような条件を監視できます。

前提条件

要件

Cisco は SireSIGHT システムおよび LOM のナレッジがあることを推奨します。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- FireSIGHT 管理センター
- FirePOWER 7000 シリーズ機器、8000 シリーズ機器
- ソフトウェア バージョン 5.2 以降

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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

LOM に接続できない

LOM と FirePOWER FireSIGHT Management Center がアプライアンスに接続することができな

いかかもしれません。 Connection 要求はこれらのエラーメッセージと失敗するかもしれません:

```
Error: Unable to establish IPMI v2 / RMCP+ session Error
```

```
Info: cannot activate SOL payload with encryption
```

次のセクションは LOM への LOM 設定および接続がインターフェイスすることを確認する方法を記述します。

設定を確認して下さい

ステップ 1: 確認し、LOM がイネーブルになって、マネージメントインターフェイスより別の IP アドレスを使用することを確認して下さい。

ステップ 2: UDP ポート 623 が双方向に開いていること、そしてルーティングが正しく設定されることをネットワーク チームと確認して下さい。 LOM が UDP ポートにはたらくので、ポート 623 上の LOM IP アドレスに Telnet で接続することができません。しかし、代替ソリューション デバイスが IPMIPING ユーティリティと IPMI を話す場合テストすることです。

IPMIPING 送信は UDP ポート 623 の得チャンネル認証機能要求データグラムによって 2 IPMI チャンネル認証機能コールを受信します (UDP および接続を使用するので 2 つの要求は保証されません。)

注: デバイスが UDP ポート 623 で受信するかどうか確認するより広範なテストに関しては、NMAP スキャンを使用して下さい。

ステップ 3: LOM の IP アドレスに ping できるか確認します。 は適当なアプライアンスの としてそうでなかったら、このコマンドを実行し、設定が正しいことを確認します。 次に例を示します。

```
ipmitool lan print
```

```
Set in Progress      : Set Complete
Auth Type Support    : NONE MD5 PASSWORD
Auth Type Enable     : Callback : NONE MD5 PASSWORD
                    : User       : NONE MD5 PASSWORD
                    : Operator  : NONE MD5 PASSWORD
                    : Admin     : NONE MD5 PASSWORD
                    : OEM       :
IP Address Source    : Static Address
IP Address           : 192.0.2.2
Subnet Mask          : 255.255.255.0
MAC Address          : 00:1e:67:0a:24:32
SNMP Community String : INTEL
IP Header            : TTL=0x00 Flags=0x00 Precedence=0x00 TOS=0x00
BMC ARP Control      : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Intrvl : 0.0 seconds
Default Gateway IP   : 192.0.2.1
Default Gateway MAC  : 00:00:00:00:00:00
Backup Gateway IP    : 0.0.0.0
Backup Gateway MAC   : 00:00:00:00:00:00
802.1q VLAN ID       : Disabled
802.1q VLAN Priority : 0
RMCP+ Cipher Suites  : 1,2,3,6,7,8,11,12,0
Cipher Suite Priv Max : XaaaXXaaaXXaaXX
                    : X=Cipher Suite Unused
```

```
: c=CALLBACK
: u=USER
: o=OPERATOR
: a=ADMIN
: O=OEM
```

接続の確認

ステップ 1: このコマンドを使用して接続できますか。

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin sdr
```

次のエラーメッセージが表示されますか。

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin sdr
```

注: 正しい IP アドレスへの、しかし間違っただ信任状が付いている接続は以前のエラーと、すぐに失敗します。無効な IP アドレスで LOM に接続する試みは約 10 秒後に時間を計り、このエラーを返します。

ステップ 2: このコマンドで接続することを試みて下さい:

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin sdr
```

ステップ 3: このエラーを得ますか。

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin sdr
```

は今このコマンドで接続することを試みます (これは使用するために暗号スイートを規定します):

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

ステップ 4: まだ接続できませんか。このコマンドで接続することを試みて下さい:

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

詳細出力でこのエラーを見ますか。

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

ステップ 5: GUI 経由で Admin パスワードを変更して、やり直してみてください。

まだ接続できませんか。このコマンドで接続することを試みて下さい:

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

詳細出力でこのエラーを見ますか。

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

ステップ 6: > ローカルコンフィギュレーション > ユーザマネージメント 『User』 を選択して下さい

- 新しい TestLomUser を作成します。
- [User Role Configuration] で [Administrator] をオンにします。
- [Allow Lights-out Management Access] をオンにします。

User Configuration

User Name	<input type="text" value="TestLomUser"/>	
Authentication	<input type="checkbox"/> Use External Authentication Method	
Password	<input type="password" value="●●●●●●●●"/>	
Confirm Password	<input type="password" value="●●●●●●●●"/>	
Maximum Number of Failed Logins	<input type="text" value="5"/>	(0 = Unlimited)
Minimum Password Length	<input type="text" value="5"/>	
Days Until Password Expiration	<input type="text" value="0"/>	(0 = Unlimited)
Days Before Password Expiration Warning	<input type="text" value="0"/>	
Options	<input type="checkbox"/> Force Password Reset on Login	
	<input type="checkbox"/> Check Password Strength	
	<input type="checkbox"/> Exempt from Browser Session Timeout	
Administrator Options	<input checked="" type="checkbox"/> Allow Lights-Out Management Access	

