

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Incapable de se connecter à LOM](#)

[Vérifiez la configuration](#)

[Vérifiez la connexion](#)

[La connexion à l'interface LOM est déconnectée pendant la réinitialisation](#)

Introduction

La Lumière--Gestion (LOM) te permet pour utiliser une interface série hors bande au-dessus de Gestion du RÉSEAU LOCAL (solénoïde) que la connexion à distance surveillent ou gèrent des appliances sans se connecter dans l'interface web de l'appliance. Vous pouvez effectuer des tâches limitées, telles que visualiser le numéro de série de châssis ou surveiller des conditions tels que la vitesse des ventilateurs et la température. Ce document fournit les divers symptômes et messages d'erreur qui peuvent apparaître quand vous configurez LOM, et comment les dépanner pas à pas.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur le système de FireSIGHT et la Lumière--Gestion (LOM).

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Centre de Gestion de FireSIGHT
- Appliances de gamme 7000 de puissance de feu, appliances de gamme 8000.
- Version de logiciel 5.2 ou plus tard

Remarque: Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Incapable de se connecter à LOM

Vous pouvez ne pouvoir pas se connecter à une appliance de centre ou de puissance de feu de Gestion de FireSIGHT utilisant la Gestion d'extinction des feux (LOM). Les demandes de connexion peuvent échouer avec les messages d'erreur suivants :

```
Error: Unable to establish IPMI v2 / RMCP+ session ErrorInfo: cannot activate SOL payload with encryption
```

La section suivante décrit comment vérifier une configuration et des connexions LOM l'interface LOM.

Vérifiez la configuration

Étape 1 : Vérifiez et confirmez que LOM est activé, et utilisez une adresse IP différente que l'interface de gestion.

Étape 2 : Vérifiez avec l'équipe de réseau que le port UDP 623 est ouvert bidirectionnel, et que les artères sont configurées correctement. Telnet à l'adresse IP LOM au-dessus du port 623.

Étape 3 : Pouvez-vous cingler l'adresse IP de LOM ? Sinon, exécutez la commande suivante comme utilisateur de base sur l'appliance applicable, et vérifiez les configurations sont corrects. Exemple :

```
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
Gratuitous ARP Intrvl : 0.0 secondsDefault 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
```

Vérifiez la connexion

Étape 1 : Pouvez-vous se connecter utilisant la commande suivante ?

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

Recevez-vous ce message d'erreur ?

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

Remarque: Se connecter à l'adresse IP correcte mais la fourniture des qualifications fausses échoue avec l'erreur ci-dessus immédiatement. Essayer à connecter à LOM à une adresse IP incorrecte chronomètre après environ 10 secondes et renvoie cette erreur.

Étape 2 : Essayez de se connecter utilisant la commande suivante :

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

Étape 3 : Obtenez-vous cette erreur ?

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

Maintenant essayez à connecter utilisant la commande suivante (ceci spécifiera la suite de chiffrement pour utiliser) :

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

Étape 4 : Ne peut pas encore se connecter ? Essayez de se connecter utilisant la commande suivante :

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

Dans la sortie bavarde voyez-vous l'erreur suivante ?

```
RAKP 2 HMAC is invalid
```

Étape 5 : Changez le mot de passe administrateur par l'intermédiaire du GUI, et de l'essai de nouveau.

Ne peut pas encore se connecter ? Essayez de se connecter utilisant la commande suivante :

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

Dans la sortie bavarde voyez-vous l'erreur suivante ?

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

Étape 6 : Naviguez vers **l'utilisateur > la configuration locale > la gestion des utilisateurs**

- Créez un nouveau `TestLomUser`
- Vérifiez le rôle de l'utilisateur de configuration à l'administrateur
- Le contrôle permet la Gestion Access d'extinction des feux

User Configuration

User Name:

Authentication: Use External Authentication Method

Password:

Confirm Password:

Maximum Number of Failed Logins: (0 = Unlimited)

Minimum Password Length:

Days Until Password Expiration: (0 = Unlimited)

Days Before Password Expiration Warning:

Options: Force Password Reset on Login
 Check Password Strength
 Exempt from Browser Session Timeout

Administrator Options: Allow Lights-Out Management Access

User Role Configuration

Sourcefire User Roles: Administrator
 External Database User
 Security Analyst
 Security Analyst (Read Only)
 Security Approver
 Intrusion Admin
 Access Admin
 Network Admin
 Maintenance User
 Discovery Admin

Custom User Roles: Intrusion Admin- Test Jose - Intrusion policy read only accesws
 test
 Test Armi

Sur le CLI de l'appliance applicable, faites suivre vos privilèges de s'enraciner, et d'exécuter les commandes suivantes. Vérifiez que `TestLomUser` est l'utilisateur sur la troisième ligne.

```
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
```

Changez l'utilisateur sur la ligne trois à l'admin.

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

Placez un niveau d'accès approprié :

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

Changez le mot de passe du nouvel utilisateur d'admin

```
ipmitool user set password 3
```

Vérifiez que les configurations sont correctes.

```
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
```

Assurez-vous que le solénoïde est activé pour le channel(1) et l'user(3) corrects.

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

[Étape 7](#) : Assurons-nous que le processus IPMI n'est pas dans un mauvais état.

```
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
```

Redémarrez le service.

