Dépannez les questions de Connectivité et d'enregistrement avec l'AMP au centre de Gestion de FireSIGHT

Contenu

Introduction

Un centre de Gestion de FireSIGHT dans votre déploiement peut connecter à Cisco le nuage. Après que vous configuriez un centre de Gestion de FireSIGHT pour se connecter au nuage, vous pouvez recevoir des enregistrements des balayages, des détections de malware, et des quarantaines. Les enregistrements sont enregistrés dans la base de données de centre de Gestion de FireSIGHT comme événements de malware. Par défaut, le nuage envoie des événements de malware pour tous les groupes dans votre organisation, mais vous pouvez limiter par le groupe quand vous configurez la connexion. Ce document discute de diverses questions et étapes de dépannage sur la caractéristique avancée de protection de malware (AMP) d'un centre de Gestion de FireSIGHT.

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

Si un centre de Gestion de FireSIGHT ne peut pas se connecter à la console de nuage de FireAMP, ou à ne pas recevoir des événements de malware, vous devez vérifier si les ports exigés blosked par le Pare-feu. Un centre de Gestion de FireSIGHT emploie le port 443 pour recevoir des événements basés sur point de malware de la console de FireAMP. Le port 32137 est exigé pour que des appliances de FirePOWER exécutent des consultations de malware dans

le nuage de Cisco.

Afin de se renseigner plus sur les numéros de port et les adresses du serveur requis, lisez les documents suivants :

- Ports de transmission requis pour l'exploitation du système de FireSIGHT
- Serveurs requis pour l'exécution d'AMP

Adresse MAC en service

Symptôme

Quand vous tentez d'enregistrer un centre de Gestion de FireSIGHT à un nuage privé et d'exécuter la connexion initiale, vous pouvez recevoir un message indiquant que l'adresse MAC est déjà en service.

Raison

Quand un centre de Gestion de FireSIGHT est dû remplacé à une défaillance matérielle, et l'unité de rechange n'est pas correctement des non enregistrés du nuage, vous pouvez éprouver cette question.

Solution

Avant que vous remplaciez une appliance, vous devez radier de l'immatriculation le centre de Gestion de FireSIGHT du nuage de FireAMP. Vous devriez également retirer votre centre de Gestion de FireSIGHT du nuage de FireAMP. Ceci empêche une adresse MAC d'être perçue en tant qu'en service.

> **Conseil** : Lisez ce document pour apprendre le processus de détail sur la façon dont radier de l'immatriculation une appliance du nuage de FireAMP et supprimer un nuage du centre de Gestion de FireSIGHT.

Erreur générale/inconnue est affichée

Symptôme

En connectant un centre réimagé ou de remplacement de FireSIGHT de Gestion à une console de FireAMP, un message d'erreur apparaît. Il affiche `erreur générale/inconnue`.

Quand `message d'erreur général/inconnu` apparaît, l'état de la connexion de FireAMP au centre de Gestion de FireSIGHT devient essentiel. L'interface web affiche une icône rouge.

Raison

Cette question se produit quand une adresse MAC d'un centre de Gestion de FireSIGHT, qui a été juste réimagé ou remplacé est toujours en cours d'enregistrement à une console de FireAMP.

Solution

Avant que vous réimagiez ou remplaciez une appliance, vous devez radier de l'immatriculation le centre de Gestion de FireSIGHT du nuage de FireAMP. Vous devriez également retirer votre centre de Gestion de FireSIGHT du nuage de FireAMP. Ceci empêche une adresse MAC d'être perçue en tant qu'en service.

> **Conseil** : Lisez ce document pour apprendre le processus de détail sur la façon dont radier de l'immatriculation une appliance du nuage de FireAMP et supprimer un nuage du centre de Gestion de FireSIGHT.

Incapable de sélectionner un nuage

Symptôme

En créant une connexion d'un centre de Gestion de FireSIGHT à la console de nuage de FireAMP, il y a aucun relâchez vers le bas les options trouvées pour le nuage des USA ou l'UE opacifient.

Raison

Cette question se produit quand un centre de Gestion de FireSIGHT ne peut pas résoudre l'adresse Internet `api.amp.sourcefire.com`.

Afin de vérifier la question, exécutez un `nslookup` sur le CLI du centre de Gestion de FireSIGHT. Vérifiez si les configurations de DN sont correctement configurées au centre de Gestion de FireSIGHT :

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

La sortie suivante est affichée quand les DN ne peut pas résoudre l'adresse Internet au centre de Gestion de FireSIGHT :

```
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
```

Est ci-dessous la sortie si des DN est correctement résolus au centre de Gestion de FireSIGHT :

```
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 un centre de Gestion de FireSIGHT ne peut pas résoudre l'adresse Internet, vous devez vérifier si les configurations de DN au centre de Gestion sont correctes.
- Si un centre de Gestion de FireSIGHT peut résoudre l'adresse Internet, mais incapable d'accéder à `api.amp.sourcefire.com` par un Pare-feu, vérifiez les règles et les configurations de Pare-feu.

Pendant le procédé de création de connexion, si un centre de Gestion de FireSIGHT ne peut pas résoudre l'adresse Internet, le message d'erreur suivant est ouvert une session le `httpsd_error_log` :

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

Par exemple, la sortie suivante de log affiche à la défense manquer central pour se terminer la commande de `boucle à 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/
```

Pendant le procédé de création de connexion, si le message suivant est ouvert une session le `httpsd_error_log` sans erreur, il indique que le centre de Gestion de FireSIGHT peut résoudre l'adresse Internet :

```
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/

Par exemple, la sortie suivante prouve qu'un centre de Gestion se termine une commande de boucle à 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/