在 FireSIGHT 系统上排除远端控制管理 (LOM) 问题

目录

简介

本文档介绍配置远端控制管理 (LOM) 时可能出现的各种症状和错误消息，以及如何逐步对其进行故障排除。通过 LOM，您能够使用带外 LAN 上串行 (SOL) 管理连接，以便远程监控或管理设备，而无需登录设备的 Web 界面。您可以执行有限的任务，例如查看机箱序列号或监控风扇转速和温度等条件。

先决条件

要求

思科建议您拥有与 FireSIGHT 系统和 LOM 相关的知识。

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
- 5.2 或更高软件版本

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

您可能无法使用 LOM 连接到 FireSIGHT 管理中心或 FirePOWER 设备。连接请求可能会失败，并显示以下错误消息：

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

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

下一部分介绍如何验证 LOM 配置及与 LOM 接口的连接。

验证配置

步骤 1：验证并确认已启用 LOM 并使用与管理界面不同的 IP 地址。

步骤 2：与网络团队确认 UDP 端口 623 处于双向打开状态，且路由配置正确。由于LOM在UDP端口上工作，因此您无法通过端口623 Telnet至LOM IP地址。但是，另一种解决方案是测试设备是否使用IPMIPING实用程序说IPMI。IPMIPING 通过 UDP 端口 623 上的 Get Channel Authentication Capabilities 请求数据报发送两个 IPMI Get Channel Authentication Capabilities 调用（两个请求，因其使用 UDP 但不保证连接。）

注意：要进行更广泛的测试以确认设备是否侦听 UDP 端口 623，请使用 NMAP 扫描。

步骤 3：您能否 ping LOM 的 IP 地址？ 如果不是，请在适用的设备上以根用户身份运行此命令，并验证设置是否正确。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
Gratituous 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：您能否使用此命令进行连接？

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

您是否收到此错误消息？

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

> **注意：**与正确 IP 地址的连接（但使用的是错误的凭证）立即失败，并显示上一个错误。约 10 秒后尝试以无效的 IP 地址连接到 LOM 超时并返回此错误。