User Role Configuration

Sourcefire User Roles	<input checked="" type="checkbox"/> Administrator <input checked="" type="checkbox"/> External Database User <input checked="" type="checkbox"/> Security Analyst <input type="checkbox"/> Security Analyst (Read Only) <input checked="" type="checkbox"/> Security Approver <input checked="" type="checkbox"/> Intrusion Admin <input checked="" type="checkbox"/> Access Admin <input checked="" type="checkbox"/> Network Admin <input checked="" type="checkbox"/> Maintenance User <input checked="" type="checkbox"/> Discovery Admin
Custom User Roles	<input type="checkbox"/> Intrusion Admin- Test Jose - Intrusion policy read only accesws <input type="checkbox"/> test <input type="checkbox"/> Test Armi

適当なアプライアンスの CLI で、これらのコマンドを定着させ、実行する特権を増やして下さい。
 。 は TestLomUser 第 3 行のユーザであることを確認します。

```
ipmitool user list 1
```

```
ipmitool user list 1
```

3 行目のユーザを admin に変更します。

```
ipmitool user set name 3 admin
```

適切なアクセス レベルを設定します。

```
ipmitool channel setaccess 1 3 callin=on link=on ipmi=on privilege=4
```

新しい admin ユーザのパスワードを変更します。

```
ipmitool user set password 3
```

は設定が正しいことを確認します。

```
ipmitool user list 1
```

```
ipmitool user list 1
```

SOL が正しいチャンネル (1) とユーザ (3) に対して有効になっていることを確認します。

```
ipmitool sol payload enable 1 3
```

ステップ 7: IPMI プロセスが悪い状態にないようにして下さい。

```
pmtool status | grep -i sfipmid
```

```
sfipmid (normal) - Running 2928 Command: /usr/local/sf/bin/sfipmid -t 180 -p power PID File: /var/sf/run/sfipmid.pid Enable File: /etc/sf/sfipmid.run
```

サービスを再起動する。

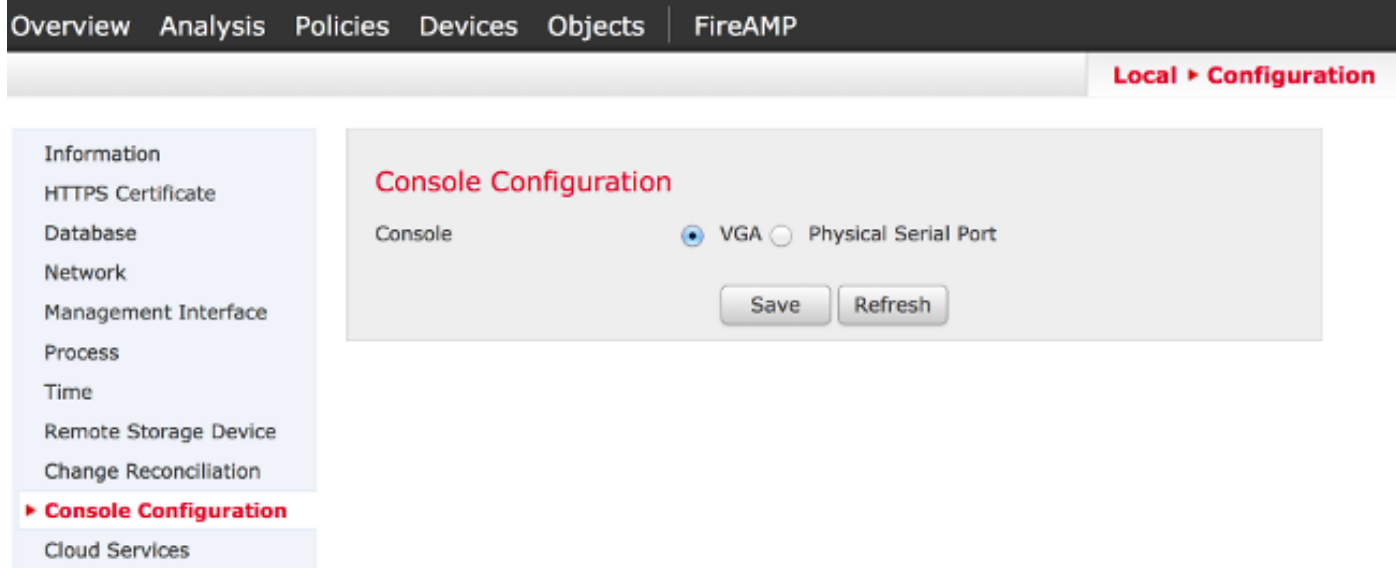
```
pmtool restartbyid sfipmid
```

PID が変更されていることを確認します。

```
pmtool status | grep -i sfipmid
```

```
sfipmid (normal) - Running 20590  
Command: /usr/local/sf/bin/sfipmid -t 180 -p power  
PID File: /var/sf/run/sfipmid.pid  
Enable File: /etc/sf/sfipmid.run
```

