Dépannage des problèmes de gestion à distance (Lights-Out Management ou LOM) sur les systèmes FireSIGHT

Contenu

Introduction

Ce document présente divers symptômes et messages d'erreur pouvant apparaître lorsque vous configurez la gestion en service réduit (Lights-Out-Management ou LOM), et la façon de résoudre chacun d'eux étape par étape. LOM vous permet d'utiliser une connexion de gestion de série sur réseau LAN (SOL) hors bande pour surveiller ou gérer à distance des appareils sans vous connecter à leur interface Web. Vous pouvez effectuer des tâches limitées, par exemple afficher le numéro de série du châssis ou surveiller certaines conditions comme la vitesse du ventilateur et la température.

Conditions préalables

Conditions requises

Cisco recommande de connaître le système FireSIGHT et LOM.

Components Used

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

- Centre de gestion FireSIGHT
- Appareils de la série 7000 et série 8000 FirePOWER
- Version de logiciel 5.0 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Impossible de se connecter à LOM

Vous pourriez ne pas être en mesure de vous connecter à un centre de gestion FireSIGHT ou à un appareil FirePOWER avec LOM. Les demandes de connexion peuvent échouer et afficher ses messages d'erreur :

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

Info: cannot activate SOL payload with encryption
```

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

Vérifier la configuration

Étape 1 : Vérifiez et confirmez que LOM est activée et utilise une adresse IP différente de l'interface de gestion.

Étape 2 : Vérifiez avec l'équipe de réseau que le port UDP 623 est ouvert de manière bidirectionnelle et que les routages sont configurés correctement. Puisque LOM fonctionne sur un port UDP, vous ne pouvez pas établir de connexion Telnet avec l'adresse IP LOM sur le port 623. Cependant, une autre solution consiste à tester si le périphérique parle IPMI avec l'utilitaire IPMIPING. IPMIPING envoie deux appels IPMI pour obtenir les capacités d'authentification du canal par l'intermédiaire d'un datagramme de demande d'obtention des capacités d'authentification du canal sur le port UDP 623 (deux demandes, car elle utilise UDP et que les connexions ne sont pas garanties.)

> **Note**: Pour un test plus complet pour confirmer si l'appareil écoute le port UDP 623, utilisez un balayage NMAP.

Étape 3 : Pouvez-vous envoyer un message Ping à l'adresse IP de LOM? Si ce n'est pas le cas, exécutez cette commande en tant qu'utilisateur racine sur l'appliance applicable et vérifiez que les paramètres 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
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
```

Vérifier la connexion

Étape 1 : Pouvez-vous vous connecter en utilisant cette commande?

```
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
```

> **Note**: Une connexion à la bonne adresse IP avec les mauvaises informations d'authentification échoue accompagnée aussitôt du message d'erreur précédent. Les tentatives de connexions à LOM avec une adresse IP non valide expirent après environ 10 secondes et renvoient cette erreur.

Étape 2 : Essayez de vous connecter avec cette commande :

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

Étape 3 : Obtenez-vous cette erreur?

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

Essayez maintenant de vous connecter à cette commande (qui spécifie la suite de chiffrement à utiliser) :

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

Étape 4 : Toujours impossible de vous connecter? Essayez de vous connecter avec cette commande :

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

Dans la sortie en clair, voyez-vous cette erreur?

```
RAKP 2 HMAC is invalid
```

Étape 5 : Modifiez le mot de passe Admin à l'aide de l'interface graphique utilisateur (GUI), puis réessayez.

Toujours impossible de vous connecter? Essayez de vous connecter avec cette commande :

