在FireSIGHT管理中心上排除AMP的连接和注册问题

目录

简介

部署中的FireSIGHT管理中心可以连接到思科云。配置FireSIGHT管理中心以连接到云后，您可以接收扫描、恶意软件检测和隔离的记录。记录作为恶意软件事件存储在FireSIGHT管理中心数据库中。默认情况下，云会为组织内的所有组发送恶意软件事件，但在配置连接时，您可以按组进行限制。本文档讨论FireSIGHT管理中心高级恶意软件防护(AMP)功能的各种问题和故障排除步骤。

端口或服务器在防火墙中被阻止

如果FireSIGHT管理中心无法连接到FireAMP云控制台，或者没有接收恶意软件事件，则必须检查所需端口是否由防火墙部署。FireSIGHT管理中心使用端口443从FireAMP控制台接收基于终端的恶意软件事件。FirePOWER设备在思科云中执行恶意软件查找时需要端口32137。

要了解有关所需端口号和服务器地址的详细信息，请阅读以下文档：

- FireSIGHT系统运行所需的通信端口
- AMP操作所需的服务器

使用中的MAC地址

症状

当您尝试将FireSIGHT管理中心注册到私有云并执行初始连接时，您可能会收到一条消息，指示MAC地址已在使用。

原因

当FireSIGHT管理中心因硬件故障而更换，并且更换设备未从云中正确注销时，您可能会遇到此问题。

解决方案

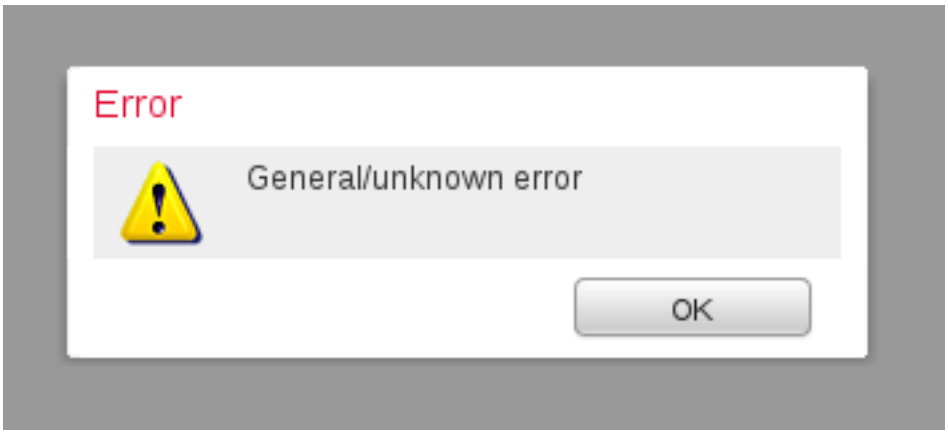
在更换设备之前，必须从FireAMP云取消注册FireSIGHT管理中心。您还应从FireAMP云中删除FireSIGHT管理中心。这可防止MAC地址被视为正在使用。

