FireSIGHT 시스템의 LOM(Lights-Out Management) 문제 해결

목차

소개

이 문서에서는 LOM(Lights-Out-Management)을 구성할 때 나타날 수 있는 다양한 증상 및 오류 메시지 및 단계별 문제 해결 방법을 제공합니다.LOM을 사용하면 어플라이언스의 웹 인터페이스에 로그인하지 않고도 어플라이언스를 원격으로 모니터링하거나 관리하기 위해 SOL(Out-of-Band Serial over LAN) 관리 연결을 사용할 수 있습니다.섀시 일련 번호를 보거나 팬 속도 및 온도 등의 조건을 모니터링하는 등의 제한된 작업을 수행할 수 있습니다.

사전 요구 사항

요구 사항

FireSIGHT System 및 LOM에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- FireSIGHT Management Center
- FirePOWER 7000 Series 어플라이언스, 8000 Series 어플라이언스
- 소프트웨어 버전 5.2 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

LOM에 연결할 수 없음

LOM이 있는 FireSIGHT Management Center 또는 FirePOWER Appliance에 연결할 수 없습니다.다음 오류 메시지와 함께 연결 요청이 실패할 수 있습니다.

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

Info: cannot activate SOL payload with encryption
```

다음 섹션에서는 LOM 컨피그레이션 및 LOM 인터페이스에 대한 연결을 확인하는 방법에 대해 설명합니다.

구성 확인

1단계:LOM이 활성화되었고 관리 인터페이스와 다른 IP 주소를 사용하는지 확인하고 확인합니다.

2단계:네트워크 팀에 UDP 포트 623이 양방향으로 열려 있고 경로가 올바르게 구성되었는지 확인합니다.LOM은 UDP 포트를 통해 작동하므로 포트 623을 통해 LOM IP 주소에 텔넷할 수 없습니다. 그러나 디바이스에서 IPMIPING 유틸리티로 IPMI를 연결하는지 테스트하는 대체 솔루션이 있습니다.IPMIPING은 UDP 포트 623의 Get Channel Authentication Capabilities 요청 데이터그램을 통해 두 개의 IPMI Get Channel Authentication Capabilities 호출을 전송합니다(UDP를 사용하고 연결을 보장하지 않는 두 개의 요청).

> **참고:**디바이스가 UDP 포트 623에서 수신 대기하는지 확인하기 위한 보다 광범위한 테스트를 보려면 NMAP 스캔을 사용합니다.

3단계:LOM의 IP 주소를 ping할 수 있습니까? 그렇지 않은 경우 이 명령을 해당 어플라이언스에서 루트 사용자로 실행하고 설정이 올바른지 확인합니다.예를 들어

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
```

연결 확인

1단계:이 명령을 사용하여 연결할 수 있습니까?

ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin sdr
이 오류 메시지가 표시됩니까?

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

> **참고:**올바른 IP 주소에 대한 연결이 잘못된 자격 증명으로 인해 즉시 이전 오류로 인해 실패합니다.약 10초 후에 잘못된 IP 주소 시간 초과에서 LOM에 연결을 시도하여 이 오류를 반환합니다.

2단계:다음 명령을 사용하여 연결을 시도합니다.

ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin sdr
3단계:이 오류가 발생했습니까?

```
Info: cannot activate SOL payload with encryption
```
이제 이 명령으로 연결을 시도합니다(사용할 암호 그룹을 지정합니다).

ipmitool -I lanplus -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
4단계:그래도 연결할 수 없습니까?다음 명령을 사용하여 연결을 시도합니다.

ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
자세한 정보 출력에서 이 오류가 표시됩니까?

