Fehlerbehebung mit Lights-Out Management (LOM) auf FireSIGHT-Systemen

Inhalt

Einführung

Dieses Dokument enthält verschiedene Symptome und Fehlermeldungen, die angezeigt werden können, wenn Sie Lights-Out-Management (LOM) konfigurieren und eine schrittweise Fehlerbehebung durchführen. LOM ermöglicht die Verwendung einer Out-of-Band-Managementverbindung (Serial over LAN, SOL) zur Remote-Überwachung oder -Verwaltung von Geräten, ohne sich bei der Webschnittstelle der Appliance anzumelden. Sie können begrenzte Aufgaben ausführen, z. B. Anzeigen der Seriennummer des Gehäuses oder Überwachen von Bedingungen wie Lüftergeschwindigkeit und -temperatur.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse des FireSIGHT-Systems und der LOM zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- FireSIGHT Management Center
- Appliances der Serie FirePOWER 7000, Appliances der Serie 8000
- Softwareversion 5.2 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Verbindung mit LOM kann nicht hergestellt werden

Sie können möglicherweise keine Verbindung zu einem FireSIGHT Management Center oder einer FirePOWER-Appliance mit LOM herstellen. Verbindungsanforderungen können mit den folgenden Fehlermeldungen fehlschlagen:

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

Info: cannot activate SOL payload with encryption
```

Im nächsten Abschnitt wird beschrieben, wie Sie eine LOM-Konfiguration und die Verbindungen zur LOM-Schnittstelle überprüfen.

Konfiguration überprüfen

Schritt 1: Überprüfen und bestätigen Sie, dass LOM aktiviert ist, und verwenden Sie eine andere IP-Adresse als die Verwaltungsschnittstelle.

Schritt 2: Überprüfen Sie gemeinsam mit dem Netzwerkteam, ob der UDP-Port 623 bidirektional offen ist und die Routen korrekt konfiguriert sind. Da LOM über einen UDP-Port funktioniert, können Sie über Port 623 keine Telnet-Verbindung zur LOM-IP-Adresse herstellen. Eine Alternative besteht jedoch darin, zu testen, ob das Gerät IPMI mit dem IPMIPING-Dienstprogramm ausgibt. IPMIPING sendet zwei IPMI Get Channel Authentication Capabilities Calls über ein Get Channel Authentication Capabilities Request Datagram auf dem UDP-Port 623 (zwei Anfragen, da dieser UDP verwendet und Verbindungen nicht garantiert sind).

> **Hinweis:** Verwenden Sie für einen ausführlicheren Test zur Überprüfung, ob das Gerät auf dem UDP-Port 623 abhört, die NMAP-Prüfung.

Schritt 3: Können Sie einen Ping an die IP-Adresse von LOM senden? Falls nicht, führen Sie diesen Befehl als root-Benutzer auf der entsprechenden Appliance aus, und überprüfen Sie, ob die Einstellungen korrekt sind. Beispiel:

```
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
```

Überprüfen der Verbindung

Schritt 1: Können Sie mit diesem Befehl eine Verbindung herstellen?

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

Wird diese Fehlermeldung angezeigt?

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

> **Hinweis:** Eine Verbindung mit der richtigen IP-Adresse, jedoch mit den falschen Anmeldeinformationen, schlägt sofort mit dem vorherigen Fehler fehl. Versucht nach etwa 10 Sekunden, eine Verbindung mit dem LOM bei einer ungültigen IP-Adresse herzustellen, und gibt diesen Fehler zurück.

Schritt 2: Versuchen Sie, eine Verbindung mit dem folgenden Befehl herzustellen:

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

Schritt 3: Erhalten Sie diesen Fehler?

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

Versuchen Sie nun, eine Verbindung mit diesem Befehl herzustellen (dieser gibt die zu verwendende Verschlüsselungssuite an):

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

Schritt 4: Kann immer noch keine Verbindung herstellen? Versuchen Sie, eine Verbindung mit dem folgenden Befehl herzustellen:

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

Wird dieser Fehler in der ausführlichen Ausgabe angezeigt?

