Solução de problemas com Lights-Out Management (LOM) em sistemas FireSIGHT

Contents

Introduction

Este documento fornece vários sintomas e mensagens de erro que podem aparecer quando você configura o Lights-Out-Management (LOM) e como solucioná-los passo a passo. O LOM permite usar uma conexão de gerenciamento Serial over LAN (SOL) fora da banda para monitorar ou gerenciar remotamente do dispositivo, sem fazer login na interface da Web do dispositivo. Você pode executar tarefas limitadas, como visualizar o número de série do chassi ou monitorar condições como velocidade e temperatura do ventilador.

Prerequisites

Requirements

A Cisco recomenda que você conheça o sistema FireSIGHT e LOM.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- FireSIGHT Management Center
- FirePOWER 7000 Series Appliances, 8000 Series Appliances
- Versão do software 5.2 ou 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.

Não é possível se conectar ao LOM

Você pode não conseguir se conectar a um FireSIGHT Management Center ou FirePOWER Appliance com LOM. As solicitações de conexão podem falhar com essas mensagens de erro:

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

Info: cannot activate SOL payload with encryption
```

A próxima seção descreve como verificar uma configuração LOM e conexões com a interface LOM.

Verifique a configuração

Passo 1: Verifique e confirme que o LOM está ativado e usa um Endereço IP diferente da interface de gerenciamento.

Passo 2: Verifique com a equipe de rede se a porta UDP 623 está bidirecionalmente aberta e se as rotas estão configuradas corretamente. Como o LOM funciona em uma porta UDP, você não pode executar telnet para o endereço IP LOM na porta 623. No entanto, uma solução alternativa é testar se o dispositivo fala IPMI com o utilitário IPMIPING. O IPMIPING envia duas chamadas de obtenção de recursos de autenticação do canal por meio do datagrama de solicitação de obtenção de recursos de autenticação do canal na porta UDP 623 (duas solicitações pois ele usa UDP e as conexões não são garantidas.)

> **Note**: Para um teste mais amplo confirmar se o dispositivo escuta na porta UDP 623, use a verificação NMAP.

Passo 3: Você pode executar o ping do endereço IP do LOM? Caso contrário, execute esse comando como usuário raiz no aplicativo aplicável e verifique se as configurações estão corretas. Por exemplo,

```
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
```

Verificar a conexão

Passo 1: Você pode se conectar usando este comando?

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

Você recebe esta mensagem de erro?

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

> **Note**: Uma conexão para o Endereço IP correto, mas com as credenciais incorretas, falha com o erro anterior imediatamente. Tenta se conectar ao LOM por um tempo limite inválido do endereço IP após cerca de 10 segundos e retorna este erro.

Passo 2: Tente se conectar com este comando:

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

Passo 3: Você recebe este erro?

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

Agora, tente se conectar a este comando (isso especifica o conjunto de cifras a ser usado):

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

Passo 4: Ainda não consegue se conectar? Tente se conectar com este comando:

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

No texto de saída, você visualiza este erro?

