Risoluzione dei problemi con Lights-Out Management (LOM) sui sistemi FireSIGHT

Sommario

Introduzione

In questo documento vengono illustrati vari sintomi e messaggi di errore che possono apparire quando si configura Lights-Out-Management (LOM) e viene spiegato come risolverli passo dopo passo. LOM consente di utilizzare una connessione di gestione Serial over LAN (SOL) fuori banda per monitorare o gestire in remoto gli accessori senza accedere all'interfaccia Web dell'accessorio. È possibile eseguire attività limitate, ad esempio visualizzare il numero di serie dello chassis o monitorare condizioni quali la velocità e la temperatura delle ventole.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del sistema FireSIGHT e del LOM.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- Centro di gestione FireSIGHT
- Appliance FirePOWER serie 7000, appliance serie 8000
- Software versione 5.2 o successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Impossibile connettersi a LOM

Potrebbe non essere possibile connettersi a un centro di gestione FireSIGHT o a un'appliance

FirePOWER con LOM. Le richieste di connessione potrebbero non riuscire con questi messaggi di errore:

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

Info: cannot activate SOL payload with encryption
```

La sezione successiva descrive come verificare una configurazione LOM e le connessioni all'interfaccia LOM.

Verifica configurazione

Passaggio 1: Verificare e confermare che LOM sia abilitato e utilizzi un indirizzo IP diverso rispetto all'interfaccia di gestione.

Passaggio 2: Verificare con il team Network che la porta UDP 623 sia aperta bidirezionalmente e che le route siano configurate correttamente. Poiché LOM funziona su una porta UDP, non è possibile connettersi in modalità Telnet all'indirizzo IP LOM sulla porta 623. Tuttavia, una soluzione alternativa consiste nel verificare se il dispositivo parla in modalità IPMI con l'utilità IPPING. IPPING invia due chiamate IPMI Get Channel Authentication Capabilities tramite un datagramma di richiesta Get Channel Authentication Capabilities sulla porta UDP 623 (due richieste poiché utilizza UDP e le connessioni non sono garantite).

> **Nota:** Per un test più approfondito per verificare se il dispositivo è in ascolto sulla porta UDP 623, utilizzare la scansione NMAP.

Passaggio 3: È possibile eseguire il ping dell'indirizzo IP di LOM? In caso contrario, eseguire questo comando come utente root sull'accessorio e verificare che le impostazioni siano corrette. Ad esempio,

```
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
```

Verifica connessione

Passaggio 1: È possibile connettersi utilizzando questo comando?

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

Viene visualizzato questo messaggio di errore?

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

> **Nota:** Una connessione all'indirizzo IP corretto, ma con credenziali errate, non riesce con l'errore precedente immediatamente. Tenta di connettersi a LOM a un indirizzo IP non valido dopo circa 10 secondi e restituisce questo errore.

Passaggio 2: Provare a connettersi con questo comando:

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

Passaggio 3: Ricevi questo errore?

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

Provare a connettersi con questo comando (che specifica la suite di cifratura da utilizzare):

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

Passaggio 4: Ancora impossibile connettersi? Provare a connettersi con questo comando:

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

Nell'output dettagliato viene visualizzato questo errore?