```
RAKP 2 HMAC is invalid
```

Schritt 5: Ändern Sie das Admin-Kennwort über die GUI, und versuchen Sie es erneut.

Kann immer noch keine Verbindung herstellen? Versuchen Sie, eine Verbindung mit dem folgenden Befehl herzustellen:

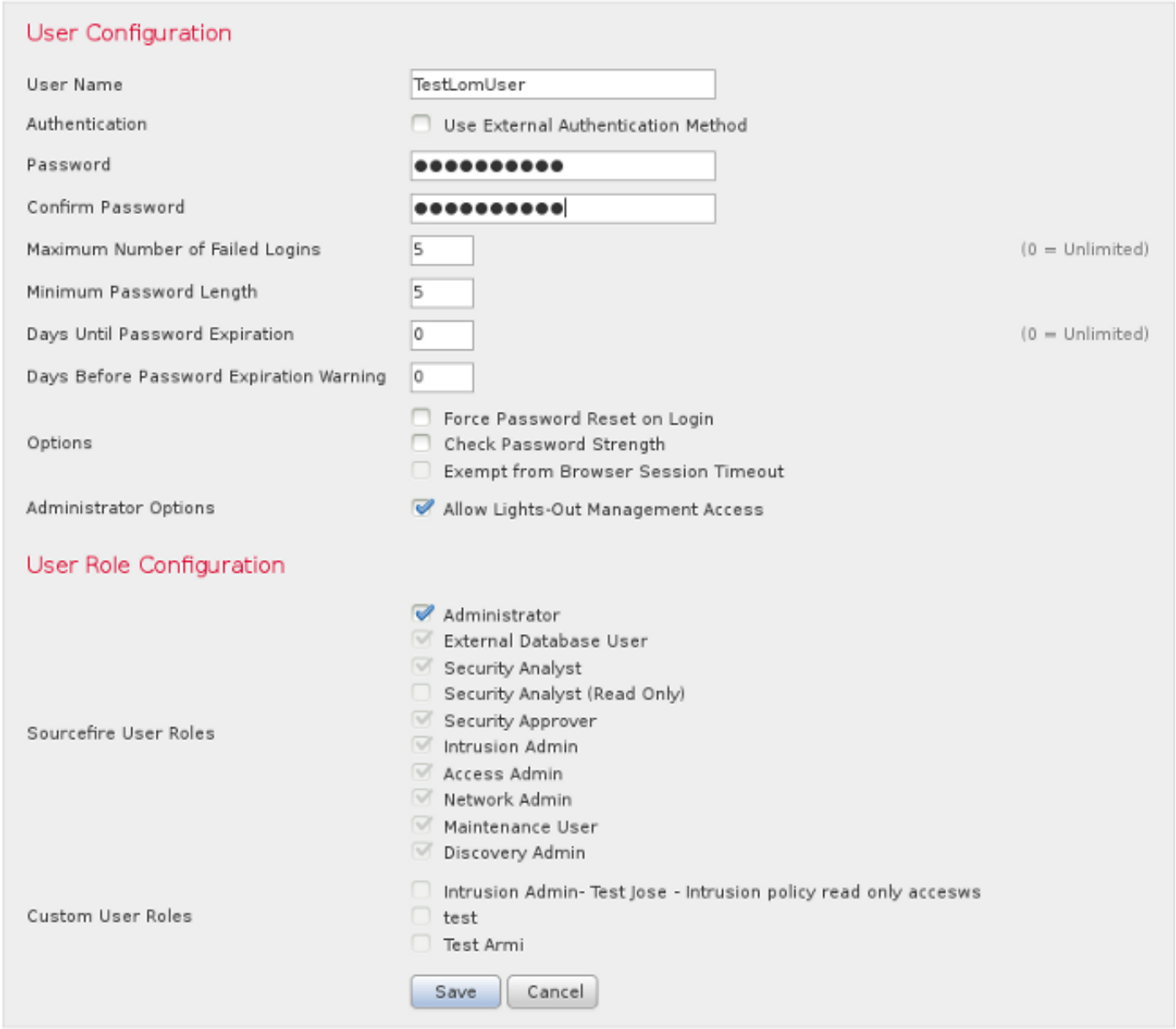
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr

Wird dieser Fehler in der ausführlichen Ausgabe angezeigt?

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

Schritt 6: Wählen Sie **Benutzer > Lokale Konfiguration > Benutzerverwaltung**

- Erstellen eines neuen TestLomUser
- Überprüfen Sie die **Benutzerrollenkonfiguration** auf **Administrator**
- Check **Allow Lights-Out Management Access**



Eskalieren Sie Ihre Berechtigungen auf der CLI der entsprechenden Appliance in root und führen Sie diese Befehle aus. Überprüfen Sie, ob TestLomUser der Benutzer der dritten Zeile ist.

