

FireSIGHT システムの Lights-Out Management (LOM) に伴う問題のトラブルシューティング

内容

[概要](#)

[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](#)

[設定の確認](#)

[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

このドキュメントでは、Lights-Out-Management (LOM) の設定時に出現するさまざまな現象とエラーメッセージ、およびそれらを段階的にトラブルシューティングする方法を示します。LOM を使用すれば、アプライアンスの Web インターフェイスにログインせずに、アウトオブバンド Serial over LAN (SOL) 管理接続を使用して、アプライアンスをリモートで監視または管理することができます。シャーシのシリアル番号の確認や、ファンの速度や温度などの状態の監視など、限られたタスクを実行できます。

前提条件

要件

FireSIGHT システムと LOM に関する知識があることが推奨されます。

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 アプライアンス、8000 シリーズ アプライアンス
- ソフトウェア バージョン 5.2 以降

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、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。

LOM に接続できない

LOM を使用して FireSIGHT Management Center または FirePOWER アプライアンスに接続できない場合があります。接続要求が次のエラー メッセージを表示して失敗します。

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

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

次の項では、LOM の設定と LOM インターフェイスへの接続を確認する方法について説明します。

設定の確認

ステップ 1 : LOM が有効になっており、管理インターフェイスとは別の IP アドレスを使用していることを確認します。

ステップ 2 : UDP ポート 623 が双方向で開いており、ルートが正しく設定されていることをネットワーク チームと一緒に確認します。LOMはUDPポート上で動作するため、ポート623経由で LOM IPアドレスにTelnet接続できません。ただし、デバイスがIPMIPINGユーティリティを使用してIPMIと通信するかどうかをテストする別のソリューションがあります。IPMIPING は、UDP ポート 623 で、Get Channel Authentication Capabilities 要求データグラムを介して 2 つの IPMI Get Channel Authentication Capabilities コールを送信します (要求を 2 つ送信するのは、UDP が使用されていて接続が保証されないためです) 。

注 : デバイスが UDP ポート 623 でリッスンするかどうかを確認するために、より詳細なテストを実施するには、NMAP スキャンを使用します。

ステップ 3 : LOM の IP アドレスに ping できるか確認します。そうでない場合は、該当するアプライアンスでrootユーザとしてこのコマンドを実行し、設定が正しいことを確認します。たとえば、

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 : 次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。

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

注 : 正しい IP アドレスに接続したが、クレデンシャルが間違っていた場合は、上記エラーが表示されて、ただちに失敗します。無効な IP アドレスで LOM に接続しようとする、約 10 秒後にタイムアウトし、このエラーが返されます。

ステップ 2 : 次のコマンドを使用して接続を試みてください。

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

ステップ 3 : 次のエラーが表示されますか。

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

次のコマンドを使用して接続を試みます (これは、使用する暗号スイートを指定します)。

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

ステップ 4 : まだ接続できない場合は、次のコマンドを使用して接続を試みてください。

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

詳細出力に次のエラーが表示されますか。

```
RAKP 2 HMAC is invalid
```

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。

まだ接続できない場合は、次のコマンドを使用して接続を試みてください。

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

詳細出力に次のエラーが表示されますか。

```
RAKP 2 message indicates an error : unauthorized name
```

ステップ 6 : [ユーザ (User)] > [ローカル設定 (Local Configuration)] > [ユーザ管理 (User Management)] の順に選択します。

- 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:

Authentication: Use External Authentication Method

Password:

Confirm Password:

Maximum Number of Failed Logins: (0 = Unlimited)

Minimum Password Length:

Days Until Password Expiration: (0 = Unlimited)

Days Before Password Expiration Warning:

Options:

- Force Password Reset on Login
- Check Password Strength
- Exempt from Browser Session Timeout

Administrator Options: Allow Lights-Out Management Access

User Role Configuration

Sourcefire User Roles:

- Administrator
- External Database User
- Security Analyst
- Security Analyst (Read Only)
- Security Approver
- Intrusion Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin

Custom User Roles:

- Intrusion Admin- Test Jose - Intrusion policy read only accesws
- test
- Test Armi

該当するアプライアンスの CLI で、自分の権限を root にエスカレートして、次のコマンドを実行します。 TestLomUser が 3 行目のユーザであることを確認します。

```
ipmitool user list 1
```

ID	Name	Callin	Link	Auth	IPMI Msg	Channel	Priv	Limit
1		false	false	true	ADMINISTRATOR			
2	root	false	false	true	ADMINISTRATOR			
3	TestLomUser	true	true	true	ADMINISTRATOR			

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
```

設定が正しいことを確認します。

```
ipmitool user list 1
```

ID	Name	Callin	Link	Auth	IPMI Msg	Channel Priv	Limit
1		false	false	false	true	ADMINISTRATOR	
2	root	false	false	false	true	ADMINISTRATOR	
3	admin	true	true	true	true	ADMINISTRATOR	

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
```

手順 7 : IPMI プロセスが無効な状態ではないことを確認します。

```
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
```

Restart the service.

