Pesquise defeitos edições da Conectividade e do registro com o AMP no centro de gerenciamento de FireSIGHT

Índice

Introdução

Um centro de gerenciamento de FireSIGHT em seu desenvolvimento pode conectar a Cisco a nuvem. Depois que você configura um centro de gerenciamento de FireSIGHT para conectar à nuvem, você pode receber registros das varreduras, das detecções do malware, e das quarentena. Os registros são armazenados no base de dados do centro de gerenciamento de FireSIGHT como eventos do malware. À revelia, a nuvem envia eventos do malware para todos os grupos dentro de sua organização, mas você pode restringir pelo grupo quando você configura a conexão. Este documento discute vários edições e passos de Troubleshooting em característica avançada da proteção do malware (AMP) de um centro de gerenciamento de FireSIGHT.

A porta ou o server são obstruídos no Firewall

Se um centro de gerenciamento de FireSIGHT é incapaz de conectar ao console da nuvem de FireAMP, ou a não receber eventos do malware, você deve verificar se as portas exigidas blosked pelo Firewall. Um centro de gerenciamento de FireSIGHT usa a porta 443 para receber eventos valor--baseados do malware do console de FireAMP. A porta 32137 é exigida para que os dispositivos de FirePOWER executem consultas do malware na nuvem de Cisco.

A fim aprender mais sobre os números de porta e os endereços do servidor exigidos, leia os seguintes documentos:

- Portas de comunicação exigidas para a operação de sistema de FireSIGHT
- Servidores obrigatórios para a operação AMP

MAC address no uso

Sintoma

Quando você tenta registrar um centro de gerenciamento de FireSIGHT a uma nuvem privada e executar a conexão inicial, você pode receber uma mensagem que indica que o MAC address é já dentro uso.

Razão

Quando um centro de gerenciamento de FireSIGHT é substituído devido a uma falha do hardware, e a unidade de substituição não está removida registro corretamente da nuvem, você pode experimentar esta edição.

Solução

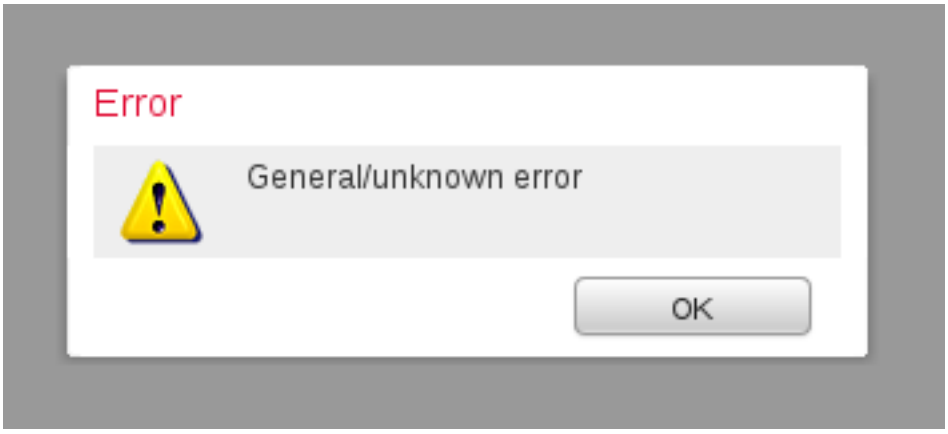
Antes que você substitua um dispositivo, você deve cancelar a matrícula o centro de gerenciamento de FireSIGHT da nuvem de FireAMP. Você deve igualmente remover seu centro de gerenciamento de FireSIGHT da nuvem de FireAMP. Isto impede que um MAC address esteja percebido como no uso.

> **Tip**: Leia este documento para aprender o processo do detalhe em como cancelar a matrícula um dispositivo da nuvem de FireAMP e suprimir de uma nuvem do centro de gerenciamento de FireSIGHT.

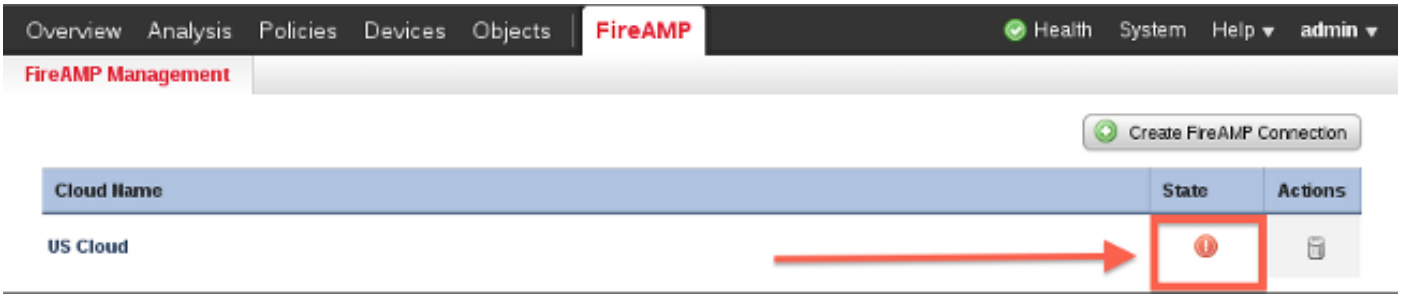
O general/erro desconhecido é indicado

Sintoma

Ao conectar um centro de gerenciamento reimaged ou da substituição de FireSIGHT a um console de FireAMP, um Mensagem de Erro aparece. Indica um `geral/erro desconhecido`.