```
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
```

Ändern Sie den Benutzer in Zeile 3 in admin.

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

Legen Sie die entsprechende Zugriffsebene fest:

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

Ändern des Kennworts des neuen Admin-Benutzers

```
ipmitool user set password 3
```

Überprüfen Sie, ob die Einstellungen korrekt sind.

```
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
```

Stellen Sie sicher, dass SOL für den richtigen Kanal(1) und Benutzer(3) aktiviert ist.

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

Schritt 7: Stellen Sie sicher, dass sich der IPMI-Prozess nicht in einem schlechten Zustand befindet.

```
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
```

Starten Sie den Dienst neu.

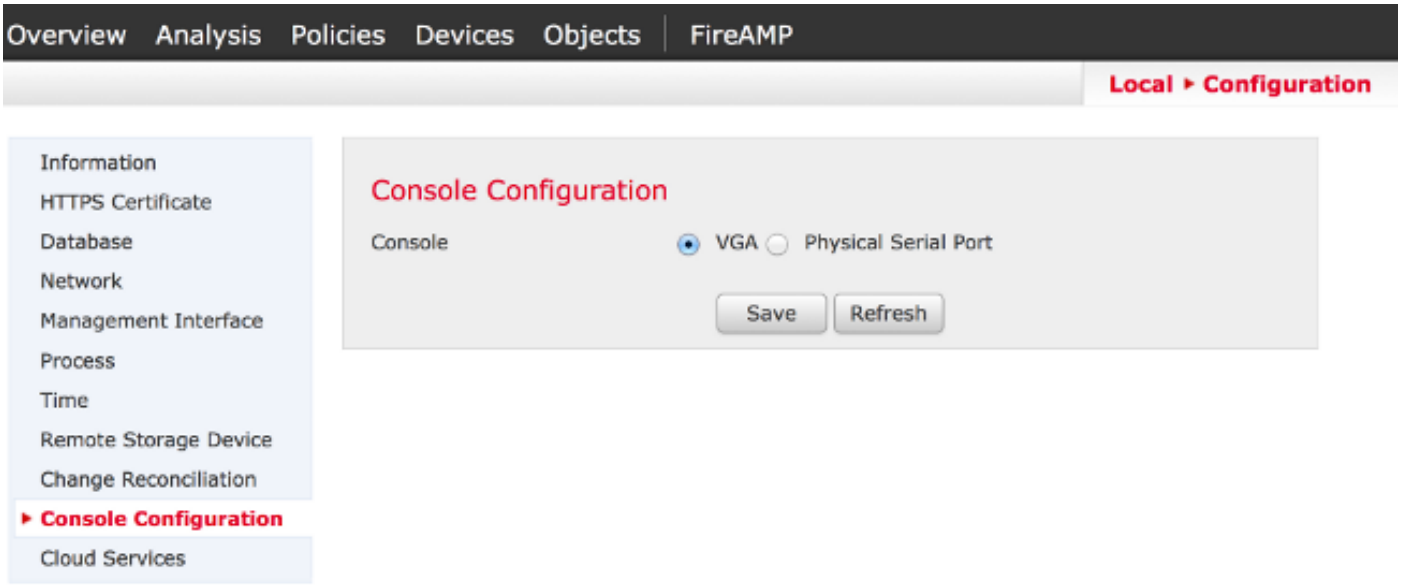
```
pmtool restartbyid sfipmid
```

Bestätigen Sie, dass sich die PID geändert hat.

