目次

概要

Lights-Out-Management（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の限られたタスクを実行できます。 このドキュメントでは、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。

前提条件

要件

FireSIGHT System と Lights-Out-Management（LOM）に精通している必要があります。

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くものです。

- 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

注: 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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

LOM に接続できない

Lights-Out Management（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 ErrorInfo: 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。 ポート 623 経由で LOM IP アドレスに Telnet で接続します。

手順 3： LOM の IP アドレスに ping できるか確認します。 できない場合は、該当するアプライアンス上で次のコマンドを root ユーザとして実行し、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
Gratituous ARP Intrvl : 0.0 secondsDefault 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、間違ったクレデンシャルを入力した場合は、上記エラーを表示して失敗します。 無効な IP アドレスで LOM に接続しようとすると、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ます。

ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin sdr
手順 3： 次のエラーが表示されますか。

```
Info: cannot activate SOL payload with encryption
```
ここで、次のコマンドを使用して接続を試みます（これにより、使用する暗号スイートが指定されます）。

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。 次のコマンドを使用して接続を試みます。

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。

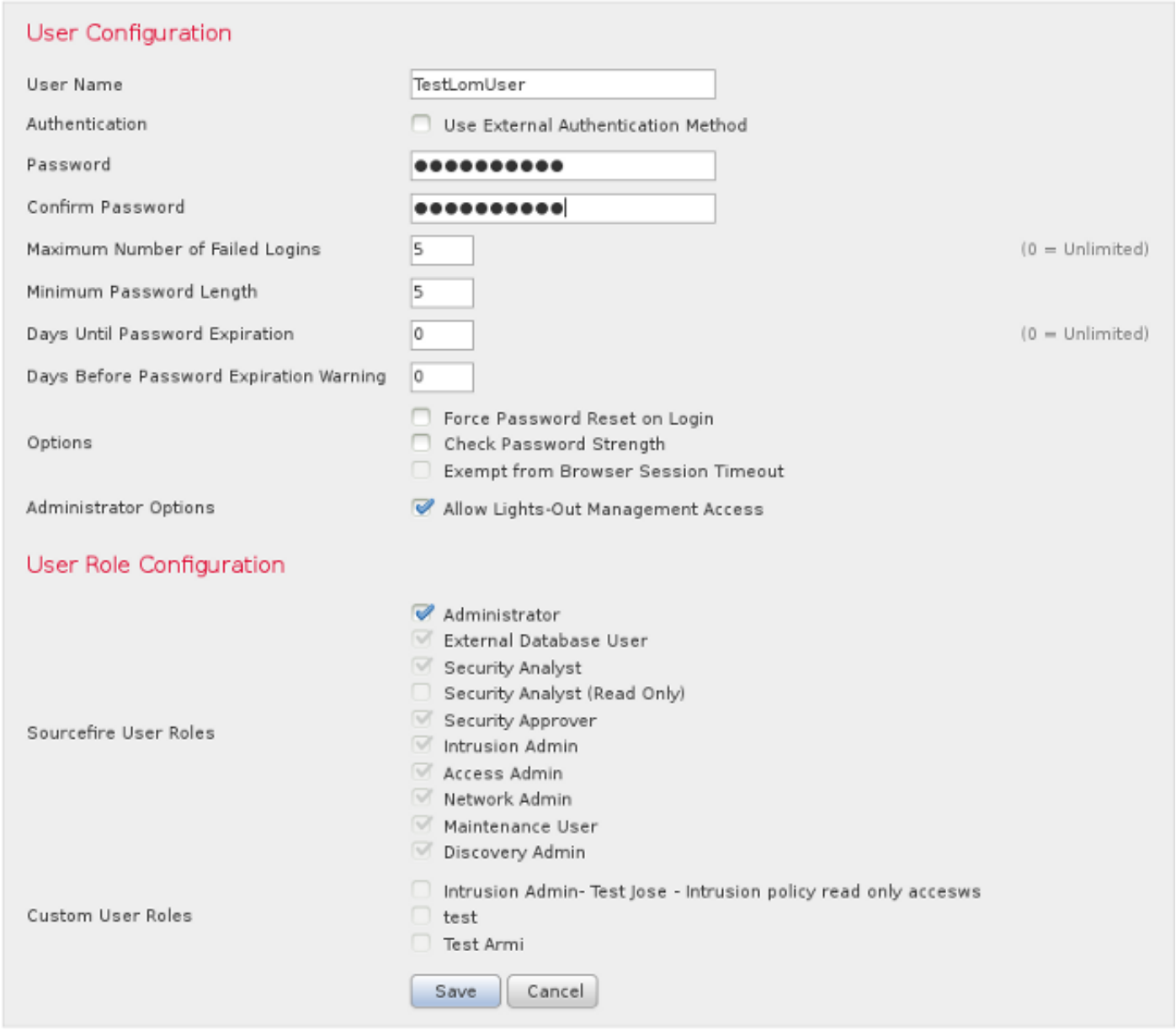
```
RAKP 2 HMAC is invalid
```
ステップ 5： GUI 経由で Admin パスワードを変更して、やり直してみてください。

