

Problemas del Troubleshooting con la Administración de las luces-Hacia fuera (LOM) en los sistemas de FireSIGHT

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Incapaz de conectar con LOM](#)

[Verifique el del de la configuración](#)

[Verifique la conexión](#)

[La conexión a la interfaz LOM es disconnected durante la reinicialización](#)

Introducción

Este documento proporciona los diversos síntomas y mensajes de error que pudieron aparecer cuando usted configura la Luz-Hacia fuera-Administración (LOM), y cómo resolverlos problemas paso a paso. LOM permite que usted utilice un serial fuera de banda sobre la Conexión de Administración LAN (solenoid) para monitorea o maneja remotamente los dispositivos sin la registración en la interfaz Web del dispositivo. Usted puede realizar las tareas limitadas, tales como visión el número de serie del chasis o monitorear las condiciones tales como la velocidad y la temperatura de la fan.

Prerrequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del sistema de FireSIGHT y de LOM.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Centro de administración de FireSIGHT
- Dispositivos de las 7000 Series de FirePOWER, dispositivos de las 8000 Series
- Versión de software 5.2 o más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Incapaz de conectar con LOM

Usted puede ser que no pueda conectar con FireSIGHT un centro de administración o el dispositivo de FirePOWER con LOM. Los pedidos de conexión pudieron fallar con estos mensajes de error:

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

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

La siguiente sección describe cómo verificar una configuración LOM y las conexiones al LOM interconectan.

Verifique el del de la configuración

Paso 1: Verifique y confirme que LOM esté habilitado y utilice una diversa dirección IP que la interfaz de administración.

Paso 2: Verifique con el equipo de la red que el puerto 623 UDP esté abierto bidireccional, y que las rutas están configuradas correctamente. Puesto que LOM trabaja sobre un puerto UDP, usted no puede Telnet a la dirección IP LOM sobre el puerto 623. el del sin embargo, una solución alternativa es probar si el dispositivo habla IPMI con la utilidad IPMIPING. IPMIPING envía dos IPMI consigue las llamadas de las capacidades de la autenticación del canal vía un datagrama de la petición de las capacidades de la autenticación del canal del conseguir en el puerto 623 UDP (dos peticiones puesto que utiliza el UDP y las conexiones no se garantizan.)

Note: Para que una prueba más extensa confirme si el dispositivo escucha en el puerto 623 UDP, utilice la exploración NMAP.

Paso 3: ¿Puede usted hacer ping la dirección IP de LOM? el del si no, funciona con este comando como `usuario raíz` en el dispositivo aplicable, y verifica las configuraciones está correcto. Por ejemplo,

```
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
```

Verifique la conexión

paso 1 del del : Puede usted conectar usando este comando?

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

¿Usted recibe este mensaje de error?

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

Note: Una conexión a la dirección IP correcta, pero con las credenciales incorrectas, falla con el error anterior inmediatamente. Las tentativas de conectar con LOM en una dirección IP no válida miden el tiempo hacia fuera después de cerca de 10 segundos y vuelven este error.

Paso 2 del : Intente conectar con este comando:

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

Paso 3: ¿Usted consigue este error?

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

El ahora intenta conectar con este comando (éste especifica la habitación de la cifra para utilizar):

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

Paso 4: ¿Todavía no puede conectar? Intente conectar con este comando:

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

¿En la salida prolija usted ve este error?

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

Paso 5: Cambie la clave del administrador vía el GUI, e intente otra vez.

¿Todavía no puede conectar? Intente conectar con este comando:

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

¿En la salida prolija usted ve este error?

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

Paso 6: Elija el usuario > la configuración local > User Management (Administración de usuario)

- Cree un nuevo TestLomUser
- Marque el rol del usuario de la configuración al administrador
- El control permite el Acceso de administración de las luces-hacia fuera

The screenshot shows a web interface for user configuration. It is divided into two main sections: "User Configuration" and "User Role Configuration".

User Configuration:

- User Name: TestLomUser
- Authentication: Use External Authentication Method
- Password: [Masked]
- Confirm Password: [Masked]
- Maximum Number of Failed Logins: 5 (0 = Unlimited)
- Minimum Password Length: 5
- Days Until Password Expiration: 0 (0 = Unlimited)
- Days Before Password Expiration Warning: 0
- 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

Buttons: Save, Cancel

En el CLI del dispositivo aplicable, extienda sus privilegios de arraigar y de funcionar con estos comandos. el del verifica que TestLomUser sea el usuario en la tercera línea.

```
ipmitool user list 1
```

```
ipmitool user list 1
```

Cambie al usuario en la línea tres al admin.

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

Fije un nivel de acceso apropiado:

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

Cambie la contraseña del nuevo Usuario administrador

```
ipmitool user set password 3
```

El verifica que las configuraciones estén correctas.

```
ipmitool user list 1
```

```
ipmitool user list 1
```

Asegurese que el solenoide está habilitado para el channel(1) y el user(3) correctos.

