Contenido

Introducción

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

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento en el sistema y la Luz-Hacia fuera-Administración (LOM) de FireSIGHT.

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 la potencia de fuego, dispositivos de las 8000 Series.
- Versión de software 5.2 o más adelante

Nota: 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 no poder conectar con un dispositivo del centro de administración o de la potencia de fuego de FireSIGHT usando la Administración de las luces-Hacia fuera (LOM). Los pedidos de conexión pueden fallar con los mensajes de error siguientes:

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

La sección siguiente describe cómo verificar una configuración y las conexiones LOM la interfaz LOM.

Verifique la configuración

Paso 1: Verifique y confirme que LOM esté habilitado, y está utilizando 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. Telnet a la dirección IP LOM sobre el puerto 623.

Paso 3: ¿Puede usted hacer ping la dirección IP de LOM? Si no, funcione con el siguiente comando como `usuario raíz` en el dispositivo aplicable, y verifique las configuraciones están 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
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
```

Verifique la conexión

Paso 1: ¿Puede usted conectar usando el siguiente comando?

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

¿Usted recibe este mensaje de error?

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

> Nota: La conexión con la dirección IP correcta pero proporcionar a las credenciales incorrectas falla con el error arriba inmediatamente. El intentar conectar con LOM en una dirección IP no válida mide el tiempo hacia fuera después de cerca de 10 segundos y vuelve este error.

Paso 2: Intente conectar usando el siguiente comando:

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

Paso 3: ¿Usted consigue este error?

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

Ahora intente conectar usando el siguiente comando (esto especificará 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 usando el siguiente comando:

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

¿En la salida prolija usted ve el error siguiente?

```
RAKP 2 HMAC is invalid
```

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

¿Todavía no puede conectar? Intente conectar usando el siguiente comando:

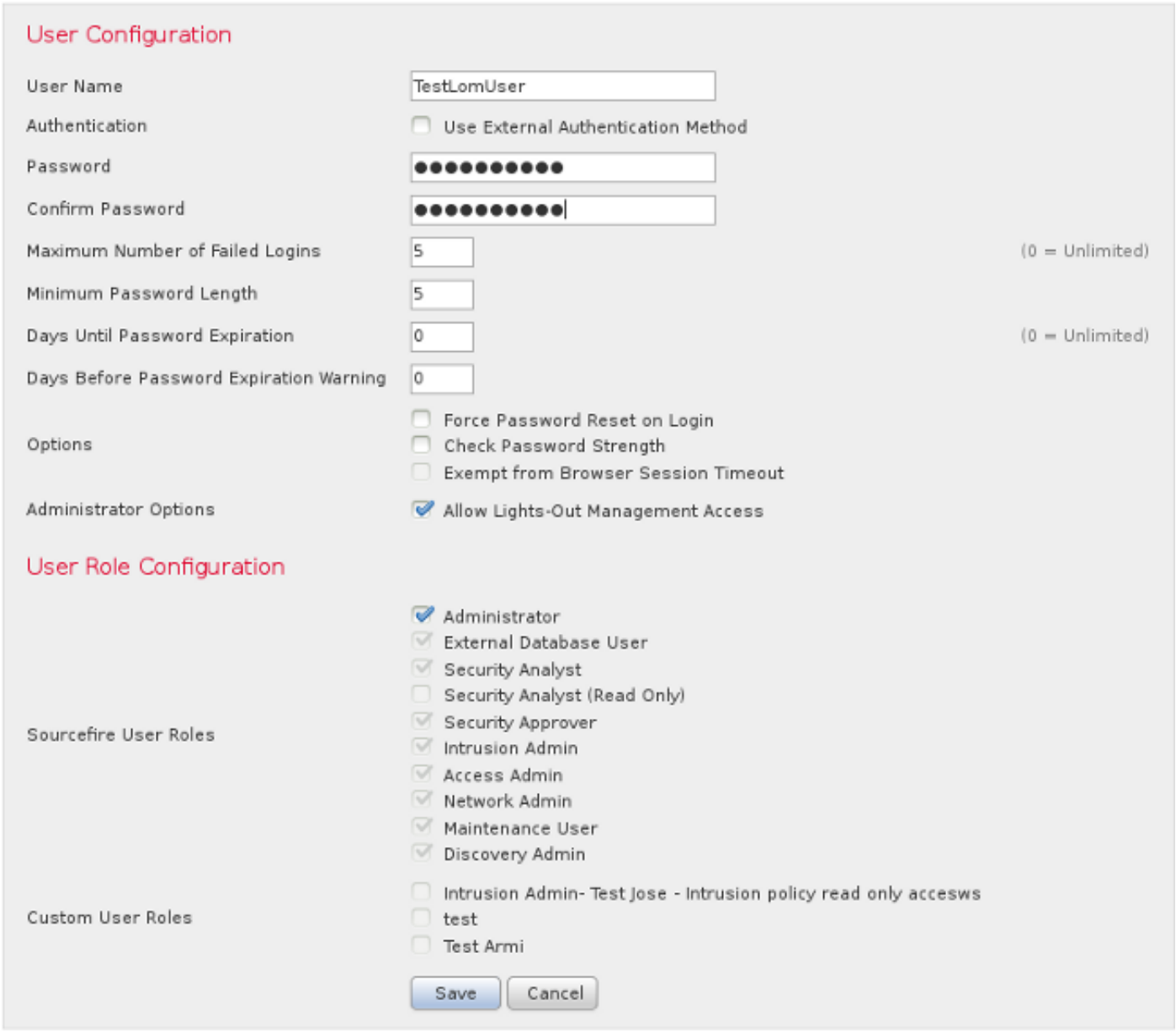
```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

¿En la salida prolija usted ve el error siguiente?