```
RAKP 2 HMAC is invalid
```

Passaggio 5: Modificare la password dell'amministratore tramite la GUI e riprovare.

Ancora impossibile connettersi? Provare a connettersi con questo comando:

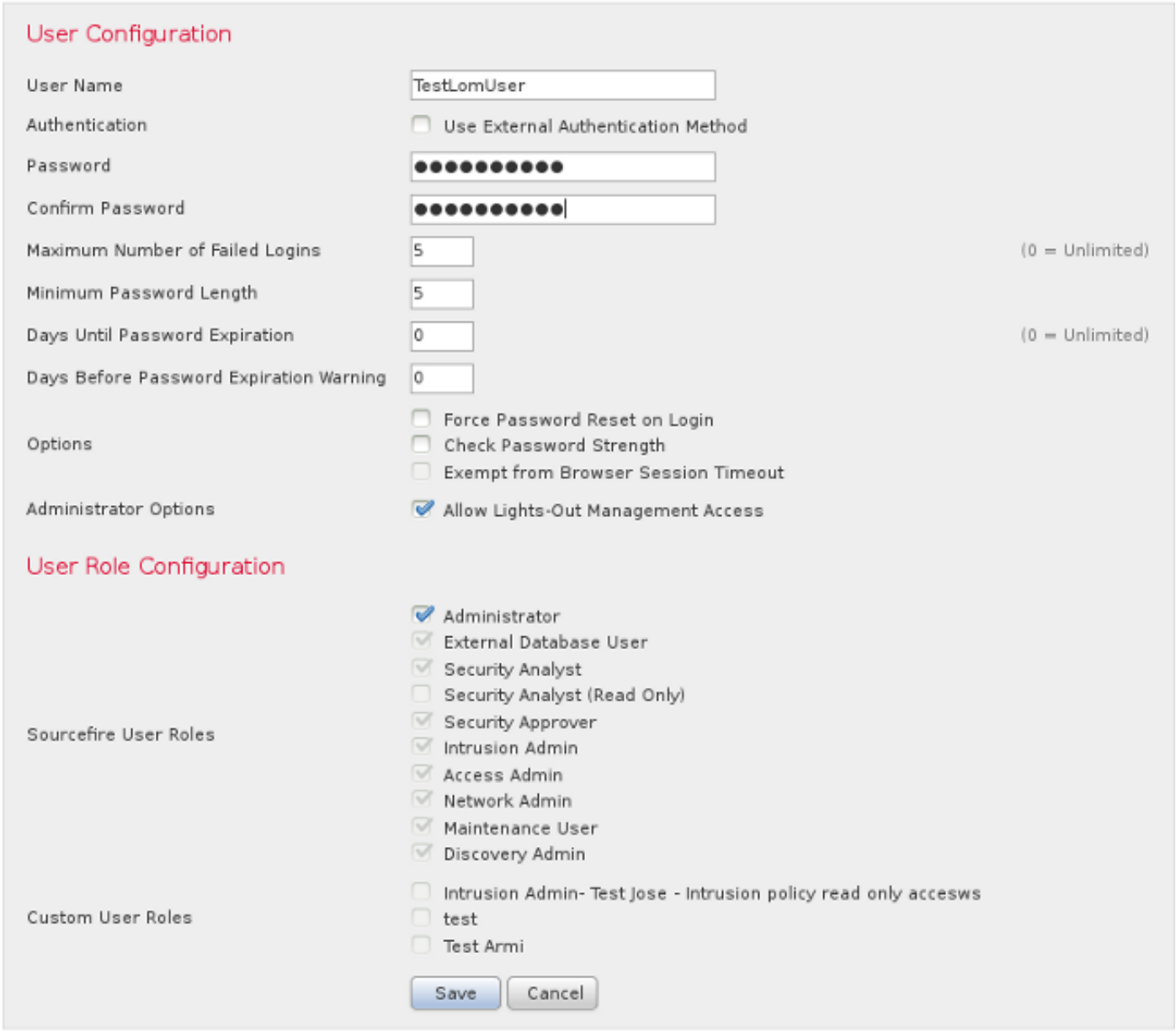
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr

Nell'output dettagliato viene visualizzato questo errore?

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

Passaggio 6: Scegliere **Utente > Configurazione locale > Gestione utente**

- Crea un nuovo TestLomUser
- Controllare la **configurazione** del **ruolo utente** in **Amministratore**
- Selezionare **Consenti accesso gestione non presidiato**



Dalla CLI dell'accessorio applicabile, assegnare i privilegi al root ed eseguire questi comandi. Verificare che TestLomUser sia l'utente della terza riga.

```
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
```

Cambiare l'utente alla riga 3 in admin.

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

Impostare un livello di accesso appropriato:

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

Cambiare la password del nuovo utente admin

```
ipmitool user set password 3
```

Verificare che le impostazioni siano corrette.

```
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
```

Verificare che SOL sia abilitato per il canale(1) e l'utente(3) corretti.

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

Passaggio 7: Verificare che lo stato del processo IPMI non sia danneggiato.