まだ接続できませんか。 次のコマンドを使用して接続を試みます。

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： [User] > [Local Configuration] > [User Management] に移動します

- 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。



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 true ADMINISTRATOR
```

```
2 root false false true ADMINISTRATOR
3 admin true true true ADMINISTRATOR
```

SOL が正しいチャネル（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 プロセスが異常な状態になってい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
```

サービスを再起動する。

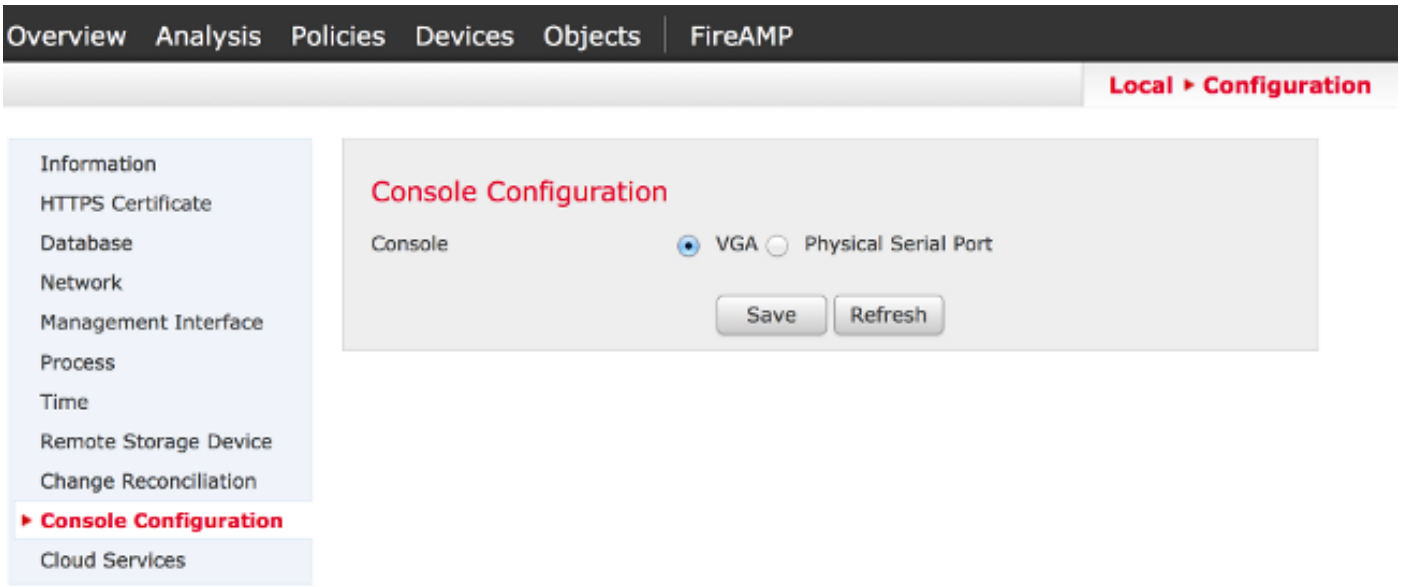
```
pmtool restartbyid sfipmid
```

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 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、[Local] > [Configuration] > [Console Configuration] に移動します。 次に、[VGA] を選択して、[Save] をクリックし、[OK] をクリックして、すぐにリブートします。



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、[Local] > [Configuration] > [Console Configuration] に移動します。 次に、[Physical Serial Port] または [LOM] を選択して、[Save] をクリックし、[OK] をクリックして、すぐにリブートします。

ここで、再接続を試します。

```
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て、電源を再投入、つまり、電源ケーブルを 1 分間物理的に外して、再度接続してから、電源をオンにします。 アプライアンスが完全に起動したら、次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。 コマンドライン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 unecessary...[-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。