

排除故障与灯管理(LOM)的问题在FireSIGHT系统

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[无法连接到LOM](#)

[验证配置](#)

[验证连接](#)

[在重新启动期间，对LOM接口的连接被断开](#)

简介

本文提供也许出现的多种症状和错误消息，当您配置灯管理(LOM)时和如何排除故障他们逐步。LOM允许您使用在LAN (SOL)管理连接的一个带外序列为了远程监控或管理设备，无需登录设备的Web接口。您能执行有限的任务，例如视图机箱序号或监控这样情况象风扇速度和温度。

先决条件

要求

思科建议您有FireSIGHT系统和LOM知识。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- FireSIGHT管理中心
- FirePOWER 7000系列设备，8000系列设备
- 软件版本5.2或以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

无法连接到LOM

您也许无法连接到FireSIGHT管理中心或FirePOWER设备有LOM的。连接请求也许失效与这些错误消息：

```
Error: Unable to establish IPMI v2 / RMCP+ session ErrorInfo: cannot activate SOL payload with encryption
```

下一部分描述如何验证LOM配置，并且对LOM的连接建立接口。

验证配置

步骤 1：验证并且确认LOM比管理接口启用并且使用一个不同的IP地址。

步骤 2：验证与网络团队UDP端口623是开放的双向，并且路由正确地配置。因为LOM在UDP端口工作，您不能远程登录到在端口623的LOM IP地址。如果设备发言IPMI用IPMIPING工具，然而，备选解决方案是测试。IPMIPING发送两个IPMI通过获得信道验证功能获得信道验证功能呼叫在UDP端口623的请求数据包(两请求，因为使用UDP和连接没有保证。)

注意：为了使确认一更加广泛的测验设备是否在UDP端口623监听，请使用NMAP扫描。

步骤 3：能否ping LOM的IP地址？，如果没有，运行此命令作为可适用的设备的root，并且验证设置正确。例如，

```
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
```

验证连接

步骤1:使用此命令，能否连接？

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

是否收到此错误消息？

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

注意：一连接对正确IP地址，但是与错误的凭证，立即失效与上一个错误。尝试连接到LOM在无效的IP地址在大约10秒之后计时并且返回此错误。

步骤2:设法连接此命令：

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

步骤 3：是否收到此错误？

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

当前设法连接此命令(这指定密码器套件使用)：

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

步骤 4：仍然不能连接？设法连接此命令：

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

在冗长的输出中是否看到此错误？

```
RAKP 2 HMAC is invalid
```

步骤 5：通过GUI更改管理员密码，并且再试一次。

仍然不能连接？设法连接此命令：

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

在冗长的输出中是否看到此错误？

RAKP 2 message indicates an error : unauthorized name

步骤 6：选择用户>本地配置>用户管理

- 创建新的TestLomUser
- 检查用户角色配置给管理员
- 检查允许灯管理访问

The screenshot shows a web interface for user configuration. The top section is titled "User Configuration" and includes fields for "User Name" (TestLomUser), "Authentication" (Use External Authentication Method), "Password" and "Confirm Password" (both masked with dots), "Maximum Number of Failed Logins" (5), "Minimum Password Length" (5), "Days Until Password Expiration" (0), and "Days Before Password Expiration Warning" (0). There are also checkboxes for "Options" (Force Password Reset on Login, Check Password Strength, Exempt from Browser Session Timeout) and "Administrator Options" (Allow Lights-Out Management Access). The bottom section is titled "User Role Configuration" and lists "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) and "Custom User Roles" (Intrusion Admin- Test Jose - Intrusion policy read only accesws, test, Test Armi). "Save" and "Cancel" buttons are at the bottom.

在可适用的设备的CLI，请升级您的权限根源和运行这些命令。验证TestLomUser是第三行的用户

。

```
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
```

更改线路的三用户对admin。

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

设置一个适当的访问级别：

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

更改新的密码

```
ipmitool user set password 3
```

验证设置正确。

```
ipmitool user list
```

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			

确保SOL为正确channel(1)和user(3)启用。

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

步骤7：保证IPMI进程不在一坏状态。

```
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
```

[重新启动服务。](#)