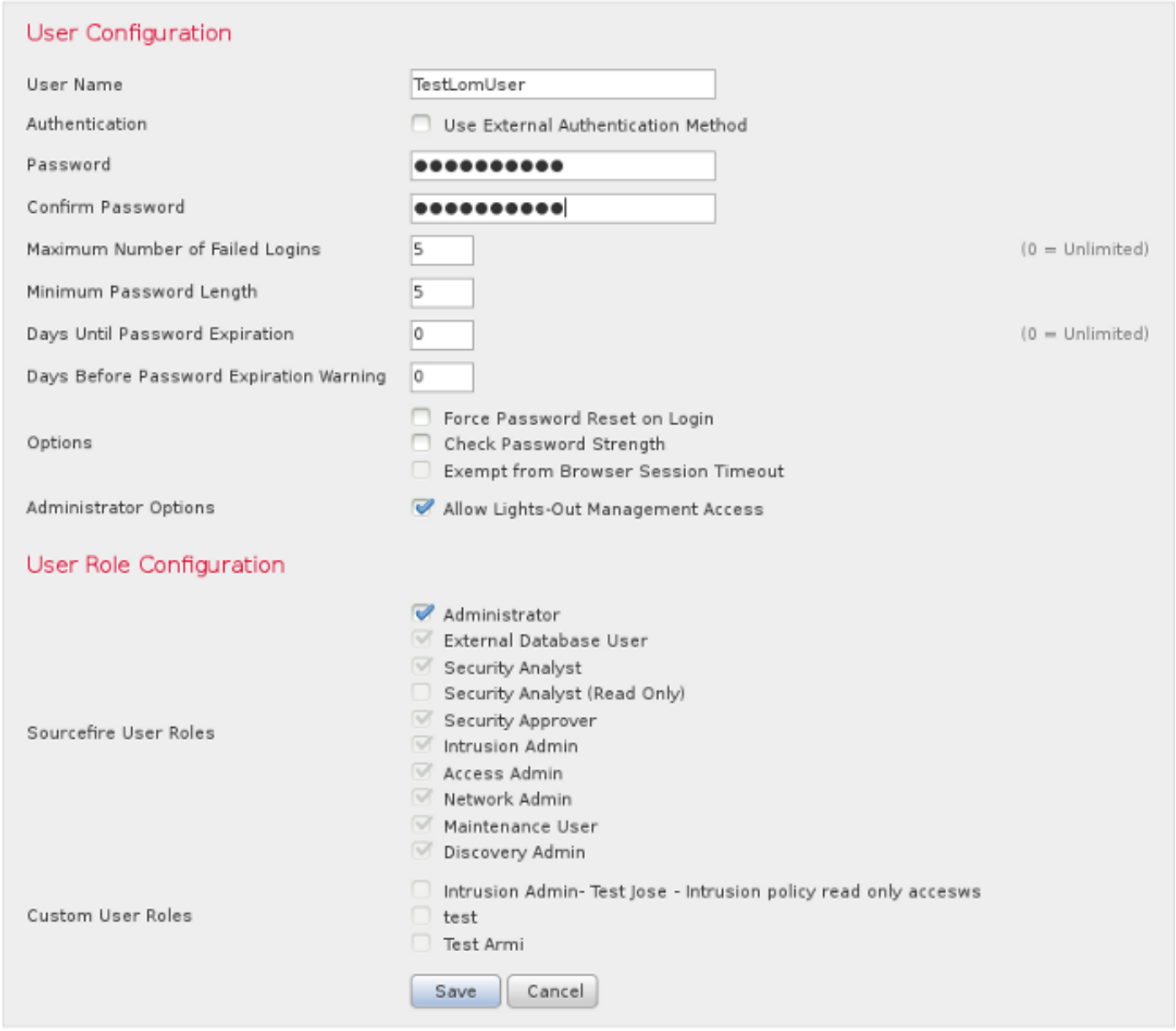
```
RAKP 2 HMAC is invalid
```
5단계:GUI를 통해 관리자 비밀번호를 변경하고 다시 시도하십시오.

그래도 연결할 수 없습니까?다음 명령을 사용하여 연결을 시도합니다.

ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
자세한 정보 출력에서 이 오류가 표시됩니까?

```
RAKP 2 message indicates an error : unauthorized name
```
6단계:User(**사용자) > Local Configuration(로컬 컨피그레이션) > User Management(사용자 관리)를 선택합니다.**

- 새 TestLomUser 만들기
- 관리자에게 **사용자 역할 구성**을 **확인합니다.**
- Allow **Lights-out Management Access(Lights-out 관리 액세스 허용) 확인**



해당 어플라이언스의 CLI에서 권한을 루트로 에스컬레이션하고 다음 명령을 실행합니다. TestLomUser가 세 번째 줄의 사용자인지 확인합니다.

```
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
```

행 3의 사용자를 admin으로 변경합니다.

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

적절한 액세스 레벨을 설정합니다.

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

새 관리자 사용자의 비밀번호 변경

ipmitool user set password 3
설정이 올바른지 확인합니다.

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
```

올바른 채널(1) 및 사용자(3)에 대해 SOL이 활성화되었는지 확인합니다.

ipmitool sol payload enable 1 3
7단계:IPMI 프로세스가 불량 상태가 아닌지 확인합니다.

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
```

