Probleemoplossing met Liight-Out Management (LOM) op FireSIGHT Systems

Inhoud

Inleiding

Dit document bevat verschillende symptomen en foutmeldingen die mogelijk verschijnen bij de configuratie van Lights-Out-Management (LOM) en hoe u de problemen stap voor stap kunt oplossen. Met LOM kunt u een out-of-band seriële over-LAN (SOL) beheerverbinding gebruiken voor het extern bewaken of beheren van apparaten zonder te loggen in de webinterface van het apparaat. U kunt beperkte taken uitvoeren, zoals het serienummer van het chassis bekijken of bijvoorbeeld de ventilatiesnelheid en -temperatuur bewaken.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van FireSIGHT System en LOM.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- FireSIGHT Management Center
- FirePOWER 7000 Series applicaties, 8000 Series applicaties
- Software, versie 5.2 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Kan geen verbinding met LOM maken

Mogelijk bent u niet in staat om verbinding te maken met een FireSIGHT Management Center of

FirePOWER-applicatie met LOM. De verbindingsverzoeken kunnen met deze foutmeldingen falen:

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

Info: cannot activate SOL payload with encryption
```

In de volgende paragraaf wordt beschreven hoe u een LOM-configuratie en -verbindingen naar de LOM-interface kunt controleren.

Controleer de configuratie

Stap 1: Controleer en bevestig dat LOM is ingeschakeld en gebruik een ander IP-adres dan de beheerinterface.

Stap 2: Controleer met het netwerkteam dat UDP-poort 623 in twee richtingen is geopend en dat de routes correct zijn geconfigureerd. Aangezien LOM via een UDP-poort werkt, kunt u niet tellen naar het LOM IP-adres in poort 623. Een alternatieve oplossing is echter om te testen of het apparaat IPMI spreekt met het IPMIPING-hulpprogramma. IPMIPING stuurt twee IPMI Get Channel Authentication Capability-oproepen via een Get Channel Authentication Capability-verzoek datagram op UDP-poort 623 (twee verzoeken omdat het UDP gebruikt en de verbindingen niet gegarandeerd zijn).

> **Opmerking:** Gebruik NMAP-scan voor een uitgebreidere test om te bevestigen of het apparaat op UDP-poort 623 luistert.

Stap 3: Kan je het IP-adres van LOM pingelen? Als dit niet het geval is, voert u deze opdracht uit als basisgebruiker op het betreffende apparaat en controleert u of de instellingen correct zijn. Bijvoorbeeld:

```
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
```

Controleer de verbinding

Stap 1: Kun je verbinding maken met deze opdracht?

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

Ontvang je deze foutmelding?

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

> **Opmerking:** Een verbinding met het juiste IP-adres, maar met de verkeerde referenties, mislukt de vorige fout onmiddellijk. Probeert na ongeveer 10 seconden verbinding te maken met LOM op een ongeldig IP-adrestijd en retourneert deze fout.

Stap 2: Probeer met deze opdracht verbinding te maken:

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

Stap 3: Begrijp je deze fout?

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

Probeer nu verbinding te maken met deze opdracht (met de te gebruiken algoritme):

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

Stap 4: Kan je nog steeds geen verbinding maken? Probeer met deze opdracht verbinding te maken:

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

Zie je deze fout in de breedste uitvoer?

