Solución de problemas de conectividad y registro con AMP en FireSIGHT Management Center

Contenido

Introducción

Un FireSIGHT Management Center de su implementación puede conectarse a la nube de Cisco. Después de configurar un FireSIGHT Management Center para conectarse a la nube, puede recibir registros de análisis, detecciones de malware y cuarentenas. Los registros se almacenan en la base de datos de FireSIGHT Management Center como eventos de malware. De forma predeterminada, la nube envía eventos de malware para todos los grupos de su organización, pero puede restringir por grupo al configurar la conexión. Este documento describe varios problemas y pasos de solución de problemas relacionados con la función de protección frente a malware avanzado (AMP) de FireSIGHT Management Center.

Puerto o servidor bloqueado en el firewall

Si un FireSIGHT Management Center no puede conectarse a la consola en la nube de FireAMP o no recibe eventos de malware, debe comprobar si el firewall bloquea los puertos necesarios. FireSIGHT Management Center utiliza el puerto 443 para recibir eventos de malware basados en terminales desde la consola de FireAMP. Se necesita el puerto 32137 para que los appliances FirePOWER realicen búsquedas de malware en la nube de Cisco.

Para obtener más información sobre los números de puerto y las direcciones de servidor requeridos, lea los siguientes documentos:

- Puertos de comunicación necesarios para el funcionamiento del sistema FireSIGHT
- Servidores necesarios para el funcionamiento de AMP

Dirección MAC en uso

Síntoma

Cuando intente registrar un FireSIGHT Management Center en una nube privada y realice la conexión inicial, es posible que reciba un mensaje que indique que la dirección MAC ya está en uso.

Motivo

Cuando se reemplaza un FireSIGHT Management Center debido a una falla de hardware y la unidad de reemplazo no se desregistra correctamente desde la nube, es posible que experimente este problema.

Solución

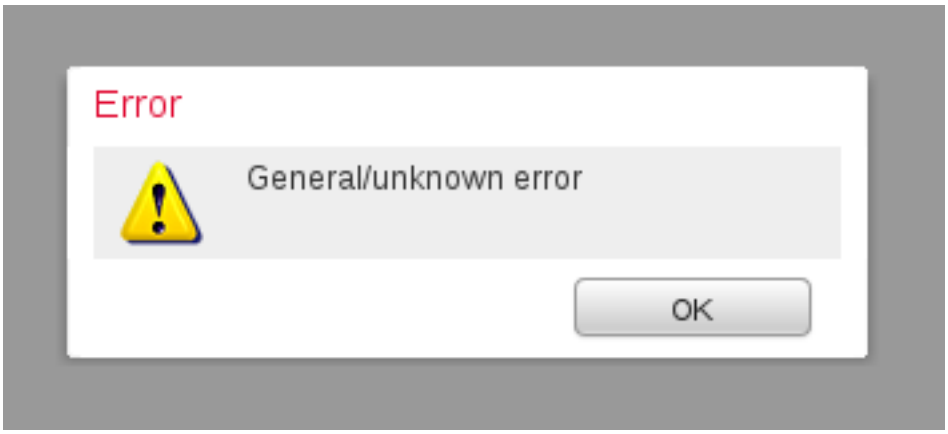
Antes de sustituir un dispositivo, debe desregistrar FireSIGHT Management Center de la nube de FireAMP. También debe eliminar su FireSIGHT Management Center de la nube de FireAMP. Esto evita que una dirección MAC se perciba como en uso.

> **Consejo:** Lea este documento para conocer el proceso detallado sobre cómo eliminar el registro de un dispositivo de la nube de FireAMP y eliminar una nube del FireSIGHT Management Center.

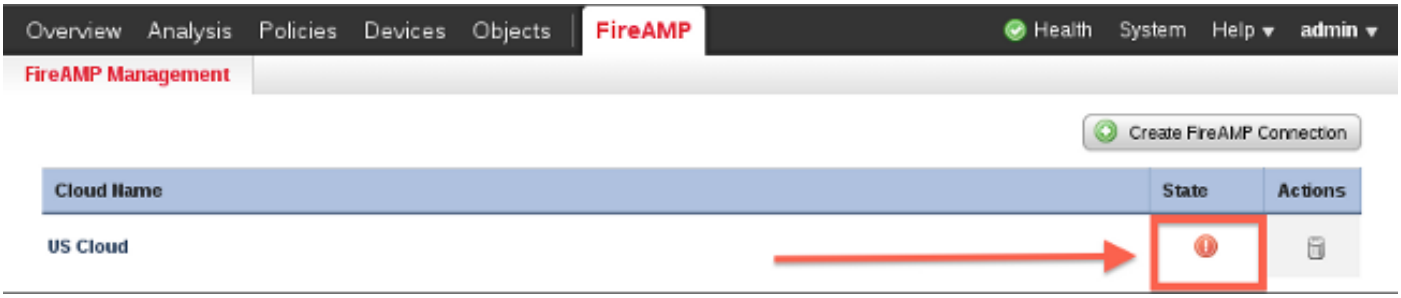
Se muestra el error general/desconocido

Síntoma

Cuando se conecta un FireSIGHT Management Center reinventado o se sustituye por una consola de FireAMP, aparece un mensaje de error. Muestra un error general/desconocido.