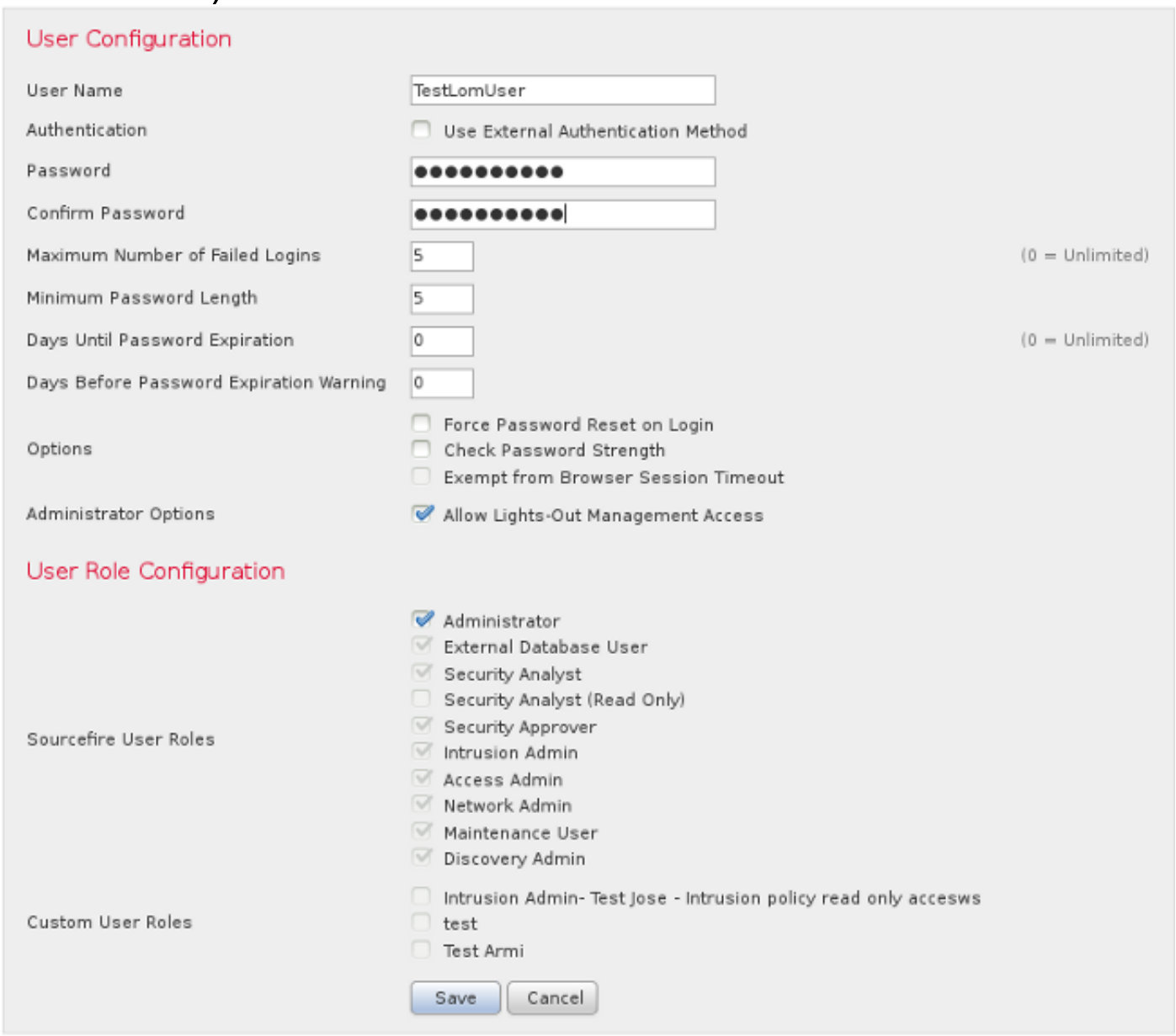
```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

Dans la sortie en clair, voyez-vous cette erreur?

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

Étape 6 : Choisissez User > Local Configuration > User Management (utilisateur > configuration locale > gestion de l'utilisateur)

- Créez un nouveau TestLomUser
- Vérifiez que **User role configuration (configuration du rôle d'utilisateur) est à Administrator (administrateur)**
- Cochez la case **Allow Lights-out Management Access (autoriser l'accès à la gestion en service réduit)**



Sur la CLI de l'appareil applicable, faites monter vos privilèges à la racine et exécutez ces commandes. 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
```

Modifiez l'utilisateur sur la troisième ligne pour admin.

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

Définissez 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 admin

```
ipmitool user set password 3
```

