Problemas de la Conectividad y del registro del Troubleshooting con el amperio en el centro de administración de FireSIGHT

Contenido

[Introducción](#)
[El puerto o el servidor se bloquea en el Firewall](#)
[Dirección MAC funcionando](#)
[Síntoma](#)
[Motivo](#)
[Solución](#)
[Visualizan al general/el Error desconocido](#)
[Síntoma](#)
[Motivo](#)
[Solución](#)
[Incapaz de seleccionar una nube](#)
[Síntoma](#)
[Motivo](#)
[Solución](#)

Introducción

Un centro de administración de FireSIGHT en su despliegue puede conectar con Cisco la nube. Después de que usted configure un centro de administración de FireSIGHT para conectar con la nube, usted puede recibir los expedientes de las exploraciones, de las detecciones del malware, y de las cuarentenas. Los expedientes se salvan en la base de datos del centro de administración de FireSIGHT como eventos del malware. Por abandono, la nube envía los eventos del malware para todos los grupos dentro de su organización, pero usted puede restringir por el grupo cuando usted configura la conexión. Este documento discute los diversos problemas y pasos de Troubleshooting en la característica avanzada de la protección de Malware (amperio) de un centro de administración de FireSIGHT.

El puerto o el servidor se bloquea en el Firewall

Si un centro de administración de FireSIGHT no puede conectar con la consola de la nube de FireAMP, o la recepción de los eventos del malware, usted debe marcar si los puertos requeridos blosked por el Firewall. Un centro de administración de FireSIGHT utiliza el puerto 443 para recibir los eventos punto final-basados del malware de la consola de FireAMP. El puerto 32137 se requiere para que los dispositivos de la potencia de fuego realicen las operaciones de búsqueda

del malware en la nube de Cisco.

Para aprender más sobre los números del puerto y las direcciones del servidor requeridos, lea los documentos siguientes:

- Puertos de comunicación requeridos para la operación del sistema de FireSIGHT
- Servidores requeridos para la operación amperio

Dirección MAC funcionando

Síntoma

Cuando usted intenta registrar un centro de administración de FireSIGHT a una nube privada y realizar la conexión inicial, usted puede recibir un mensaje que indica que la dirección MAC es ya funcionando.

Motivo

Cuando un centro de administración de FireSIGHT es substituido debido a una falla de hardware, y las unidades de reemplazo no se desregistran correctamente de la nube, usted puede experimentar este problema.

Solución

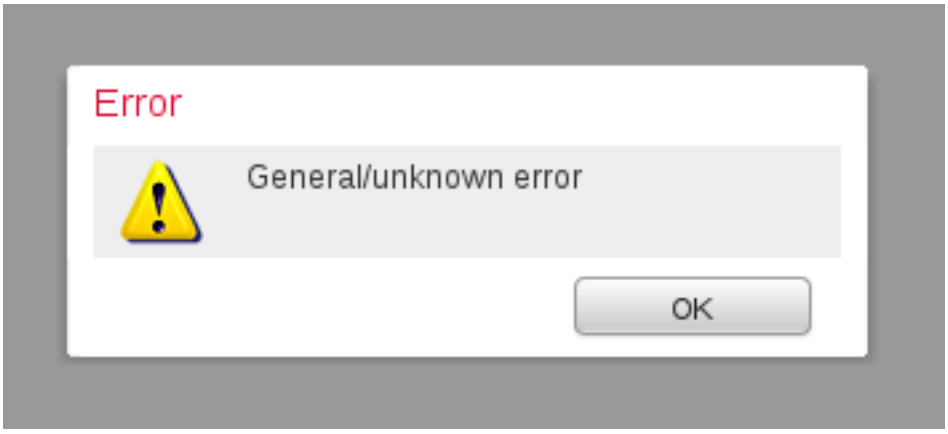
Antes de que usted substituya un dispositivo, usted debe desregistrar el centro de administración de FireSIGHT de la nube de FireAMP. Usted debe también quitar su centro de administración de FireSIGHT de la nube de FireAMP. Esto evita que una dirección MAC sea percibida como funcionando.

> Consejo: Lea este documento para aprender el proceso del detalle en cómo desregistrar un dispositivo de la nube de FireAMP y borrar una nube del centro de administración de FireSIGHT.

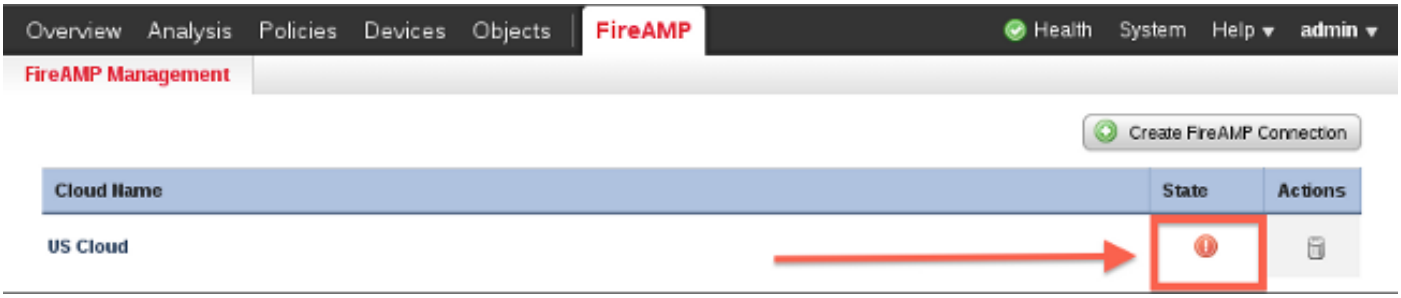
Visualizan al general/el Error desconocido