Cuando aparece el mensaje de error general/desconocido, el estado de la conexión de FireAMP en FireSIGHT Management Center se vuelve crítico. La interfaz web muestra un icono rojo.



Motivo

Este problema se produce cuando una dirección MAC de FireSIGHT Management Center, que acaba de volver a crear una imagen o reemplazarse, se sigue registrando en una consola de FireAMP.

Solución

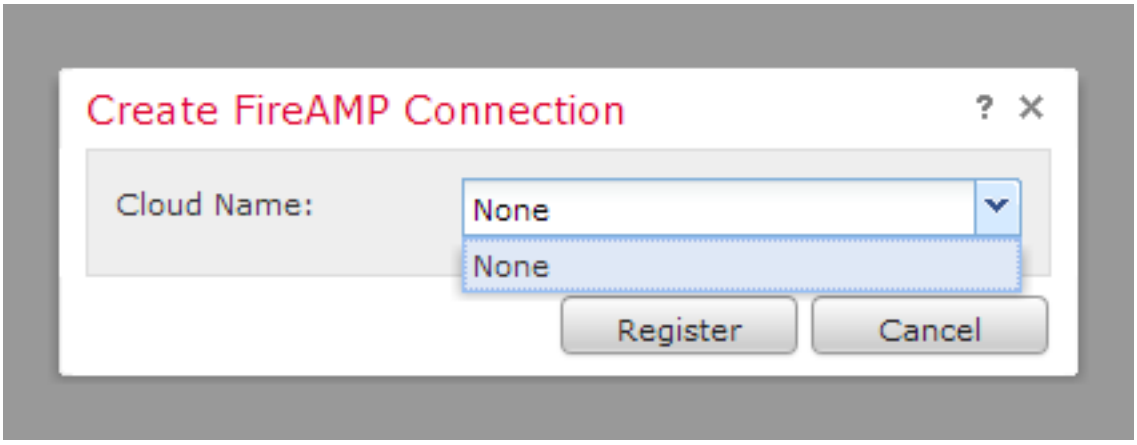
Antes de recrear imágenes o sustituir un dispositivo, debe desregistrar FireSIGHT Management Center de la nube de FireAMP. También debe eliminar su FireSIGHT Management Center de la nube de FireAMP. Esto evita que una dirección MAC se perciba como en uso.

> **Consejo:** Lea este documento para conocer el proceso detallado sobre cómo eliminar el registro de un dispositivo de la nube de FireAMP y eliminar una nube del FireSIGHT Management Center.

No se puede seleccionar una nube

Síntoma

Al crear una conexión de FireSIGHT Management Center a la consola en la nube de FireAMP, no se han encontrado opciones desplegables para la nube de EE. UU. o de la UE.



Motivo

Este problema ocurre cuando un FireSIGHT Management Center no puede resolver el nombre de host api.amp.sourcefire.com.

Para verificar el problema, realice una nslookup en la CLI de FireSIGHT Management Center.

Compruebe si la configuración de DNS está configurada correctamente en FireSIGHT Management Center:

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

Se muestra el siguiente resultado cuando DNS no puede resolver el nombre de host en 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
```

A continuación se muestra el resultado si el DNS se resuelve correctamente en el 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
```

Solución

- Si un FireSIGHT Management Center no puede resolver el nombre de host, debe verificar si la configuración de DNS del Management Center es correcta.
- Si un FireSIGHT Management Center puede resolver el nombre de host, pero no puede acceder a api.amp.sourcefire.com a través de un firewall, verifique las reglas y la configuración del firewall.

Durante el proceso de creación de la conexión, si un FireSIGHT Management Center no puede resolver el nombre de host, se registra el siguiente mensaje de error en el registro_error_httpsd:

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

Por ejemplo, el siguiente resultado del registro muestra que el Centro de Defensa no puede completar el comando curl en 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/
```

Durante el proceso de creación de la conexión, si se registra el siguiente mensaje en el registro de errores httpsd sin error, indica que el FireSIGHT Management Center puede resolver el nombre de host:

```
getCloudData completed
```

Por ejemplo, el siguiente resultado muestra que un Management Center completa un comando curl en 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/
```