Vérifiez que les paramètres sont corrects.

```
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 SOL est activé pour le canal(1) et l'utilisateur(3) appropriés.

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

Étape 7 : Assurez-vous que le processus IPMI n'est pas en 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.

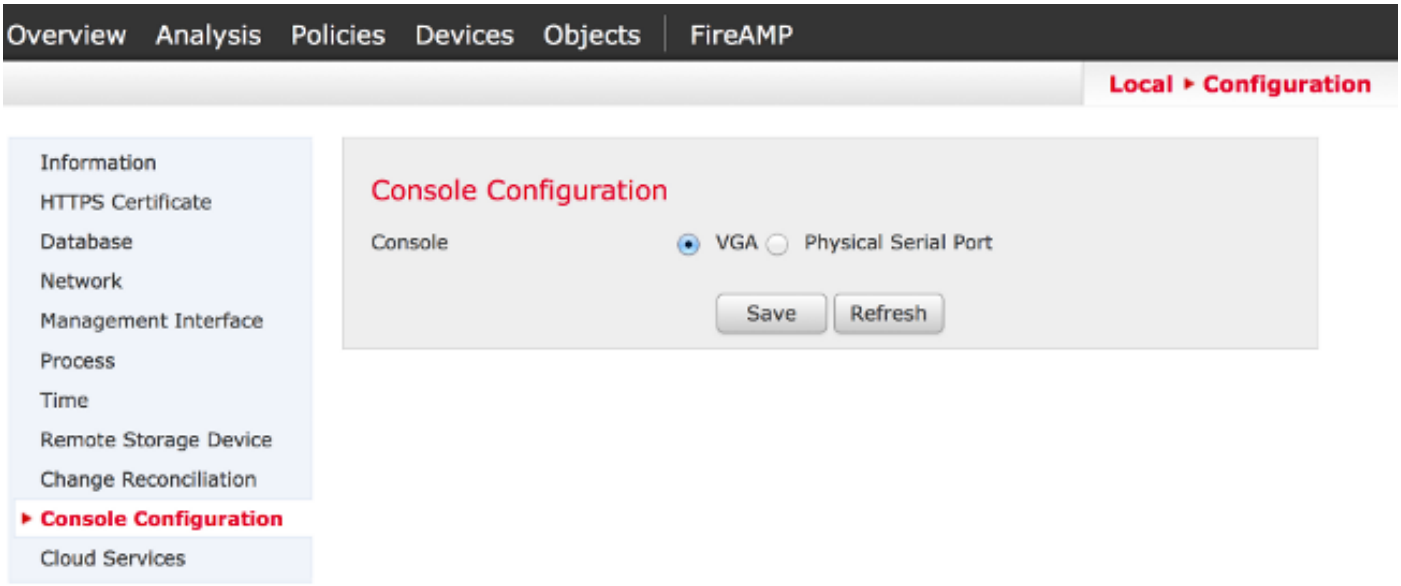
```
pmtool restartbyid sfipmid
```

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 LOM dans l'interface graphique utilisateur (GUI), puis redémarrez l'appareil. Dans l'interface graphique utilisateur (GUI) de l'appareil, choisissez **Local > Configuration > Console Configuration** (local > configuration > configuration de la console). Sélectionnez **VGA**, cliquez sur **Save** (enregistrer), puis cliquez sur OK afin de redémarrer.



Ensuite, activez LOM dans l'interface graphique utilisateur (GUI), puis redémarrez l'appareil. Dans l'interface graphique utilisateur (GUI) de l'appareil, choisissez **Local > Configuration > Console Configuration** (local > configuration > configuration de la console). Choisissez **Physical Serial Port (port série physique) ou LOM, cliquez surSave** (enregistrer), puis cliquez sur OK pour redémarrer.

Maintenant, essayez de vous connecter de nouveau.

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

Étape 9 : Arrêtez le périphérique et terminez un cycle d'alimentation, c'est-à-dire retirez physiquement le câble d'alimentation pendant une minute, rebranchez-le, puis mettez-le sous tension. Une fois l'appareil mis sous tension, exécutez la commande suivante :

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

Étape 10 : Exécutez cette commande à partir de l'appareil en question. Cette étape effectue une réinitialisation à froid de la bmc :

```
ipmitool bmc reset cold
```

Étape 11 : Exécutez cette commande depuis un système sur le même réseau local que l'appareil (autrement dit, sans passer par aucun routeur intermédiaire) :

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

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

Envoyez le fichier de résultats /var/tmp/arpcache au service d'assistance technique de Cisco afin de déterminer si le BMC répond à une demande d'ARP.

La connexion à l'interface LOM s'est déconnectée au cours du redémarrage

Lorsque vous redémarrez un centre de gestion FireSIGHT ou un appareil FirePOWER, vous pourriez perdre la connexion à l'appareil. La sortie lors du redémarrage de l'appareil par

l’intermédiaire de la CLI est affichée ici :

```
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
```

La sortie en surbrillance **Unmounting fuse control filesystem (désinstallation du système de fichiers de la commande par fusible). Un indique que la connexion à l’appareil est interrompue en raison du protocole STP (Spanning Tree Protocol) qui est activé sur le commutateur auquel le système FireSIGHT est connecté.** Après le redémarrage des appareils gérés, cette erreur s’affiche :

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

> **Note**: Avant de pouvoir vous connecter à un appareil LOM/SOL, vous devez désactiver le protocole STP (Spanning Tree Protocol) sur n’importe quel équipement de commutation de tierce partie connecté à l’interface de gestion de l’appareil.

Une connexion LOM du système FireSIGHT est partagée avec le port de gestion. Le lien du port de gestion s’affaiblit pour une durée très brève pendant le redémarrage. Puisque le lien s’affaiblit et qu’il est ensuite récupéré, cela pourrait déclencher un délai dans le port du commutateur (généralement 30 secondes avant que commence la circulation du trafic) en raison de l’écoute ou de la connaissance de l’état du port du commutateur causé par la configuration STP sur le port.