排除故障与安培的连接和注册问题在FireSIGHT管理中心

目录

简介

在您的部署的一个FireSIGHT管理中心能连接到思科网云。在您配置FireSIGHT管理中心连接到网云后，您能接收扫瞄、恶意软件检测和检疫记录。记录在FireSIGHT管理中心数据库存储作为恶意软件事件。默认情况下，网云发送所有组的恶意软件事件在您的组织内，但是您能由组限制，当您配置连接时。本文讨论多种问题和故障排除步骤在FireSIGHT管理中心的先进的恶意软件保护(安培)功能。

波尔特或服务器在防火墙阻塞

如果FireSIGHT管理中心无法连接到FireAMP Cloud控制台或者不接收恶意软件事件，您必须检查需要的端口是否由防火墙blosked。接收的FireSIGHT管理中心用途端口443终端根据从FireAMP控制台的恶意软件事件。端口32137要求为了FirePOWER设备能在思科Cloud中执行恶意软件查找。

为了得知更多所需端口编号和服务器地址，请读以下文档：

- FireSIGHT系统操作的需要的通信端口
- 安培操作的所需的服务器

MAC地址在使用中

症状

当您尝试注册FireSIGHT管理中心到一私有网云和进行初始连接时，您可以收到表明的消息MAC地址已经是在使用中的。

原因

当FireSIGHT管理中心替换的归结于硬件故障时，并且替换单元没有从网云适当地未注册，您可以遇到此问题。

解决方案

在您替换设备前，您必须注销登记从FireAMP Cloud的FireSIGHT管理中心。您应该从FireAMP网云也删除您的FireSIGHT管理中心。这防止MAC地址被察觉作为在使用中。

> **提示**：读本文了解关于怎样的详细信息进程注销登记从FireAMP Cloud的一个设备和删除从FireSIGHT管理中心的一网云。

常规/未知错误显示

症状

当连接一个被再镜像的或更换FireSIGHT管理中心对FireAMP控制台时，错误消息出现。它显示/。

当/出现时， FireAMP连接的状态在FireSIGHT管理中心的变得关键。Web接口显示一个红色图标。

原因

此问题出现，当FireSIGHT管理中心的MAC地址，被再了镜像或替换时仍然注册对FireAMP控制台。

解决方案

在您再镜像或替换设备前，您必须注销登记从FireAMP Cloud的FireSIGHT管理中心。您应该从FireAMP网云也删除您的FireSIGHT管理中心。这防止MAC地址被察觉作为在使用中。

> **提示**：读本文了解关于怎样的详细信息进程注销登记从FireAMP Cloud的一个设备和删除从FireSIGHT管理中心的一网云。

无法选择Cloud

症状

当创建从FireSIGHT管理中心的一连接到FireAMP Cloud控制台，没有时请下降下来为美国Cloud或EU找到的选项Cloud。

原因

当FireSIGHT管理中心无法解决主机名api.amp.sourcefire.com此问题出现。

为了验证问题，请执行在FireSIGHT管理中心CLI的一nslookup。检查DNS设置是否在FireSIGHT管理中心适当地配置：

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

当DNS无法解决在FireSIGHT管理中心时的主机名以下输出显示：

```
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
```

下面输出，如果DNS在FireSIGHT管理中心适当地被解决：

```
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管理中心无法解决主机名，您需要验证，如果在管理中心的DNS设置正确。
- 如果FireSIGHT管理中心能解决主机名，但是无法通过防火墙访问api.amp.sourcefire.com，请检查防火墙规则和设置。

在连接创建进程中，如果FireSIGHT管理中心无法解决主机名，以下错误消息登陆httpsd_error_log：

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

例如，日志输出以下表示防御中心失败完成命令到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/

在连接创建进程中，如果下列信息登陆`httpsd_error_log`，不用错误，它表明FireSIGHT管理中心能解决主机名：

```
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/
```

例如，以下表示管理中心完成命令对`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/
```