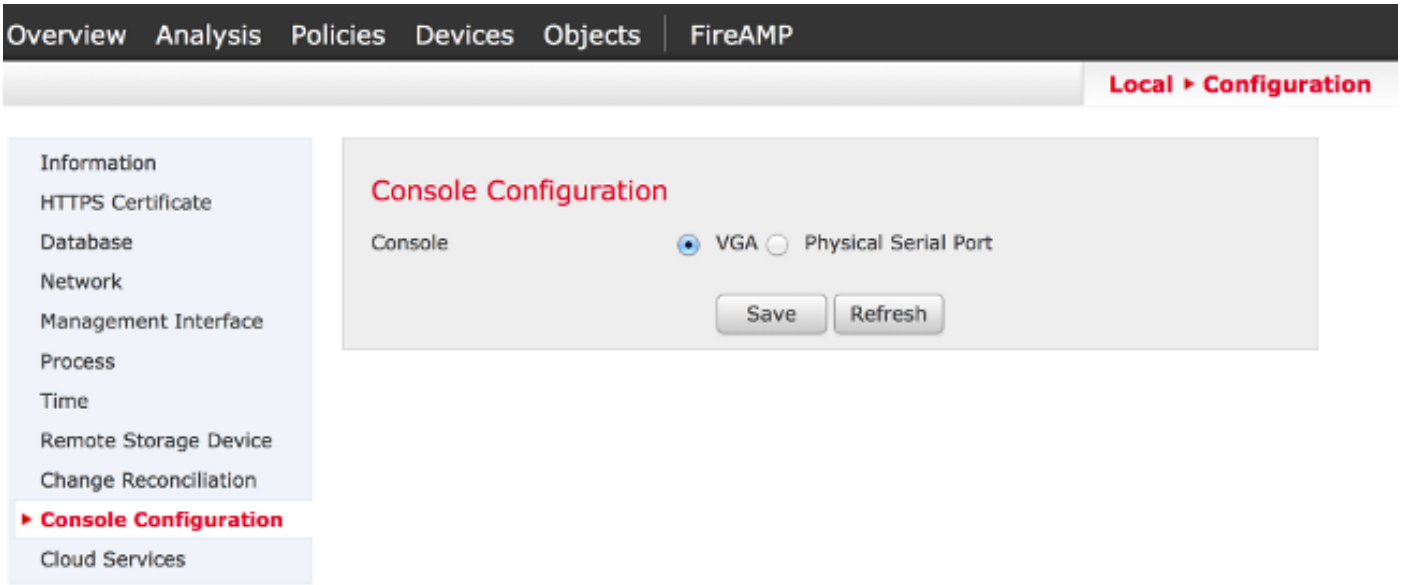
서비스를 다시 시작합니다.

pmtool restartbyid sfipmid
PID가 변경되었는지 확인합니다.

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
```

8단계:GUI에서 LOM을 비활성화한 다음 어플라이언스를 재부팅합니다.어플라이언스의 GUI에서 Local(로컬) > **Configuration(컨피그레이션) > Console Configuration(콘솔 컨피그레이션)을** 선택합니다.재부팅하려면 **VGA**를 선택하고 **Save**(저장)를 클릭한 다음 OK(확인)를 클릭합니다.



그런 다음 GUI에서 LOM을 활성화한 다음 어플라이언스를 재부팅합니다.어플라이언스의 GUI에서

Local(로컬) > **Configuration(컨피그레이션) > Console Configuration(콘솔 컨피그레이션)을 선택합니다**. Physical **Serial Port** 또는 LOM을 선택하고 **Save**를 클릭한 다음 **OK**를 클릭하여 재부팅합니다.

이제 다시 연결해 보십시오.

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

9단계:장치를 종료하고 전원 주기를 완료합니다. 즉, 1분 동안 전원 케이블을 물리적으로 분리한 다음 다시 연결한 다음 전원을 켜십시오. 어플라이언스의 전원이 완전히 켜진 후 다음 명령을 실행합니다.

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

10단계:해당 어플라이언스에서 이 명령을 실행합니다.이는 특히 bmc의 콜드 리셋을 수행합니다.

ipmitool bmc reset cold

11단계:디바이스와 동일한 로컬 네트워크의 시스템에서 이 명령을 실행합니다(즉, 중간 라우터를 통과하지 않음).

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

arp -an > /var/tmp/arpcache

BMC가 ARP 요청에 응답하는지 확인하기 위해 결과/var/tmp/arpcache 파일을 Cisco 기술 지원부에 전송합니다.

다시 부팅하는 동안 LOM 인터페이스에 대한 연결 끊김

FireSIGHT Management Center 또는 FirePOWER Appliance를 재부팅하면 어플라이언스에 대한 연결이 끊어질 수 있습니다.CLI를 통해 어플라이언스를 재부팅할 때의 출력은 다음과 같습니다.

```
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
```

강조 표시된 출력 Unmounting **fuse control filesystem.UN**은 FireSIGHT System이 연결된 스위치에서 STP(Spanning Tree Protocol)가 활성화되어 있어 어플라이언스에 대한 연결이 중단되었음을 표시합니다.관리되는 디바이스가 재부팅되면 다음 오류가 표시됩니다.

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

참고:LOM/SOL을 사용하여 어플라이언스에 연결하려면 먼저 디바이스의 관리 인터페이스에 연결된 타사 스위칭 장비에서 STP(Spanning Tree Protocol)를 비활성화해야 합니다.

FireSIGHT 시스템의 LOM 연결은 관리 포트와 공유됩니다.관리 포트에 대한 링크는 재부팅 중에 매우 짧은 시간 동안 삭제됩니다.링크가 다운되어 다시 작동하기 때문에, 포트에 STP를 구성하여 수신 또는 학습 스위치 포트 상태로 인해 스위치 포트(일반적으로 트래픽 전달을 시작하기 30초 전)의 지연이 발생할 수 있습니다.