```
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
```

Schritt 8: Deaktivieren Sie das LOM in der GUI, und starten Sie die Appliance neu. Wählen Sie in der Benutzeroberfläche der Appliance **Lokal > Konfiguration > Konsolenkonfiguration aus**. Wählen Sie **VGA aus**, klicken Sie auf **Speichern**, und klicken Sie auf **OK**, um neu zu starten.



Aktivieren Sie anschließend das LOM in der GUI, und starten Sie die Appliance neu. Wählen Sie in der Benutzeroberfläche der Appliance **Lokal > Konfiguration > Console Configuration aus**. Wählen Sie **Physical Serial Port** oder LOM aus, klicken Sie auf **Save**, und klicken Sie auf **OK**, um neu zu starten.

Versuchen Sie jetzt erneut, eine Verbindung herzustellen.

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

Schritt 9: Fahren Sie das Gerät herunter, und schalten Sie es ein, indem Sie das Netzkabel eine Minute lang entfernen, es wieder anschließen und dann wieder einschalten. Wenn die Einheit vollständig hochgefahren ist, führen Sie folgenden Befehl aus:

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

Schritt 10: Führen Sie diesen Befehl von der betreffenden Appliance aus. Dies bewirkt insbesondere ein Kaltstart des bmc:

```
ipmitool bmc reset cold
```

Schritt 11: Führen Sie diesen Befehl von einem System aus, das sich im selben lokalen Netzwerk wie das Gerät befindet (d. h. kein zwischengeschalteter Router durchläuft):

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

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

Senden Sie die resultierende Datei /var/tmp/arpcache an den technischen Support von Cisco, um festzustellen, ob der BMC auf eine ARP-Anfrage reagiert.

Die Verbindung zur LOM-Schnittstelle wird beim Neustart getrennt.

Beim Neustart eines FireSIGHT Management Center oder einer FirePOWER-Appliance geht die Verbindung zur Appliance möglicherweise verloren. Die Ausgabe beim Neustart der Appliance über die CLI wird hier angezeigt:

```
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
```

Die hervorgehobene Ausgabe **Dateisystem** zum **Entfernen der Sicherung aus der Sicherung. Un** zeigt an, dass die Verbindung zur Appliance unterbrochen wird, weil das Spanning Tree Protocol (STP) auf dem Switch aktiviert wurde, mit dem das FireSIGHT-System verbunden ist. Nach dem Neustart der verwalteten Geräte wird dieser Fehler angezeigt:

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

> **Hinweis:** Bevor Sie eine Verbindung zu einer Appliance mit LOM/SOL herstellen können, müssen Sie das Spanning Tree Protocol (STP) für alle Switching-Geräte von Drittanbietern deaktivieren, die mit der Verwaltungsschnittstelle des Geräts verbunden sind.

Eine LOM-Verbindung des FireSIGHT-Systems wird mit dem Management-Port gemeinsam genutzt. Während des Neustarts wird die Verbindung für den Management-Port für kurze Zeit unterbrochen. Da die Verbindung ausfällt und wieder hochfährt, kann dies eine Verzögerung am Switch-Port (in der Regel 30 Sekunden, bevor der Datenverkehr weitergeleitet wird) aufgrund des Status des Überwachungs- oder Learning-Switch-Ports auslösen, der durch die Konfiguration von STP auf dem Port verursacht wird.