步骤 2：尝试使用此命令进行连接：

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

步骤 3：您是否收到错误消息？

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

现在尝试使用此命令连接（这指定要使用的密码套件）：

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

步骤 4：仍然无法连接？尝试使用此命令进行连接：

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

在详细输出中，您是否看到此错误？

```
RAKP 2 HMAC is invalid
```

步骤 5：通过 GUI 更改管理员密码，然后重试。

仍然无法连接？尝试使用此命令进行连接：

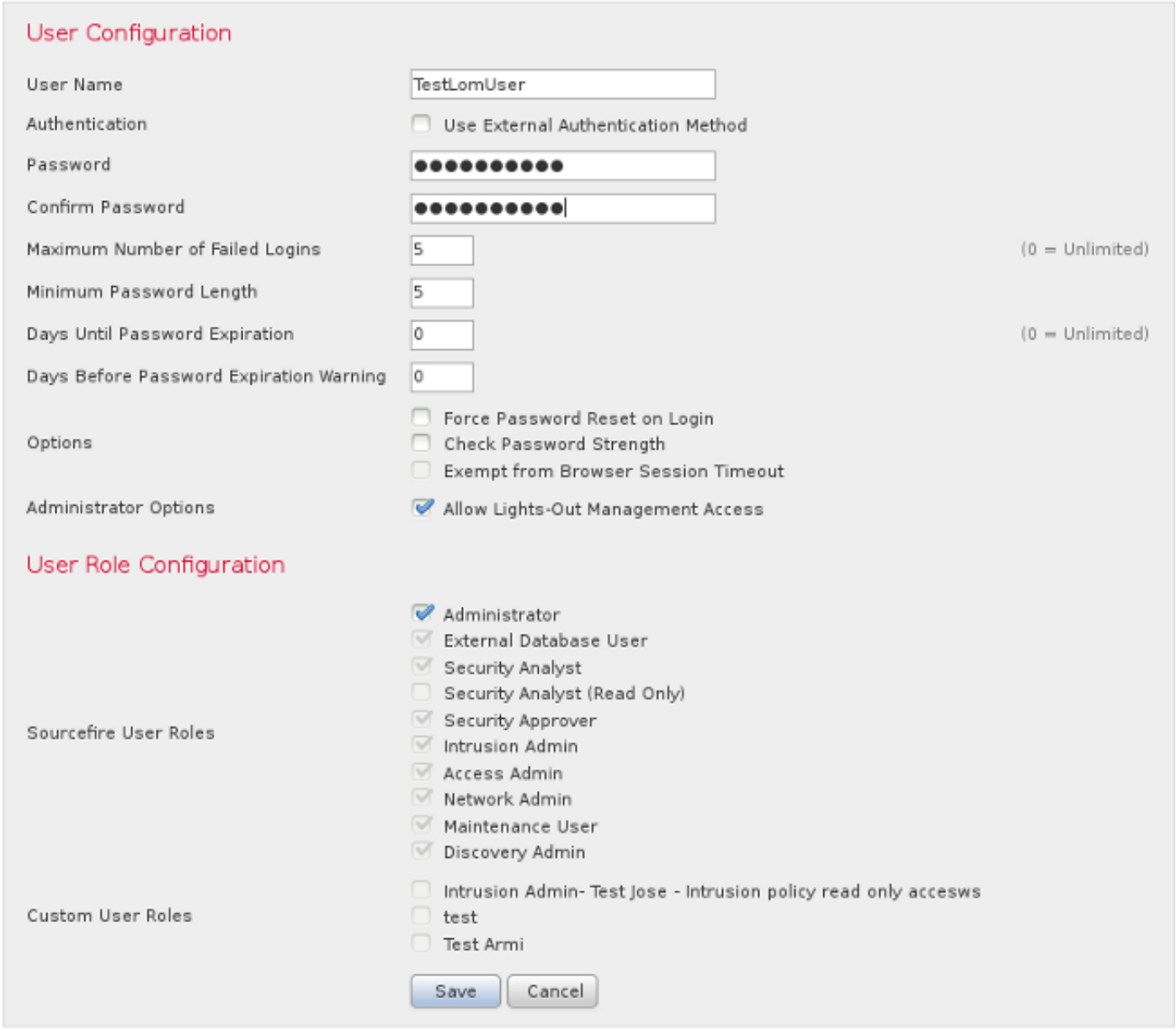
```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

在详细输出中，您是否看到此错误？

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

步骤 6：依次选择用户 > 本地配置 > 用户管理

- 创建新的 TestLomUser
- 向**管理员核实用户角色配置**
- 选中**允许远端控制管理访问**



在适用设备的 CLI 上，将权限升级为 root 并运行这些命令。 验证TestLomUser是第三行上的用户。

```
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
```

将第三行的用户更改为 admin。

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

设置适当的访问级别：

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

更改新 admin 用户的密码

ipmitool user set password 3

验证设置是否正确。

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
```