> **提示：**请阅读本文档，了解如何从FireAMP云注销设备和从FireSIGHT管理中心删除云的详细流程。

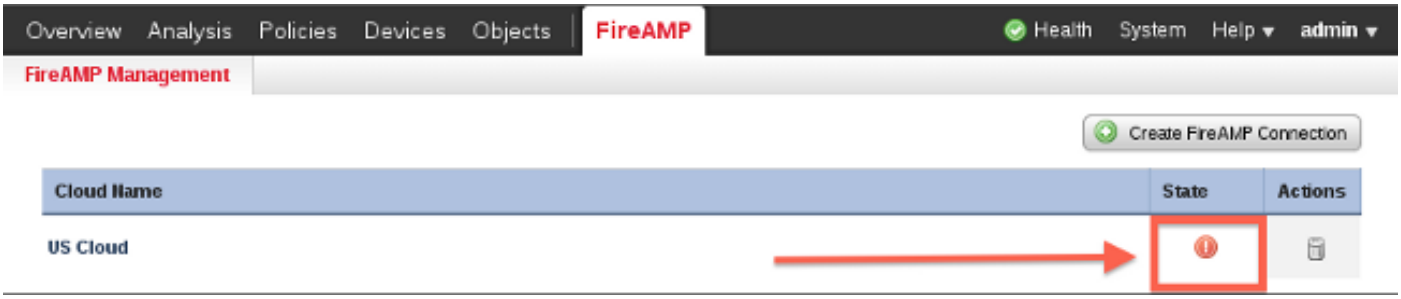
显示常规/未知错误

症状

将重新映像或更换的FireSIGHT管理中心连接到FireAMP控制台时，会显示错误消息。它显示一般/未知错误。



出现“General/unknown”错误消息时，FireSIGHT管理中心上的FireAMP连接状态变得至关重要。网络界面显示红色图标。



原因

当刚刚重新映像或更换的FireSIGHT管理中心的MAC地址仍注册到FireAMP控制台时，会发生此问题。

解决方案

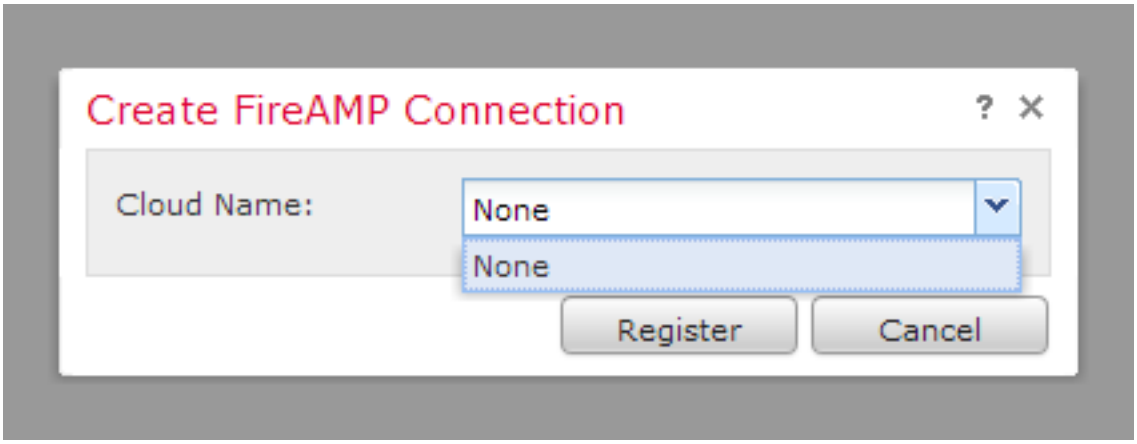
在重新映像或更换设备之前，必须从FireAMP云取消注册FireSIGHT管理中心。您还应从FireAMP云中删除FireSIGHT管理中心。这可防止MAC地址被视为正在使用。

> **提示：**请阅读本文档，了解如何从FireAMP云注销设备和从FireSIGHT管理中心删除云的详细流程。

无法选择云

症状

当创建从FireSIGHT管理中心到FireAMP云控制台的连接时，找不到适用于美国云或欧盟云的下拉选项。



原因

当FireSIGHT管理中心无法解析主机名api.amp.sourcefire.com时，会发生此问题。

要验证问题，请在FireSIGHT管理中心的CLI上执行nslookup。检查FireSIGHT管理中心上的DNS设置是否配置正确：

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

当DNS无法解析FireSIGHT管理中心的主机名时，将显示以下输出：

```
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
```

如果DNS在FireSIGHT管理中心上正确解析，则输出如下：

```
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
```

解决方案

- 如果FireSIGHT管理中心无法解析主机名，则需要验证管理中心上的DNS设置是否正确。
- 如果FireSIGHT管理中心能够解析主机名，但无法通过防火墙访问api.amp.sourcefire.com，请检查防火墙规则和设置。

在连接创建过程中，如果FireSIGHT管理中心无法解析主机名，则httpsd_error_log中会记录以下错误消息:

Error attempting curl for FireAMP: System

例如，以下日志输出显示防御中心未能完成api.amp.sourcefire.com的curl命令：

```
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/
```

在连接创建过程中，如果以下消息在httpsderrorlog中记录且未出现错误，则表明FireSIGHT管理中心能够解析主机名：

```
getCloudData completed
```

例如，以下输出显示管理中心完成了curl命令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/