```
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
```

Riavviare il servizio.

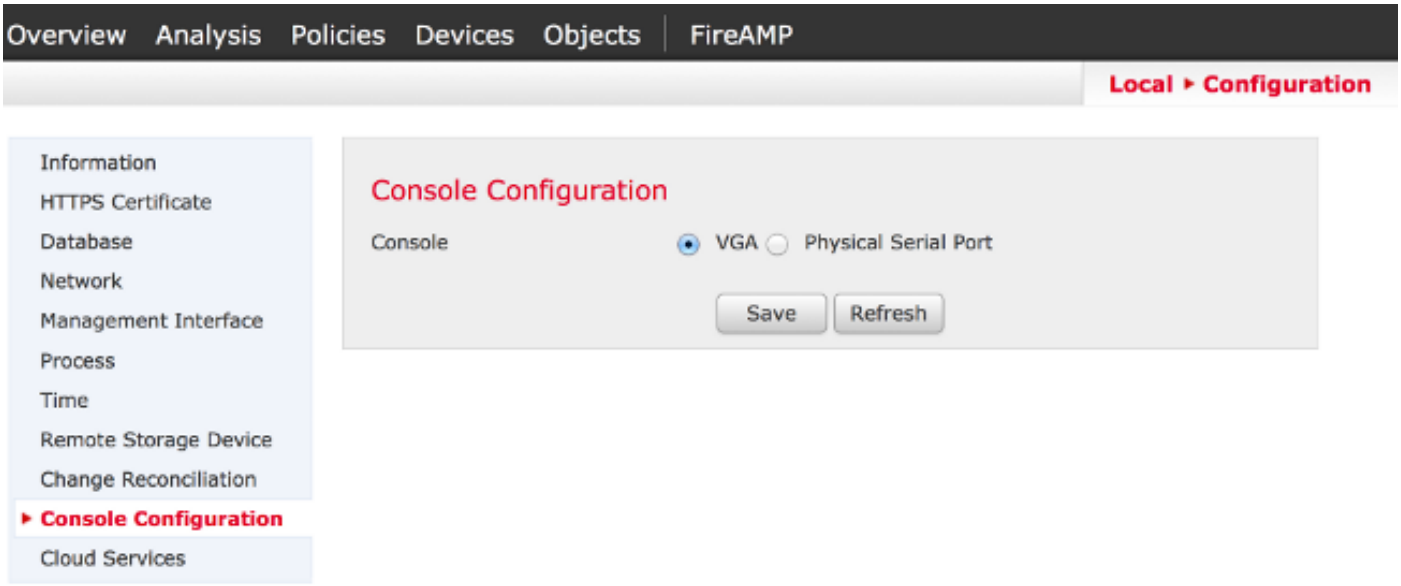
```
pmtool restartbyid sfipmid
```

Confermare che il PID è stato modificato.

```
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
```

Passaggio 8: Disabilitare il LOM nella GUI, quindi riavviare l'accessorio. Nell'interfaccia utente dell'accessorio, scegliere **Locale > Configurazione > Configurazione console**. Selezionare **VGA**, fare clic su **Salva**, quindi su **OK** per riavviare il sistema.



In seguito, attivare il LOM nella GUI, quindi riavviare l'accessorio. Nella GUI dell'accessorio, scegliere **Locale > Configurazione > Configurazione console**. Scegliere **Porta seriale fisica** o LOM, fare clic su **Salva**, quindi su **OK** per riavviare.

Riprovare a connettersi.

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

Passaggio 9: Spegnere il dispositivo e completare un ciclo di alimentazione, ovvero rimuovere fisicamente il cavo di alimentazione per un minuto, ricollegarlo e accenderlo. Dopo l'accensione dell'accessorio eseguire questo comando:

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

Passaggio 10: Eseguire questo comando dall'accessorio in questione. In particolare, viene eseguito un reset a freddo del bmc:

```
ipmitool bmc reset cold
```

Passaggio 11: Eseguire questo comando da un sistema nella stessa rete locale del dispositivo (ossia, non passa attraverso alcun router intermedio):

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

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

Inviare al supporto tecnico Cisco il file /var/tmp/arpcache risultante per determinare se il BMC risponde a una richiesta ARP.

La connessione all'interfaccia LOM viene interrotta durante il riavvio

Quando si riavvia un centro di gestione FireSIGHT o un accessorio FirePOWER, la connessione all'accessorio potrebbe essere interrotta. Di seguito è riportato l'output del riavvio dell'accessorio dalla 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
```

L'output evidenziato **Smontaggio del file system di controllo del fusibile. Un** indica che la connessione all'accessorio è interrotta perché è stato abilitato il protocollo Spanning Tree Protocol (STP) sullo switch a cui è collegato il sistema FireSIGHT. Una volta riavviati i dispositivi gestiti, viene visualizzato questo errore:

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

> **Nota:** Prima di collegarsi a un accessorio con LOM/SOL, è necessario disattivare il protocollo Spanning Tree Protocol (STP) su qualsiasi dispositivo di commutazione di terze parti collegato all'interfaccia di gestione del dispositivo.

Una connessione LOM di FireSIGHT System viene condivisa con la porta di gestione. Il collegamento della porta di gestione viene interrotto per un breve periodo durante il riavvio. Poiché il collegamento si interrompe e torna attivo, la porta dello switch potrebbe subire un ritardo (generalmente 30 secondi prima che inizi a passare il traffico) dovuto allo stato della porta dello switch in ascolto o in apprendimento causato dalla configurazione di STP sulla porta.