```
RAKP 2 HMAC is invalid
```

Stap 5: Wijzig het Admin-wachtwoord via de GUI en probeer het nogmaals.

Kan je nog steeds geen verbinding maken? Probeer met deze opdracht verbinding te maken:

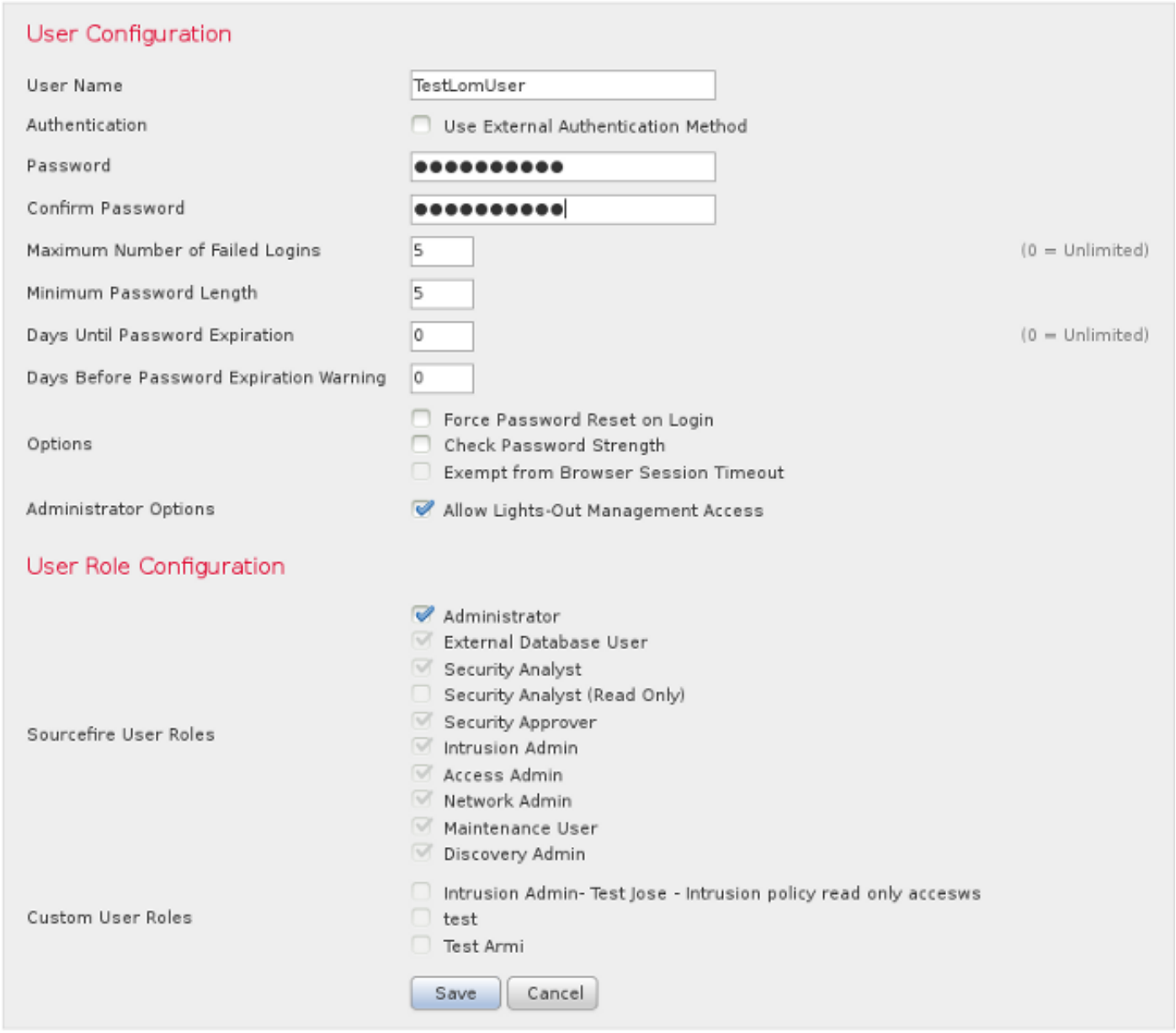
```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

Zie je deze fout in de breedste uitvoer?

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

Stap 6: **Gebruiker** kiezen **> Local Configuration > User Management**

- Een nieuwe TestLinkUser maken
- Controleer de **configuratie** van de **gebruikersrol** aan de **beheerder**
- **Toegang voor** uiteinde-**glasvezelbeheer**



Verhoog uw rechten op de CLI van het toepasbare apparaat om deze opdrachten uit te schakelen en uit te voeren. Controleer dat TestLayerUser de gebruiker op de derde regel is.

```
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
```

Wijzig de gebruiker op regel drie in beheer.

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

Stel een goed toegangsniveau in:

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

Wijzig het wachtwoord van de nieuwe beheerder gebruiker

```
ipmitool user set password 3
```

Controleer of de instellingen correct zijn.

```
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
```

Zorg ervoor dat SOL is ingeschakeld voor het juiste kanaal(1) en de juiste gebruiker(3).

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

Stap 7: Zorg ervoor dat het IPMI-proces niet in een slechte toestand verkeert.

```
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
```

Start de service opnieuw.