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

Paso 7 del : Asegúrese de que el proceso IPMI no esté en un mún estado.

```
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
```

[Reiniciar el servicio.](#)

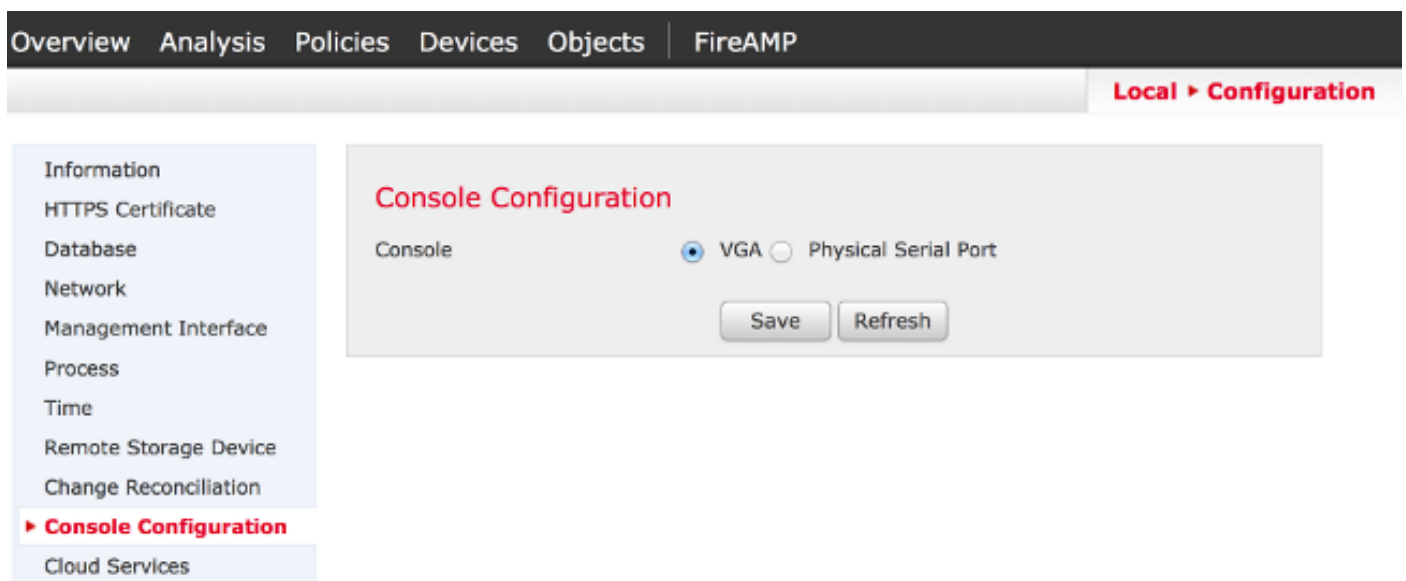
```
pmtool restartbyid sfipmid
```

Confirme que el PID ha cambiado.

```
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
```

Paso 8: Inhabilite el LOM en el GUI, después reinicie el dispositivo. En el GUI del dispositivo, elija el **Local > la configuración > la configuración de la consola**. Seleccione el **VGA**, haga clic la **salvaguardia**, y haga clic la **AUTORIZACIÓN** para reiniciar. del del



Luego, habilite el LOM en el GUI, después reinicie el dispositivo. En el GUI del dispositivo, elija el

Local > la configuración > la configuración de la consola. Elija el puerto de serial física o LOM, haga clic la **salvaguardia**, y haga clic la **AUTORIZACIÓN** para reiniciar.

Ahora, intente conectar otra vez.

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

Paso 9: Apague el dispositivo y complete un ciclo del poder, es decir, quitan físicamente el cable de alimentación eléctrica para un minuto, lo conectan detrás, y después lo accionan encendido. el del después de los poderes del dispositivo para arriba funciona con completamente este comando:

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

Paso 10: Funcione con este comando del dispositivo en la pregunta. Esto hace específicamente una restauración fría del bmc:

```
ipmitool bmc reset cold
```

Paso 11: Funcione con este comando de un sistema en la misma red local que el dispositivo (es decir, no pasa a través de ningún router intermedio):

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

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

Envíe Soporte técnico de Cisco el archivo resultante de `/var/tmp/arpcache` para determinar si el BMC responde a un pedido ARP.

La conexión a la interfaz LOM es disconnected durante la reinicialización

Cuando usted reinicia un centro de administración de FireSIGHT o un dispositivo de FirePOWER, la conexión al dispositivo pudo ser perdida. La salida cuando reiniciar el dispositivo vía el CLI se muestra aquí:

```
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
```

El filesystem resaltado del control del fusible de Unmounting de la salida. La O.N.U muestra que la conexión al dispositivo es interrumpido debido al Spanning Tree Protocol (STP) que es habilitado en el Switch con donde el sistema de FireSIGHT está conectado. Una vez

que los dispositivos administrados reinician, se visualiza este error:

```
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
```

Note: Antes del usted puede conectarse a un dispositivo con LOM/SOL, usted debe inhabilitar el Spanning Tree Protocol (STP) en cualquier equipo de Switching de tercera persona conectado con la interfaz de administración del dispositivo.

Una conexión LOM del sistema de FireSIGHT se comparte con el puerto de administración. El link para el puerto de administración cae por mismo un tiempo breve durante la reinicialización. Puesto que va el link abajo y salvaguardia que viene, éste podría accionar un retardo en el puerto del switch (típicamente 30 segundos antes de que comienza a pasar el tráfico) debido al estado de puerto del switch que escuchaba o de aprendizaje causado teniendo STP configurado en el puerto.