请确保 SOL 启用于正确的信道 (1) 和用户 (3)。

ipmitool sol payload enable 1 3

步骤 7：确保 IPMI 进程未处于错误状态。

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。

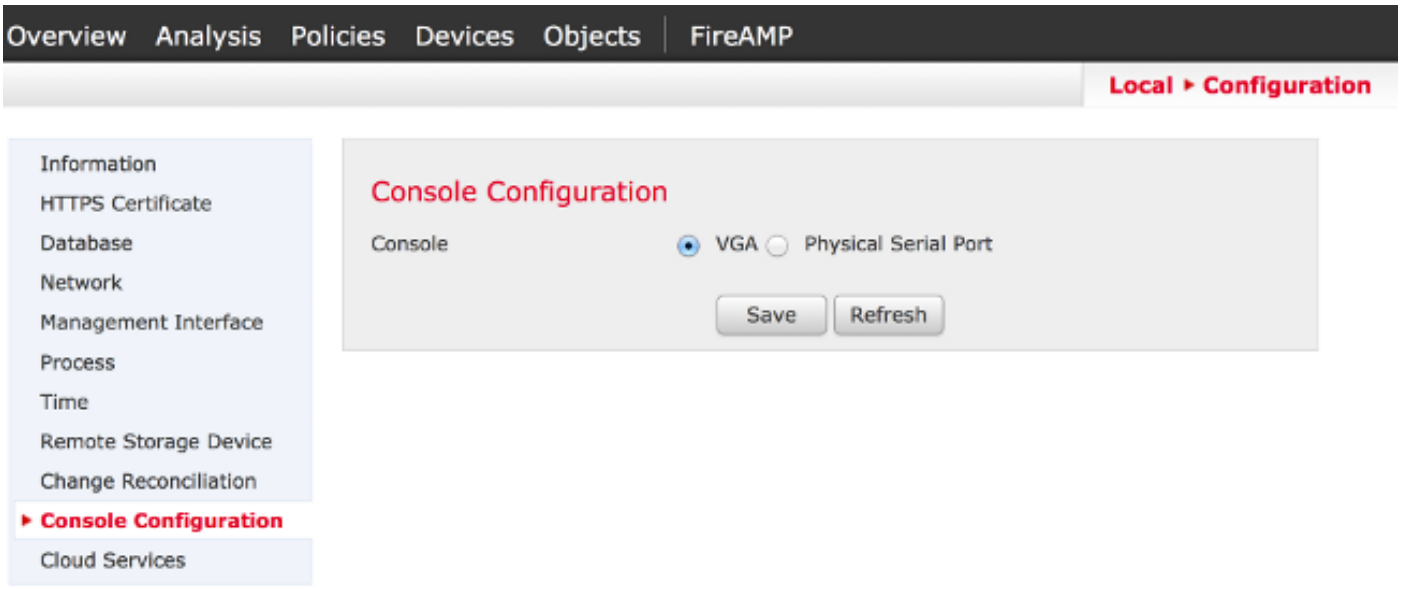
pmtool restartbyid sfipmid

确认 PID 已更改。

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::在 GUI 中禁用 LOM，然后重新启动设备。在设备 GUI 中，依次选择**本地 > 配置 > 控制台配置**。选择 VGA，点击**保存**，然后点击**确定以重新启动。**



然后，在 GUI 中启用 LOM，再重新启动设备。在设备 GUI 中，依次选择**本地 > 配置 > 控制台配置**。 选择**物理串行端口或 LOM，点击保存**，然后点击**确定以重新启动。**

现在，再次尝试连接。

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

步骤 9：关闭设备并完成电源循环，即物理上拔下电源线一分钟，重新插上，然后打开电源。设备完全通电后，运行以下命令：

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

步骤 10：从相关设备运行此命令。该操作会专门执行 bmc 的冷复位：

```
ipmitool bmc reset cold
```

步骤 11：从与设备相同的本地网络上的系统运行此命令（即，不通过任何中间路由器）：

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

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

向思科技术支持发送生成的 /var/tmp/arpcache 文件，以确定 BMC 是否响应 ARP 请求。

重新启动期间与 LOM 接口的连接断开

重新启动 FireSIGHT 管理中心或 FirePOWER 设备时，与设备的连接可能会丢失。通过 CLI 重新启动设备时的输出如下所示：

```
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
```

突出显示的输出 **Unmounting fuse control filesystem.Un 显示，由于在连接 FireSIGHT 系统的交换机上启用了生成树协议 (STP)，与设备的连接中断。**受管设备重新启动后，系统将显示以下错误：

```
Error sending SOL data; FAIL
                              SOL session closed by BMC
```

> **注意：**在使用 LOM/SOL 连接到设备前，必须在连接到设备管理接口的任何第三方交换设备上禁用生成树协议 (STP)。

FireSIGHT 系统的 LOM 连接与管理端口共享。在重新启动期间，管理端口的链路会短暂断开。由于链路断开并重新接通，这可能会触发交换机端口出现延迟（通常延迟 30 秒后再开始传递流量），这是由于在端口上配置了 STP 而导致的侦听或学习交换机端口状态。