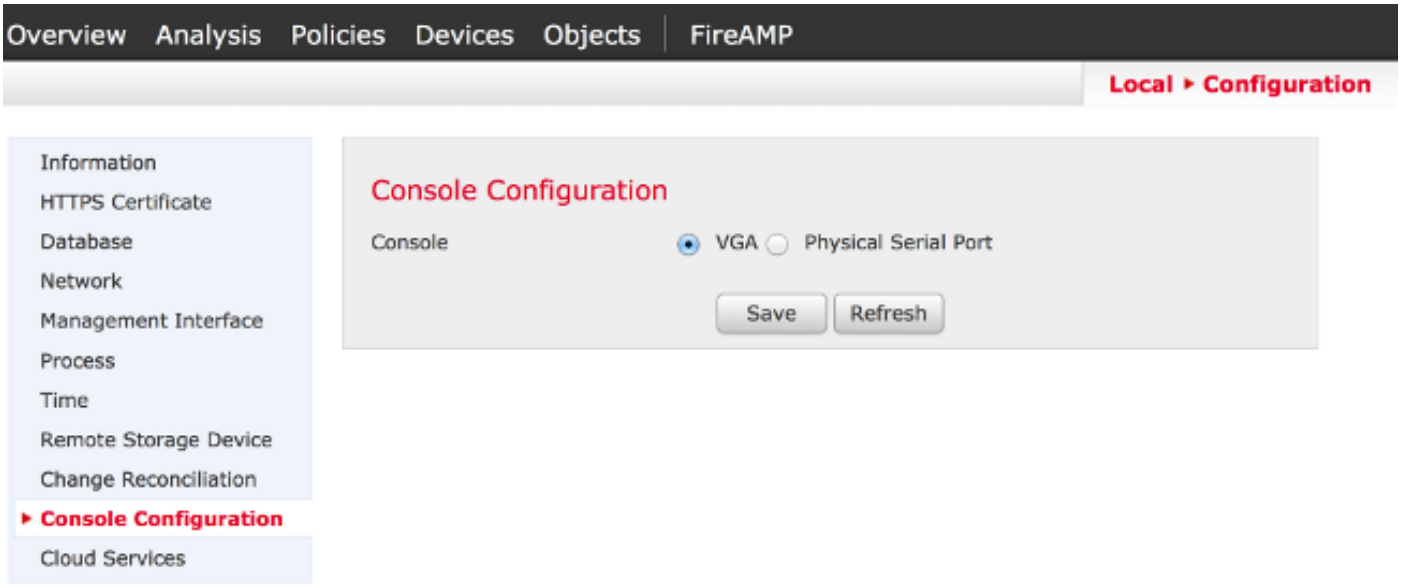
```
pmtool restartbyid sfipmid
```

Bevestig dat de PID is gewijzigd.

```
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
```

Stap 8: Schakel het LOM in de GUI uit en start het apparaat opnieuw. Kies in de GUI van het apparaat **Local > Configuration > Console Configuration**. Selecteer **VGA**, klik op **Opslaan** en klik **op OK** om opnieuw te starten.



Schakel vervolgens de LOM in de GUI in en start het apparaat opnieuw. Kies in de GUI van het apparaat **Local > Configuration > Console Configuration**. Kies **Physical Serial Port** of LOM, klik op **Opslaan** en klik **OK** om te herstarten.

Probeer weer verbinding te maken.

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

Stap 9: Sluit het apparaat af en voltooi een stroomprogramma, d.w.z. verwijder de voedingskabel een minuut, stop het terug en schakel de stroom in. Nadat het apparaat in werking is, voert u deze opdracht volledig uit:

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

Stap 10: Start deze opdracht vanaf het apparaat in kwestie. Dit doet specifiek een koude reset van de bmc:

```
ipmitool bmc reset cold
```

Stap 11: Start deze opdracht van een systeem op hetzelfde lokale netwerk als het apparaat (in dat geval gaat de router niet door):

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

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

Verzend Cisco Technical Support van het resulterende /var/tmp/arpcache-bestand om te bepalen of de BMC op een ARP-verzoek reageert.

Verbinding met LOM-interface wordt verbroken tijdens herstart

Wanneer u een FireSIGHT Management Center of een FirePOWER-applicatie opnieuw start, gaat de verbinding met het apparaat mogelijk verloren. Het resultaat bij het opnieuw opstarten van het apparaat via de CLI wordt hier weergegeven:

```
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
```

De gemarkeerde uitvoer **Bestanden van zekeringsregeling niet monteren. U** toont aan dat de verbinding met het apparaat wordt onderbroken door het feit dat Spanning Tree Protocol (STP) is ingeschakeld op de switch waar FireSIGHT System is aangesloten. Zodra de beheerde apparaten zijn herstart, wordt deze fout weergegeven:

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

> **Opmerking:** Voordat u met LOM/SOL op een apparaat kunt aansluiten, moet u Spanning Tree Protocol (STP) uitschakelen in een externe switching-apparatuur die is aangesloten op de beheerinterface van het apparaat.

Een LOM-verbinding van FireSIGHT System wordt gedeeld met de beheerpoort. De link voor de beheerpoort wordt tijdens de herstart voor een korte tijd verlaagd. Aangezien de link naar beneden gaat en naar boven komt, kan dit een vertraging in de switchpoort veroorzaken (gewoonlijk 30 seconden voordat de verbinding begint door te geven) door de luisterstaat of de lerende switchpoort veroorzaakt door het hebben van STP op de poort.