Resuelva problemas con la administración remota (LOM) en sistemas FireSIGHT

Contenido

Introducción

Este documento proporciona los diversos síntomas y mensajes de error que pueden aparecer cuando configura la administración automatizada (LOM) y la forma de solucionar los problemas paso a paso. La LOM permite utilizar una conexión de administración de serie a LAN (SOL) fuera de banda para controlar o administrar de forma remota los dispositivos no conectados a la interfaz web del dispositivo. Se pueden realizar tareas limitadas, como ver el número de serie de chasis o monitorear las condiciones de temperatura y velocidad del ventilador.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre el sistema FireSIGHT y la LOM.

Componentes Utilizados

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

- Centro de administración de FireSIGHT
- Dispositivos FirePOWER de la serie 7000 y dispositivos de la serie 8000
- Software versión 5.2 o posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

No se puede conectar a la LOM

Es posible que no pueda conectarse al Centro de administración de FireSIGHT o a un dispositivo FirePOWER con LOM. Las solicitudes de conexión pueden fallar y mostrar 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 la configuración de la LOM y las conexiones a la interfaz de LOM.

Verificar configuración

Paso 1: Verifique y confirme que la LOM esté habilitada y utilice una dirección IP diferente a la de la interfaz de administración.

Paso 2: Verifique con el equipo de red que el puerto 623 del UDP esté abierto bidireccionalmente y que las rutas se hayan configurado correctamente. Debido a que LOM funciona sobre un puerto UDP, no puede realizar Telnet a la dirección IP de LOM sobre el puerto 623. Sin embargo, una solución alternativa es probar si el dispositivo habla IPMI con la utilidad IPMIPING. IPMIPING envía dos llamadas de funcionalidades de autenticación de obtención de canal de la IPMI a través de un datagrama de solicitud de funcionalidades de autenticación de obtención de canal en el puerto 623 del UDP (dos solicitudes debido a que se utiliza el UDP y las conexiones no están garantizadas).

> **Nota:** Para una prueba más extensa a fin de confirmar si el dispositivo detecta el puerto 623 del UDP, utilice el escaneo del NMAP.

Paso 3: ¿Puede hacer ping en la dirección IP de la LOM? Si no es así, ejecute este comando como usuario raíz en el dispositivo aplicable y verifique que la configuración sea correcta. 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 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: ¿Puede conectarse con este comando?

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

¿Recibió este mensaje de error?

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

> **Nota:** Una conexión a la dirección IP correcta con las credenciales incorrectas falla y muestra inmediatamente el error anterior. Los intentos de conexión a la LOM con una dirección IP no válida dan como resultado un tiempo de espera tras 10 segundos y devuelven este error.

Paso 2: Intente conectarse con este comando:

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

Paso 3: ¿Recibe este error?

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

Ahora intente conectarse con este comando (esto especifica la suite cipher que se utilizará):

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

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

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

En el resultado detallado, ¿ve este error?

```
RAKP 2 HMAC is invalid
```

Paso 5: Cambie la contraseña de Administrador mediante la GUI y vuelva a intentarlo.