Síntoma

Al conectar un centro de administración reimaged o del reemplazo de FireSIGHT con una consola de FireAMP, un mensaje de error aparece. Visualiza un `general/un Error desconocido`.



Cuando aparece el `general/el mensaje de error desconocido`, el estado de la conexión de FireAMP en el centro de administración de FireSIGHT llega a ser crítico. La interfaz Web visualiza un icono rojo.



Motivo

Este problema ocurre cuando una dirección MAC de un centro de administración de FireSIGHT, que reimaged o acaba de substituirse todavía se está registrando a una consola de FireAMP.

Solución

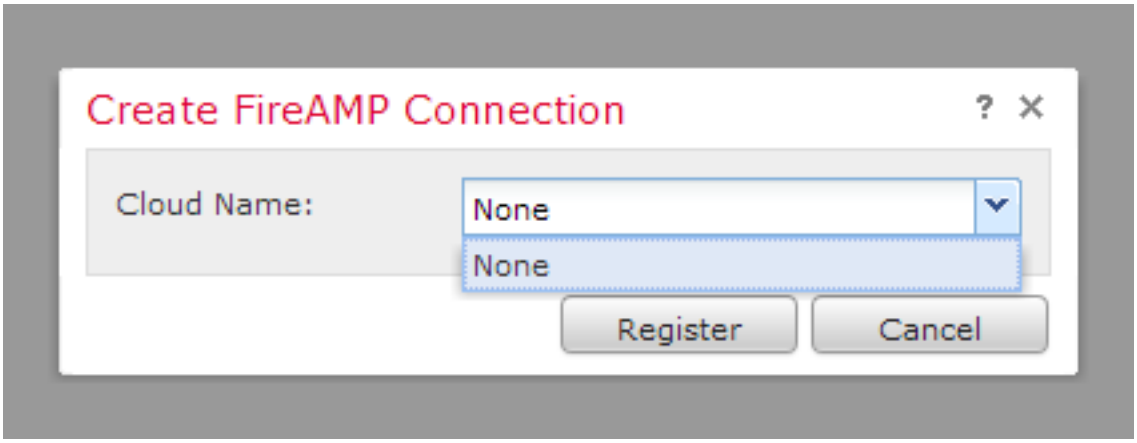
Antes de que usted nueva imagen o substituya un dispositivo, usted deba desregistrar el centro de administración de FireSIGHT de la nube de FireAMP. Usted debe también quitar su centro de administración de FireSIGHT de la nube de FireAMP. Esto evita que una dirección MAC sea percibida como funcionando.

> Consejo: Lea este documento para aprender el proceso del detalle en cómo desregistrar un dispositivo de la nube de FireAMP y borrar una nube del centro de administración de FireSIGHT.

Incapaz de seleccionar una nube

Síntoma

Al crear una conexión de un centro de administración de FireSIGHT a la consola de la nube de FireAMP, hay ningún caiga abajo las opciones encontradas para la nube E.E.U.U. o la nube EU.



Motivo

Este problema ocurre cuando un centro de administración de FireSIGHT no puede resolver el nombre de host `api.amp.sourcefire.com`.

Para verificar el problema, realice un `nslookup` en el CLI del centro de administración de FireSIGHT. Marque si las configuraciones DNS se configuran correctamente en el centro de administración de FireSIGHT:

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

Se visualiza el producto siguiente cuando el DNS no puede resolver el nombre de host en el centro de administración 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
```

Abajo está la salida si el DNS se resuelve correctamente en el centro de administración 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
```

Solución

- Si un centro de administración de FireSIGHT no puede resolver el nombre de host, usted necesita verificar si las configuraciones DNS en el centro de administración están correctas.
- Si un centro de administración de FireSIGHT puede resolver el nombre de host, pero incapaz de acceder `api.amp.sourcefire.com` con un Firewall, marque las reglas de firewall y las configuraciones.

Durante el proceso de la creación de la conexión, si un centro de administración de FireSIGHT no puede resolver el nombre de host, el mensaje de error siguiente se abre una sesión el `httpsd_error_log`:

Error attempting curl for FireAMP: System

Por ejemplo, la salida del registro siguiente muestra a defensa el fall de centro para completar el comando del `rizo a 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 la creación de la conexión, si el siguiente mensaje se abre una sesión el `httpsd_error_log` sin un error, indica que el centro de administración de FireSIGHT puede resolver el nombre de host:

```
getCloudData completed
```

Por ejemplo, el producto siguiente muestra que un centro de administración completa un comando del `rizo a 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/
```