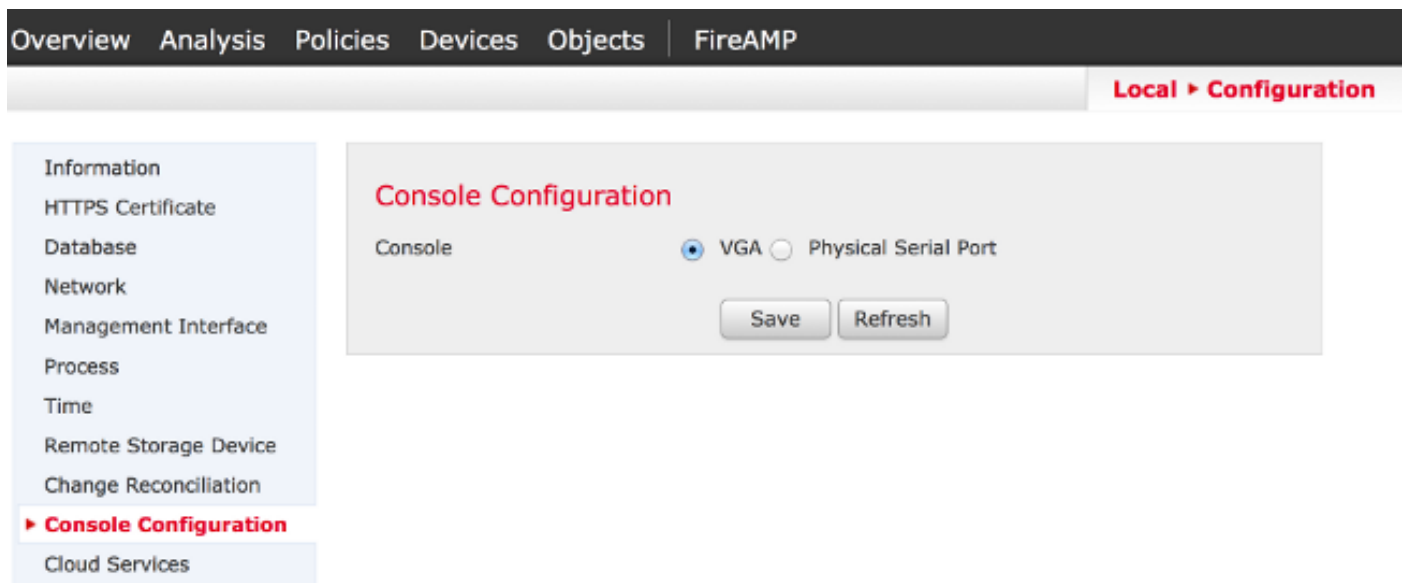
```
pmtool restartbyid sfipmid
```

Confirmez que le PID a changé.

```
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
```

[Étape 8](#) : Désactivez le LOM dans le GUI, puis redémarrez l'appliance. Dans le GUI des appareils naviguez vers **des gens du pays > la configuration > la configuration de console**. Alors sélectionnez le **VGA**, cliquez sur la **sauvegarde** et cliquez sur OK pour redémarrer maintenant.



Après, activez le LOM dans le GUI, puis redémarrez l'appliance. Dans le GUI des appareils naviguez vers **des gens du pays > la configuration > la configuration de console**. Alors sélectionnez le **port série physique** ou le LOM, cliquez sur la **sauvegarde** et cliquez sur OK pour redémarrer maintenant.

Maintenant, essayez à connecter de nouveau.

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

[Étape 9](#) : Arrêtez le périphérique et terminez-vous un arrêt et redémarrage, c.-à-d., enlèvent physiquement le câble d'alimentation pour 1 minute, le branchent de retour et le mettent sous tension alors. Après l'appliance actionne exécutent entièrement la commande suivante :

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

Étape 10 : Exécutez la commande suivante de l'appliance en question. Ceci fera spécifiquement une remise à froid du bmc :

```
ipmitool bmc reset cold
```

Étape 11 : Exécutez la commande suivante d'un système sur le même réseau local que le périphérique (c.-à-d., ne traversant pas tout routeur intermédiaire) :

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin power status arp -an > /var/tmp/arpcache
```

Envoyez à support technique de Cisco le fichier en résultant de /var/tmp/arpcache pour déterminer si le BMC répond à une demande d'ARP.

La connexion à l'interface LOM est déconnectée pendant la réinitialisation

Quand vous redémarrez un centre de Gestion de FireSIGHT ou une appliance de puissance de feu, la connexion à l'appliance peut être perdue. La sortie quand la réinitialisation de l'appliance par l'intermédiaire de la ligne de commande est ci-dessous :

```
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 unnecessary...[-10G[ OK ]..
Turning off swapfile /Volume/.swaptwo
[-10G[ OK ] other currently mounted file systems...
Unmounting fuse control filesystem.Un
```

Le système de fichiers mis en valeur de contrôle de fusible d'Unmounting de sortie. L'ONU prouve que la connexion à l'appliance est due interrompu au Protocole Spanning Tree (STP) étant activé sur le commutateur à où le FireSIGHT Systeme est connecté. Une fois que les réinitialisations de périphériques gérés, l'erreur suivante est affichées :

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

Remarque: Avant que vous puissiez se connecter à une appliance utilisant LOM/SOL, vous devez désactiver le Protocole Spanning Tree (STP) relatif à n'importe quel tiers matériel de commutation connecté à l'interface de gestion du périphérique.

Une connexion LOM de système de FireSIGHT est partagée avec le port de gestion. Le lien pour le port de gestion chute pendant un temps très bref pendant la réinitialisation. Puisque le lien va vers le bas et se réactive, ceci pourrait déclencher un retard dans le port de commutateur (typiquement 30 secondes avant qu'il commence passer le trafic) dû à l'état de écoute ou apprenant de port de commutateur provoqué en ayant STP configuré sur le port.