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

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

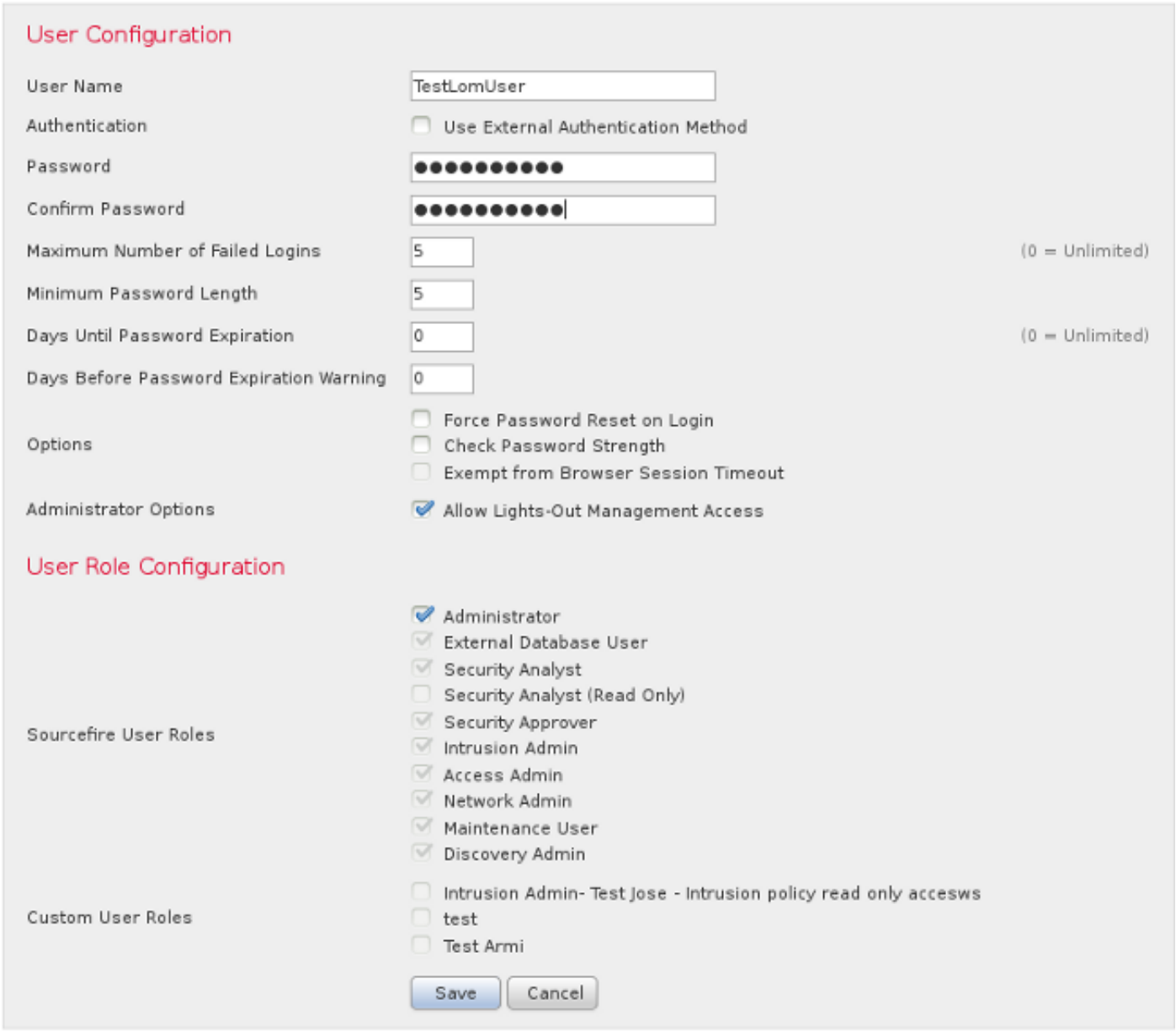
En el resultado detallado, ¿ve este error?

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

Paso 6: Seleccione User > Local Configuration > User Management (Usuario > Configuración

Local > Administración de usuarios).

- Cree un usuario TestLomUser nuevo.
- Marque **User role configuration (Configuración del rol de usuario) en Administrator (Administrador).**
- Marque **Allow Lights-out Management Access (Permitir acceso a la administración automatizada).**



En la CLI del dispositivo correspondiente, amplíe los privilegios a superusuario y ejecute estos comandos. Verifique que TestLomUser sea el usuario de 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 el usuario en la tercera línea a admin.

ipmitool user set name 3 admin

Establezca un nivel de acceso adecuado:

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

Cambie la contraseña del nuevo usuario admin.

ipmitool user set password 3

Verifique que la configuración sea correcta.

