Résolution des problèmes de connectivité et d'enregistrement avec AMP sur FireSIGHT Management Center

Contenu

Introduction

Un FireSIGHT Management Center de votre déploiement peut se connecter au cloud Cisco. Après avoir configuré FireSIGHT Management Center pour se connecter au cloud, vous pouvez recevoir des enregistrements d'analyses, de détections de programmes malveillants et de mises en quarantaine. Les enregistrements sont stockés dans la base de données FireSIGHT Management Center en tant qu'événements de programme malveillant. Par défaut, le cloud envoie des événements de programmes malveillants pour tous les groupes de votre organisation, mais vous pouvez les limiter par groupe lorsque vous configurez la connexion. Ce document traite de divers problèmes et des étapes de dépannage de la fonction AMP (Advanced Malware Protection) d'un FireSIGHT Management Center.

Le port ou le serveur est bloqué dans le pare-feu

Si FireSIGHT Management Center ne parvient pas à se connecter à la console de cloud FireAMP ou ne reçoit pas d'événements de programme malveillant, vous devez vérifier si les ports requis sont bloqués par le pare-feu. Un FireSIGHT Management Center utilise le port 443 pour recevoir les événements de programmes malveillants basés sur les terminaux depuis la console FireAMP. Le port 32137 est requis pour que les appliances FirePOWER effectuent des recherches de programmes malveillants dans le cloud Cisco.

Pour en savoir plus sur les numéros de port et les adresses de serveur requis, lisez les documents suivants :

- Ports de communication requis pour le fonctionnement de FireSIGHT System
- Serveurs requis pour le fonctionnement d'AMP

Adresse MAC utilisée

Symptôme

Lorsque vous essayez d'enregistrer un FireSIGHT Management Center dans un cloud privé et d'effectuer la connexion initiale, vous pouvez recevoir un message indiquant que l'adresse MAC est déjà utilisée.

Motif

Lorsqu'un FireSIGHT Management Center est remplacé en raison d'une défaillance matérielle et que l'unité de remplacement n'est pas correctement désinscrite du cloud, vous pouvez rencontrer ce problème.

Solution

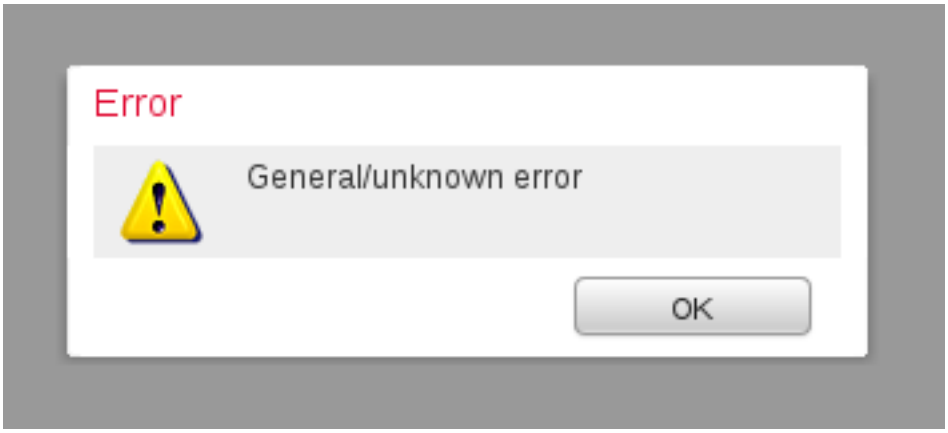
Avant de remplacer un appareil, vous devez annuler l'enregistrement de FireSIGHT Management Center à partir du cloud FireAMP. Vous devez également supprimer FireSIGHT Management Center du cloud FireAMP. Cela empêche qu'une adresse MAC ne soit perçue comme étant utilisée.

> **Astuce** : Lisez ce document pour en savoir plus sur la procédure à suivre pour annuler l'enregistrement d'un appareil dans le cloud FireAMP et supprimer un cloud de FireSIGHT Management Center.

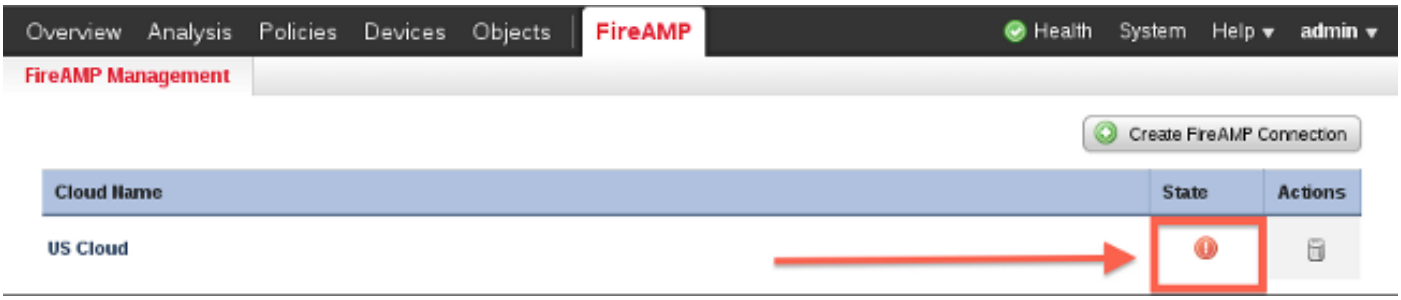
Erreur générale/inconnue affichée

Symptôme

Lors de la connexion d'un FireSIGHT Management Center réinstallé ou de remplacement à une console FireAMP, un message d'erreur s'affiche. Il affiche une erreur Général/Inconnu.