```
RAKP 2 HMAC is invalid
```

Passo 5: Altere a senha do administrador com a interface de usuário e tente novamente.

Ainda não consegue se conectar? Tente se conectar com este comando:

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

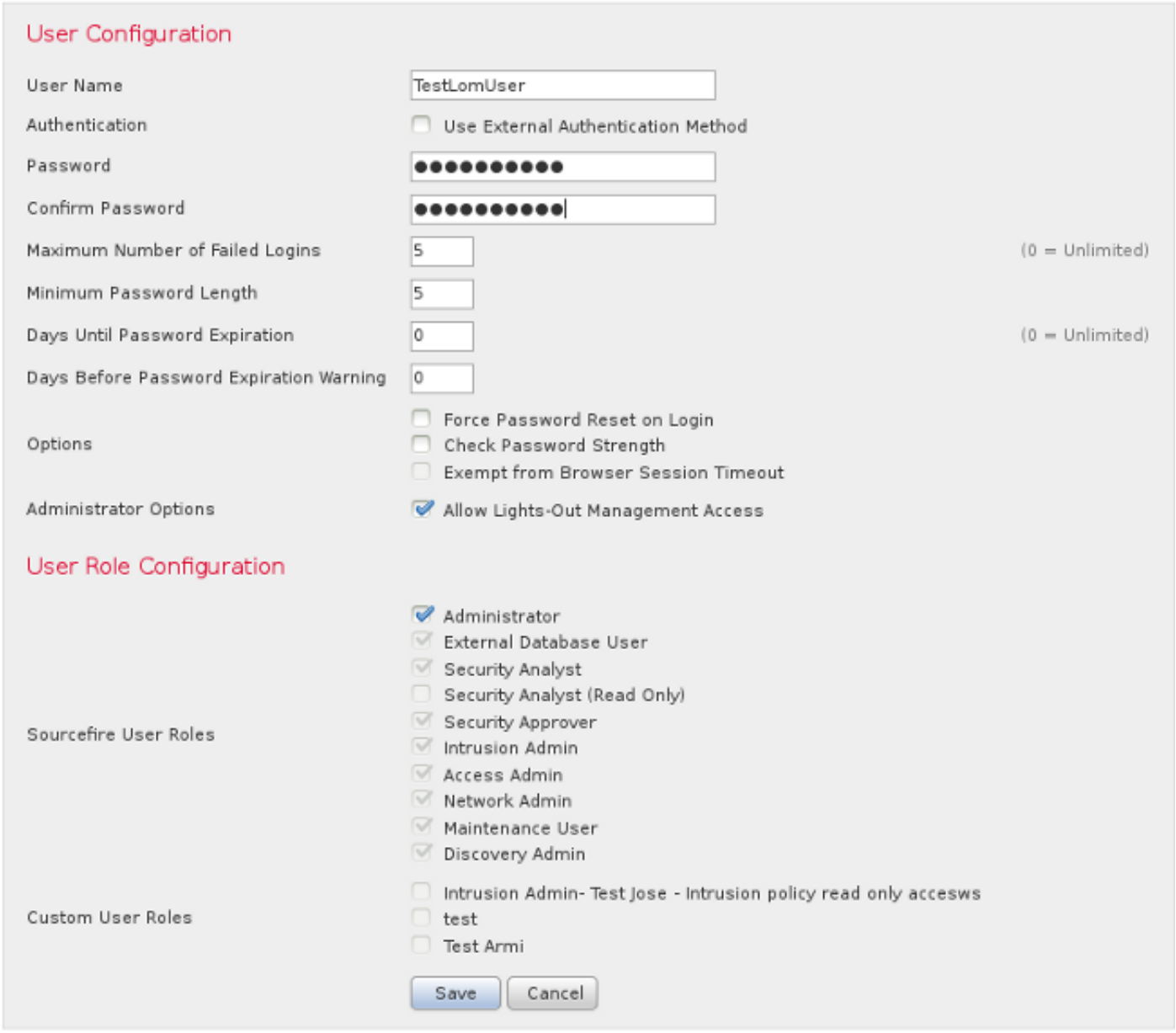
No texto de saída, você visualiza este erro?

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

Passo 6: Escolha User > Local Configuration > User Management (Usuário > Configuração local > Gerenciamento de usuários)

- Criar um novo TestLomUser

- Verifique a **User role configuration (configuração de função de usuário) para Administrator (Administrador)**
- Marque **Allow Lights-out Management Access (Permitir o acesso do Lights-out Management)**



Na CLI do dispositivo aplicável, escale os seus privilégios para raiz e execute esses comandos. Verifique se TestLomUser é o usuário na terceira linha.

```
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
```

Altere o usuário na linha três para admin.

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

Defina um nível de acesso apropriado:

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

Alterar a senha do novo admin user

```
ipmitool user set password 3
```

Verifique se as configurações estão corretas.

```
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
```

Certifique-se de que o SOL esteja ativado para o channel(1) e user(3) corretos.

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

Passo 7: Certifique-se de que o processo IPMI não esteja em estado inválido.