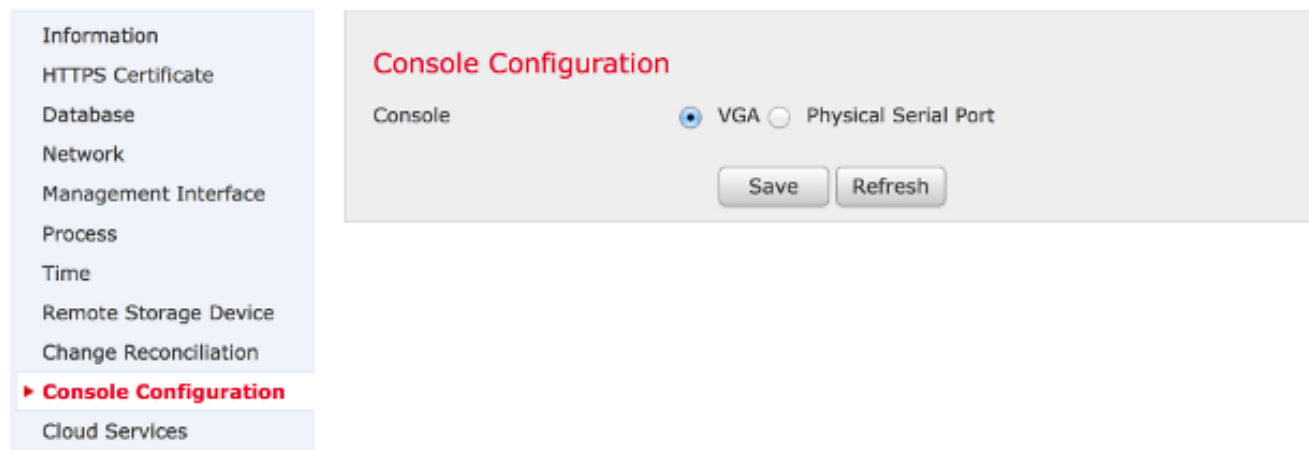
```
pmtool restartbyid sfipmid
```

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 で LOM を無効にしてから、アプライアンスをリブートします。アプライアンスの GUI で、[ローカル (Local)] > [設定 (Configuration)] > [コンソールの設定 (Console Configuration)] の順に選択します。[VGA] を選択して [保存 (Save)] をクリックした後、[OK] をクリックして再起動します。



Information
HTTPS Certificate
Database
Network
Management Interface
Process
Time
Remote Storage Device
Change Reconciliation
▶ Console Configuration
Cloud Services

Console Configuration

Console VGA Physical Serial Port

Save Refresh

その後で、GUI で LOM を有効にしてから、アプライアンスをリブートします。アプライアンスの GUI で、[ローカル (Local)] > [設定 (Configuration)] > [コンソールの設定 (Console Configuration)] の順に選択します。[物理的シリアルポート (Physical Serial Port)] または [LOM] を選択して [保存 (Save)] をクリックしてから、OK をクリックしてリブートします。

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
```

手順 9：デバイスをシャットダウンし、電源を再投入します。つまり、電源ケーブルを1分間物理的に取り外してから、電源をオンにします。アプライアンスの電源がオンになると、次のコマンドが完全に実行されます。

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

手順 10：疑わしいアプライアンスから次のコマンドを実行します。これにより、bmc のコールドリセットが実行されます。

```
ipmitool bmc reset cold
```

ステップ 11：デバイスと同じローカル ネットワーク上にある (つまり、中間ルータを通過しない) システムから次のコマンドを実行します。

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

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

BMC が ARP 要求に応答しているかどうかを判断するために、結果の /var/tmp/arpcache ファイルをシスコ テクニカル サポートに送信します。

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 または FirePOWER アプライアンスをリブートすると、アプライアンスへの接続が失われる場合があります。CLI 経由でアプライアンスをリブートした場合の出力を以下に示します。

```
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.Un** は、FireSIGHT System が接続されたスイッチ上でスパニング ツリー プロトコル (STP) が有効にされたことによってアプライアンスへの接続が解除されたことを示します。管理対象デバイスがリブートすると、次のエラーが表示されます。

```
Error sending SOL data; FAIL
```

```
SOL session closed by BMC
```

注 : LOM/SOL を使用してアプライアンスに接続するには、デバイスの管理インターフェイスに接続されたサードパーティ スイッチング機器でスパニング ツリー プロトコル (STP) を無効にする必要があります。

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。