Lorsque le message d'erreur Général/inconnu apparaît, l'état de la connexion FireAMP sur FireSIGHT Management Center devient critique. L'interface Web affiche une icône rouge.



Motif

Ce problème se produit lorsqu'une adresse MAC d'un FireSIGHT Management Center, qui vient d'être réinstallée ou remplacée, est toujours enregistrée dans une console FireAMP.

Solution

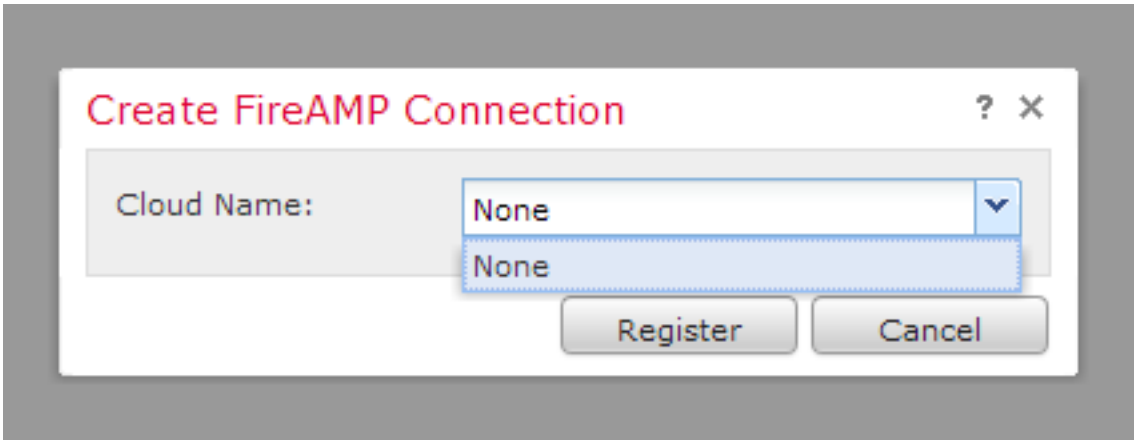
Avant de réinstaller ou de remplacer un appareil, vous devez annuler l'enregistrement de FireSIGHT Management Center à partir du cloud FireAMP. Vous devez également supprimer FireSIGHT Management Center du cloud FireAMP. Cela empêche qu'une adresse MAC ne soit perçue comme étant utilisée.

> **Astuce** : Lisez ce document pour en savoir plus sur la procédure à suivre pour annuler l'enregistrement d'un appareil dans le cloud FireAMP et supprimer un cloud de FireSIGHT Management Center.

Impossible de sélectionner un cloud

Symptôme

Lors de la création d'une connexion entre FireSIGHT Management Center et la console de cloud FireAMP, aucune option de liste déroulante n'est disponible pour le cloud américain ou le cloud de l'UE.



Motif

Ce problème se produit lorsqu'un FireSIGHT Management Center ne parvient pas à résoudre le nom d'hôte api.amp.sourcefire.com.

Afin de vérifier le problème, exécutez une commande nslookup sur la CLI de FireSIGHT Management Center. Vérifiez si les paramètres DNS sont correctement configurés sur FireSIGHT Management Center :

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
```

Le résultat suivant s'affiche lorsque DNS ne parvient pas à résoudre le nom d'hôte sur FireSIGHT Management Center :

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com

Server:         192.168.45.2
Address:        192.168.45.2#53

** server can't find api.amp.sourcefire.com
```

Vous trouverez ci-dessous la sortie si le DNS est correctement résolu sur FireSIGHT Management Center :

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
Server:         192.168.45.1
Address:        192.168.45.1#53

Non-authoritative answer:
api.amp.sourcefire.com
Name:   xxxx.xxxx.xxxx
Address: xx.xx.xx.xx
```

Solution

- Si FireSIGHT Management Center ne parvient pas à résoudre le nom d'hôte, vous devez vérifier si les paramètres DNS du Management Center sont corrects.
- Si FireSIGHT Management Center est en mesure de résoudre le nom d'hôte, mais ne peut pas accéder à api.amp.sourcefire.com via un pare-feu, vérifiez les règles et paramètres du pare-feu.

Lors du processus de création de connexion, si un FireSIGHT Management Center ne parvient pas à résoudre le nom d'hôte, le message d'erreur suivant est consigné dans le httpsd_error_log :

```
Error attempting curl for FireAMP: System
```

Par exemple, la sortie de journal suivante montre que le Centre de défense n'a pas terminé la commande curl sur api.amp.sourcefire.com :

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:38:13.433765 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
```

```
[Thu Jul 18 12:38:14.338174 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352374 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
Error attempting curl for FireAMP: System (/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L
--max-redirs 5 --max-filesize 104857600 --sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H
Accept: application/vnd.sourcefire.fireamp.dc+json; version=1
https://api.amp.sourcefire.com/clouds) Failed at /usr/local/sf/lib/perl/5.10.1/SF/System.pm line
7499., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352432 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
No cloud data returned at /usr/local/sf/lib/perl/5.10.1/SF/FireAMP.pm line 145., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352478 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```

Lors du processus de création de connexion, si le message suivant est consigné dans le httpsd_error_log sans erreur, il indique que FireSIGHT Management Center est en mesure de résoudre le nom d'hôte :

```
getCloudData completed
```

Par exemple, le résultat suivant montre qu'un Management Center termine une commande curl sur api.amp.sourcefire.com :

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:42:54.949461 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.856432 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.931106 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```