```
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
```

Reinicie o serviço.

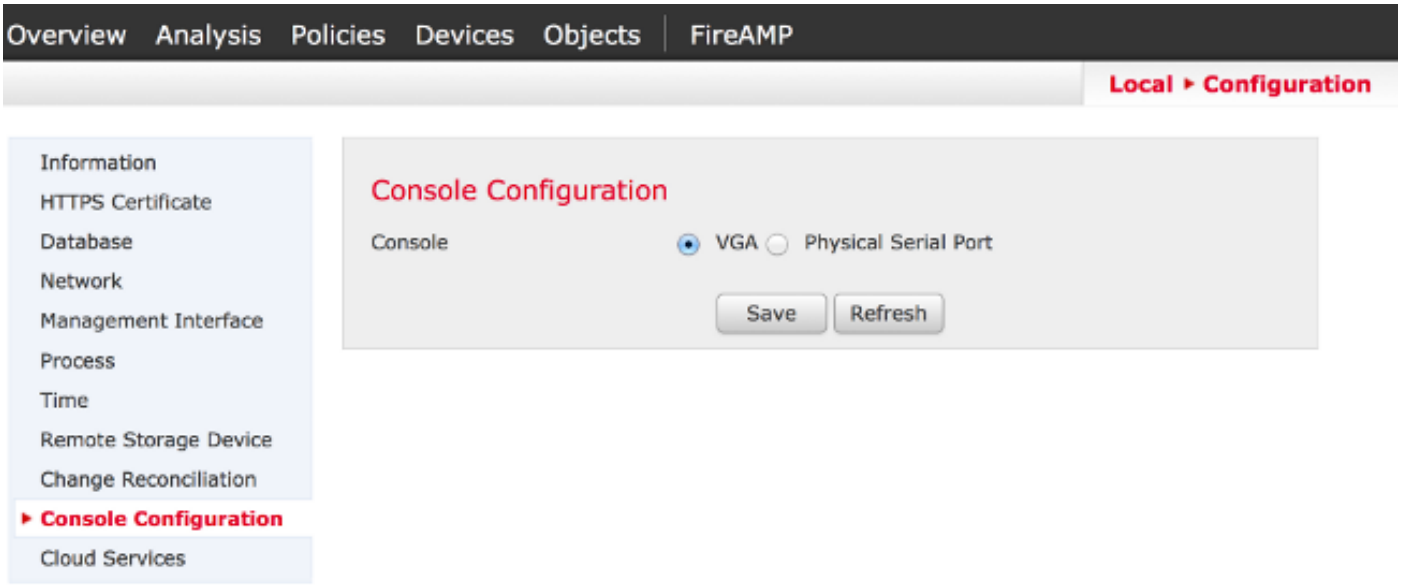
```
pmtool restartbyid sfipmid
```

Confirme se o PID mudou.

```
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
```

Passo 8: Desative o LOM na interface do usuário e, em seguida, reinicie o dispositivo. Na interface do usuário do dispositivo, escolha **Local > Configuration > Console Configuration** (Local > Configuração > Configuração do console). Selecione **VGA** , clique em **Save** (Salvar) e clique em **OK para reinicializar.**



Posteriormente, ative o LOM na interface de usuário e, em seguida, reinicie o dispositivo. Na interface do usuário do dispositivo, escolha **Local > Configuration > Console Configuration** (Local > Configuração > Configuração do console). Escolha **Physical Serial Port (Porta serial física) ou LOM, clique em Save** (Salvar) e em **OK para reinicializar.**

Agora, tente se conectar novamente.

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

Etapa 9: Desligue o dispositivo e conclua um ciclo de energia, isto é, remova fisicamente o cabo de alimentação por um minuto, conecte-o novamente e ligue-o. Depois que o dispositivo for ligado, execute completamente este comando:

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

Etapa 10: Execute este comando com o dispositivo em questão. Especificamente, isso faz uma redefinição forçada de bmc:

```
ipmitool bmc reset cold
```

Etapa 11: Execute este comando em um sistema na mesma rede local que o dispositivo (isto é, não passa por nenhum roteador intermediário):

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

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

Envie ao suporte técnico da Cisco o arquivo /var/tmp/arpcache resultante para determinar se o BMC responde a uma solicitação ARP.

A conexão à Interface LOM é desconectada durante a reinicialização

Quando você reinicializa um FireSIGHT Management Center ou um FirePOWER Appliance, a conexão ao dispositivo pode ser perdida. A saída quando reinicializamos o dispositivo por meio da CLI é mostrada aqui:

```
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
```

A saída realçada **Unmounting fuse control filesystem. Un mostra que a conexão para o dispositivo é interrompida devido ao Spanning Tree Protocol (STP) estar ativado no switch ao qual o sistema FireSIGHT está conectado.** Depois que o dispositivo gerenciado é reinicializado, esse erro é exibido:

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

> **Note**: Antes de poder se conectar a um dispositivo com LOM/SOL, você deve desativar o STP (Spanning Tree Protocol) em qualquer equipamento de switching de terceiros conectado à interface de gerenciamento do dispositivo.

Uma conexão de LOM do sistema FireSIGHT é compartilhado com a porta de gerenciamento. O link para a porta de gerenciamento é removido por um tempo muito breve durante a reinicialização. Como o link está sendo desativado e ativado novamente, isso pode acionar um atraso na porta do switch (normalmente 30 segundos antes de começar a passar o tráfego) devido ao estado da porta de escuta ou de aprendizado causado pelo STP configurado na porta.