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
```

Asegúrese de habilitar la SOL para el canal (1) y el usuario (3) adecuados.

ipmitool sol payload enable 1 3

Paso 7: Asegúrese de que el proceso de la IPMI no esté en mal 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.

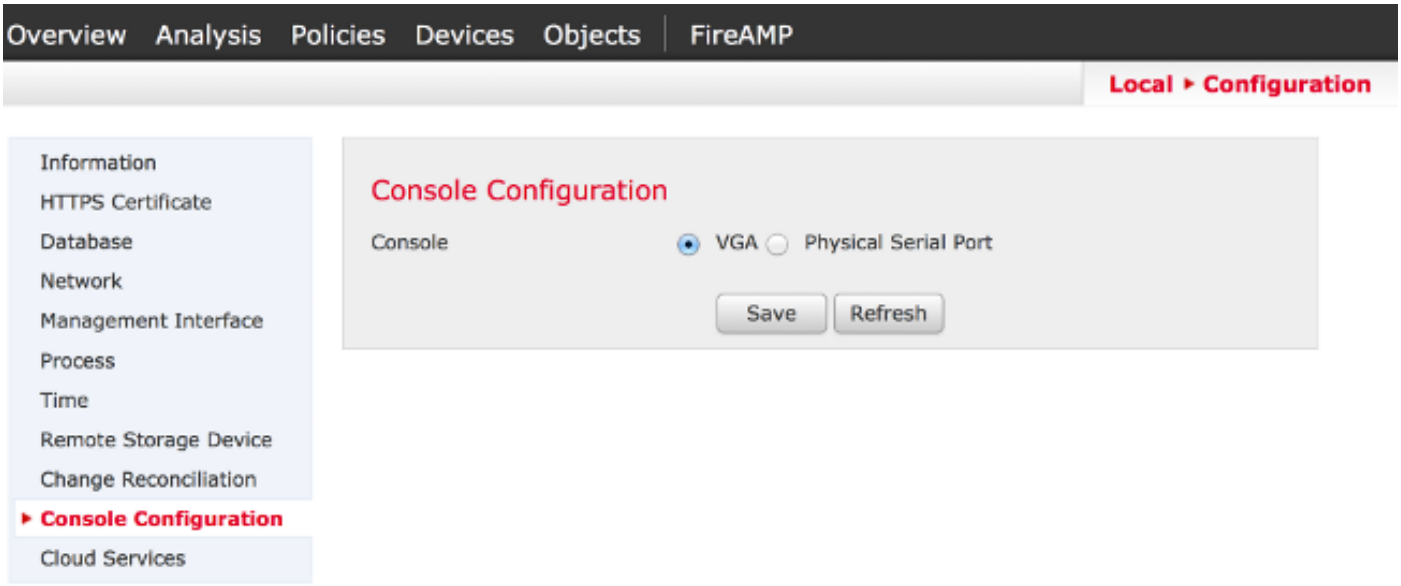
pmtool restartbyid sfipmid

Confirme que el PID haya 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: Deshabilite la LOM en la GUI y reinicie el dispositivo. En la GUI del dispositivo, seleccione **Local > Configuration > Console Configuration (Local > Configuración > Configuración de la consola)**. Seleccione **VGA**, haga clic en **Save (Guardar)** y luego en **OK (Aceptar) para reiniciar.**



Luego habilite la LOM en la GUI y reinicie el dispositivo. En la GUI del dispositivo, seleccione **Local > Configuration > Console Configuration (Local > Configuración > Configuración de la consola)**. Seleccione **Physical Serial Port (Puerto serial físico) o LOM, haga clic en Save (Guardar)** y luego en **OK (Aceptar).**

Ahora intente conectarse de nuevo.

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

Paso 9: Apague el dispositivo y complete un ciclo de alimentación, es decir, extraiga físicamente el cable de alimentación durante un minuto, vuelva a enchufarlo y luego encienda. Después de que el dispositivo se encienda completamente ejecute este comando:

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

Paso 10: Ejecute este comando desde el dispositivo en cuestión. Esto específicamente reinicia en frío el BMC:

```
ipmitool bmc reset cold
```

Paso 11: Ejecute este comando desde un sistema en la misma red local que el dispositivo (no pase por ningún router intermedio):

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

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

Envíe al soporte técnico de Cisco el archivo resultante de /var/tmp/arpcache para determinar si el BMC responde a la solicitud del ARP.

La conexión a la interfaz de LOM se desconecta durante el reinicio

Cuando reinicie el Centro de administración de FireSIGHT o un dispositivo FirePOWER, es posible que se pierda la conexión con el dispositivo. Aquí se muestra el resultado del reinicio del dispositivo mediante la CLI:

```
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 resultado resaltado es **Unmounting fuse control filesystem. Un muestra que la conexión con el dispositivo se interrumpe debido a que el protocolo de árbol de expansión (STP) está habilitado en el switch donde se conecta el sistema FireSIGHT.** Una vez que los dispositivos administrados se reinician, se muestra este error:

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

> **Nota:** Antes de conectarse a un dispositivo mediante la LOM/SOL, debe deshabilitar el protocolo de árbol de expansión (STP) en cualquier equipo de switching de terceros conectado a la interfaz de administración del dispositivo.

La conexión de la LOM del sistema FireSIGHT se comparte con el puerto de administración. El enlace del puerto de administración cae durante un período muy breve en el reinicio. Dado que el enlace cae y regresa, se puede activar una demora en el puerto de switch (generalmente 30 segundos antes de que comience a circular tráfico) debido al estado de audición o conocimiento del puerto de switch ocasionado por el STP configurado en el puerto.