ステップ 8: GUI の LOM を無効にし、そしてアプライアンスをリブートして下さい。アプライアンスの GUI で、ローカル > 設定 > コンソール設定を選択して下さい。VGA を選択し、『SAVE』をクリックし、リブートするために『OK』をクリックして下さい。



その後、GUI の LOM を有効にし、そしてアプライアンスをリブートして下さい。アプライアンスの GUI で、ローカル > 設定 > コンソール設定を選択して下さい。物理的なシリアルポートか LOM を選択し、『SAVE』をクリックし、リブートするために『OK』をクリックして下さい

。

ここで、再接続を試みます。

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

ステップ 9： デバイスをシャットダウンし、電源の再投入を、すなわち、物理的に取除き 1 分用の電源コードを、差し込み、次に動力を与えます完了して下さい。アプライアンスが作動した後は十分にこのコマンドを実行します：

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

ステップ 10： 疑わしいアプライアンスからこのコマンドを実行して下さい。これはとりわけ bmc のコールドリセットをします：

```
ipmitool bmc reset cold
```

ステップ 11： デバイスと同じローカルネットワークのシステムからこのコマンドを実行して下さい (すなわち、パススルーはあらゆる中間ルータ)：

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin power status
```

```
arp -an > /var/tmp/arpcache
```

BMC が ARP 要求に応答したかどうか確認するために Cisco テクニカル サポートを /var/tmp/arpcache 生じるファイル送信して下さい。

LOM インターフェイスへの接続がリブート中に解除される

FireSIGHT Management Center が FirePOWER アプライアンスをリブートするとき、アプライアンスへの接続は失われるかもしれません。CLI によってアプライアンスをリブートすることがここに示されている場合の出力：

```
admin@FireSIGHT:~$ sudo shutdown -r now
```

```
Broadcast message from root (ttyS0) (Tue Nov 19 19:40:30 Stopping Sourcefire 3D
Sensor 7120...nfemsg: Host ID 1 on card 0 endpoint 1 de-registering ... nfemsg: Host ID 2 on
card 0 endpoint 1 de-registering ... nfemsg: Host ID 27 on card 0 endpoint 1 de-registering
.....ok Stopping Netronome Flow Manager: nfemsg: Fail callback unregistered Unregistered NFM
fail hook handler nfemsg: Card 0 Endpoint #1 messaging disabled nfemsg: Module EXIT WARNING:
Deprecanfp nfp.0: [ME] CSR access problem for ME 25 ted config file nfp nfp.0: [vPCI] Removed
virtual device 01:00.4 /etc/modprobe.conf, all config files belong into /etc/modprobe.d/.
success. No NMSB present: logging unnecessary...[-10G[ OK ].. Turning off swapfile
/Volume/.swaptwo
[-10G[ OK ] other currently mounted file systems...
Unmounting fuse control filesystem.
Un
```

強調表示された出力 **Unmounting fuse control filesystem.** アプライアンスへの接続が FireSIGHT システムがに接続されるスイッチでイネーブルになっている Spanning Tree Protocol (STP) が中断した原因であることを示します。管理対象装置リブートが、このエラー下記のように表示されれば：

```
admin@FireSIGHT:~$ sudo shutdown -r now
```

```
Broadcast message from root (ttyS0) (Tue Nov 19 19:40:30 Stopping Sourcefire 3D
```

```
Sensor 7120...nfemsg: Host ID 1 on card 0 endpoint 1 de-registering ... nfemsg: Host ID 2 on
card 0 endpoint 1 de-registering ... nfemsg: Host ID 27 on card 0 endpoint 1 de-registering
.....ok Stopping Netronome Flow Manager: nfemsg: Fail callback unregistered Unregistered NFM
fail hook handler nfemsg: Card 0 Endpoint #1 messaging disabled nfemsg: Module EXIT WARNING:
Deprecanfp nfp.0: [ME] CSR access problem for ME 25 ted config file nfp nfp.0: [vPCI] Removed
virtual device 01:00.4 /etc/modprobe.conf, all config files belong into /etc/modprobe.d/.
success. No NMSB present: logging unnecessary...[-10G[ OK ].. Turning off swapfile
/Volume/.swaptwo
[-10G[ OK ] other currently mounted file systems...
Unmounting fuse control filesystem.
Un
```

注: LOM/SOL とアプライアンスに接続できる前にデバイスのマネージメントインターフェイスに接続されるあらゆるサード・パーティ切り替え装置の Spanning Tree Protocol (STP) を無効にして下さい。

FireSIGHT System の LOM 接続は管理ポートと共有されます。管理ポートのリンクがリブート中に瞬間的にドロップされます。リンクがダウンしてからアップするため、ポート上での STP の設定によって引き起こされるスイッチポート状態のリスニングまたは学習が原因となって、スイッチポート内の遅延 (通常は、トラフィックの転送を開始する前の 30 秒) がトリガーされる可能性があります。