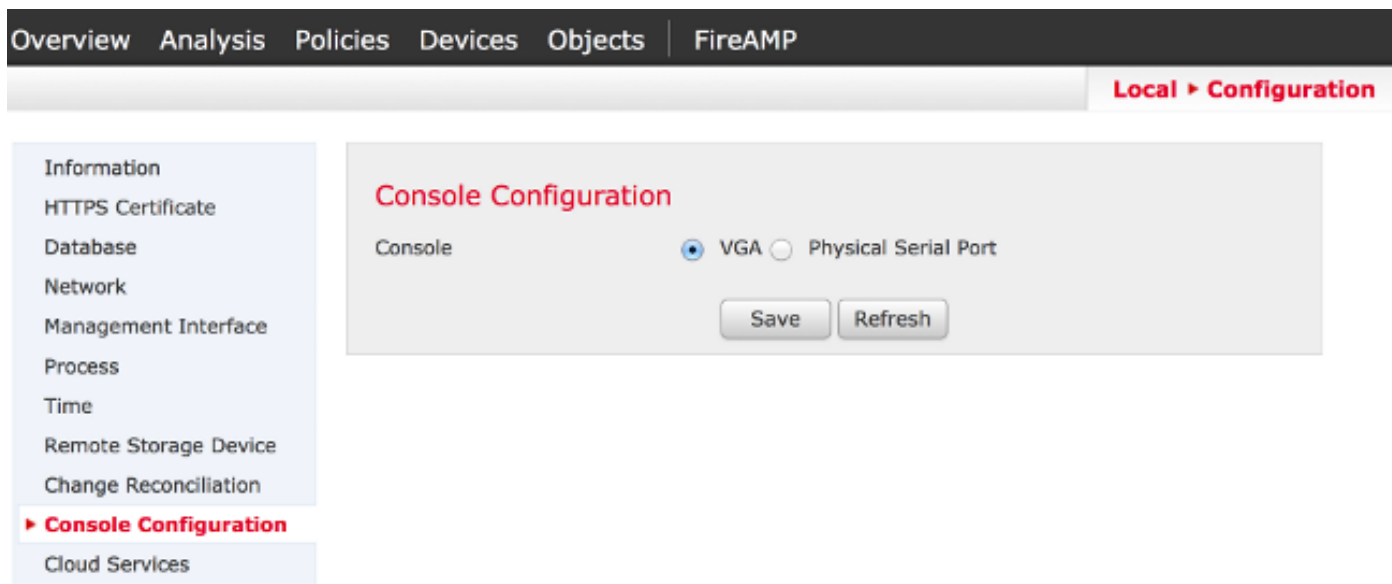
```
pmtool restartbyid sfipmid
```

确认PID更改。

```
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
```

步骤 8:禁用在GUI的LOM，然后重新启动设备。在设备的GUI中，请选择本地> Configuration>控制台配置。选择VGA，点击“Save”，并且点击OK键为了重新启动。



之后，请启用在GUI的LOM，然后重新启动设备。在设备的GUI中，请选择本地> Configuration>控制台配置。选择物理串行端口或LOM，点击“Save”，并且点击OK键重新启动。

现在，请设法再连接。

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

步骤 9：关闭设备并且完成重新通电，即，物理的一分钟的拔掉电源电缆，插入它回到，然后启动。 ，在设备启动后充分地运行此命令：

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

步骤 10：从有问题的设备运行此命令。这特别地执行bmc的冷重置：

```
ipmitool bmc reset cold
```

步骤 11：从在本地网络的一个系统运行此命令和设备一样(即不穿过任何中间路由器)：

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin power status arp -an > /var/tmp/arpcache
```

发送思科技术支持发生的/var/tmp/arpcache文件为了确定BMC是否回答ARP请求。

在重新启动期间，对LOM接口的连接被断开

当您重新启动FireSIGHT管理中心或FirePOWER设备时，对设备的连接也许丢失。输出，当重新启动设备通过CLI显示此处时：

```
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
```

选中项目输出显示对设备的连接中断归结于生成树协议启用在FireSIGHT系统连接的交换机。一旦受管理设备重新启动，此错误显示：

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

```
SOL session closed by BMC
```

注意：在您能连接到有LOM/SOL的前一个设备，您在所有第三方交换设备必须禁用生成树协议连接对设备的管理接口。

FireSIGHT系统的LOM连接用管理端口共享。在重新启动期间，管理端口的链路下降在一个非常短的时间。因为链路断开并且恢复，这可能触发延迟的交换机端口(典型地30秒，在开始通过流量)前由于有造成的侦听的或学习的交换机端口端口状态在端口配置的STP。