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

Paso 6: Navegue al **usuario > a 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**



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

```
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
```

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
```

Verifique que las configuraciones estén correctas.

```
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
```

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

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

Paso 7: Aseeguremosnos que el proceso IPMI no está 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.

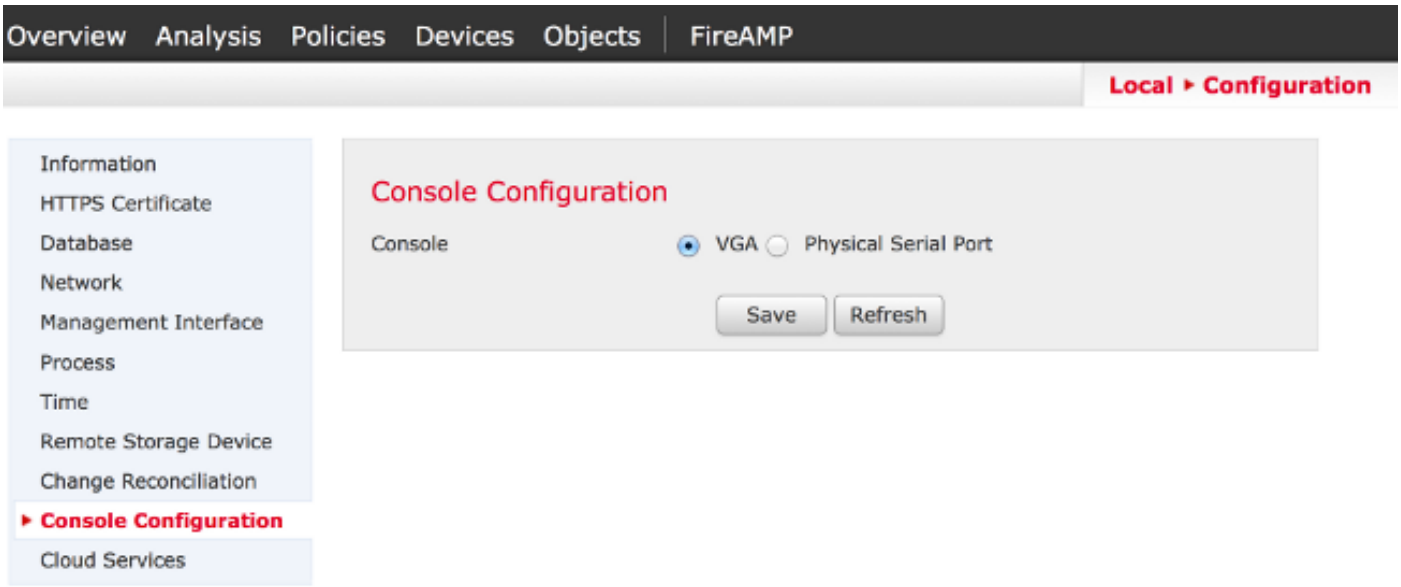
```
pmtool restartbyid sfipmid
```

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 navegue al **Local > a la configuración > a la configuración de la consola**. Después seleccione el **VGA**, haga clic la **salvaguardia** y haga clic la **AUTORIZACIÓN** ahora para reiniciar.



Luego, habilite el LOM en el GUI, después reinicie el dispositivo. En el GUI del dispositivo navegue al **Local > a la configuración > a la configuración de la consola**. Después seleccione el **puerto de serial física** o LOM, haga clic la **salvaguardia** y haga clic la **AUTORIZACIÓN** ahora 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 1 minuto, lo conectan detrás y después lo accionan encendido. Después del dispositivo los poderes para arriba funcionan con completamente el siguiente

comando:

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

Paso 10: Funcione con el siguiente comando del dispositivo en la pregunta. Esto hará específicamente una restauración fría del bmc:

```
ipmitool bmc reset cold
```

Paso 11: Funcione con el siguiente comando de un sistema en la misma red local que el dispositivo (es decir, no pasando a través de cualquier 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 está respondiendo 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 la potencia de fuego, la conexión al dispositivo puede ser perdida. La salida cuando reiniciar el dispositivo vía la línea de comando está abajo:

```
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
```

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 FireSIGHT Syste está conectado. Una vez que los dispositivos administrados reinician, se visualiza el error siguiente:

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

> Nota: Antes del usted puede conectarse a un dispositivo usando 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.