Quando o `geral/mensagem de erro desconhecido` aparece, o estado da conexão de FireAMP no centro de gerenciamento de FireSIGHT torna-se crítico. A interface da WEB indica um ícone vermelho.



Razão

Esta edição ocorre quando um MAC address de um centro de gerenciamento de FireSIGHT, que reimaged ou seja substituído apenas está sendo registrado ainda a um console de FireAMP.

Solução

Antes que você nova imagem ou substitui um dispositivo, você deve cancelar a matrícula o centro de gerenciamento de FireSIGHT da nuvem de FireAMP. Você deve igualmente remover seu centro de gerenciamento de FireSIGHT da nuvem de FireAMP. Isto impede que um MAC address esteja percebido como no uso.

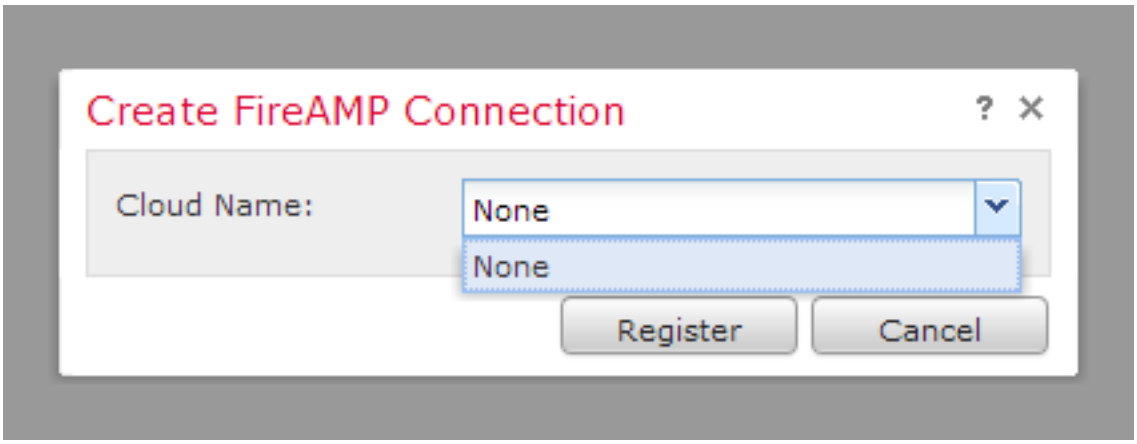
> **Tip**: Leia este documento para aprender o processo do detalhe em como cancelar a matrícula um dispositivo da nuvem de FireAMP e suprimir de uma nuvem do centro de gerenciamento de FireSIGHT.

Incapaz de selecionar uma nuvem

Sintoma

Ao criar uma conexão de um centro de gerenciamento de FireSIGHT ao console da nuvem de FireAMP, há nenhum deixe cair para baixo as opções encontradas para a nuvem E.U. ou a

nuvem EU.



Razão

Esta edição ocorre quando um centro de gerenciamento de FireSIGHT é incapaz de resolver o hostname `api.amp.sourcefire.com`.

A fim verificar a edição, execute um `nslookup no` CLI do centro de gerenciamento de FireSIGHT. Verifique se os ajustes DNS são configurados corretamente no centro de gerenciamento de FireSIGHT:

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

A seguinte saída é indicada quando o DNS é incapaz de resolver o hostname no centro de gerenciamento 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
```

Está abaixo a saída se o DNS é resolvido corretamente no centro de gerenciamento 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
```

Solução

- Se um centro de gerenciamento de FireSIGHT é incapaz de resolver o hostname, você precisa de verificar se os ajustes DNS no centro de gerenciamento estão corretos.
- Se um centro de gerenciamento de FireSIGHT pode resolver o hostname, mas incapaz de

alcançar `api.amp.sourcefire.com` com um Firewall, verifique as regras e os ajustes do Firewall.

Durante o processo da criação da conexão, se um centro de gerenciamento de FireSIGHT é incapaz de resolver o hostname, o seguinte Mensagem de Erro é entrado o `httpsd_error_log`:

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

Por exemplo, o seguinte registro de saída mostra à defesa o failing Center para terminar o comando da `onda 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 o processo da criação da conexão, se o seguinte mensagem é entrado o `httpsd_error_log` sem um erro, indica que o centro de gerenciamento de FireSIGHT pode resolver o hostname:

```
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/
```

Por exemplo, a seguinte saída mostra que um centro de gerenciamento termina um comando da `onda 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/
```