Solucione problemas de conectividade e registro com o AMP no FireSIGHT Management Center

Contents

Introduction

Um FireSIGHT Management Center em sua implantação pode se conectar à nuvem da Cisco. Depois de configurar um FireSIGHT Management Center para se conectar à nuvem, você pode receber registros de verificações, detecções de malware e quarentenas. Os registros são armazenados no banco de dados do FireSIGHT Management Center como eventos de malware. Por padrão, a nuvem envia eventos de malware para todos os grupos dentro da sua organização, mas você pode restringir por grupo ao configurar a conexão. Este documento discute vários problemas e as etapas de solução de problemas do recurso Advanced Malware Protection (AMP) de um FireSIGHT Management Center.

A porta ou o servidor está bloqueado no firewall

Se um FireSIGHT Management Center não puder se conectar ao FireAMP Cloud Console ou não receber eventos de malware, verifique se as portas necessárias estão bloqueadas pelo firewall. Um FireSIGHT Management Center usa a porta 443 para receber eventos de malware baseados em endpoints do console FireAMP. A porta 32137 é necessária para que os dispositivos FirePOWER executem pesquisas de malware no Cisco Cloud.

Para saber mais sobre os números de porta e endereços de servidor necessários, leia os seguintes documentos:

- Portas de comunicação necessárias para operação do sistema FireSIGHT
- Servidores necessários para operação da AMP

Endereço MAC em uso

Sintoma

Ao tentar registrar um FireSIGHT Management Center em uma nuvem privada e executar a conexão inicial, você poderá receber uma mensagem indicando que o endereço MAC já está em uso.

Razão

Quando um FireSIGHT Management Center é substituído devido a uma falha de hardware e a unidade de substituição não está adequadamente desregistrada na nuvem, você pode enfrentar esse problema.

Solução

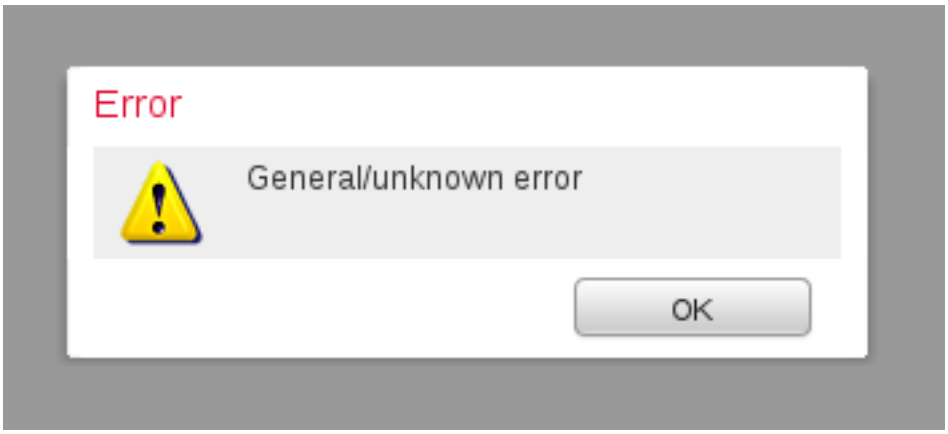
Antes de substituir um dispositivo, você deve cancelar o registro do FireSIGHT Management Center da nuvem do FireAMP. Você também deve remover o FireSIGHT Management Center da nuvem do FireAMP. Isso evita que um endereço MAC seja percebido como sendo usado.

> **Tip**: Leia este documento para saber mais sobre como cancelar o registro de um dispositivo da nuvem do FireAMP e excluir uma nuvem do FireSIGHT Management Center.

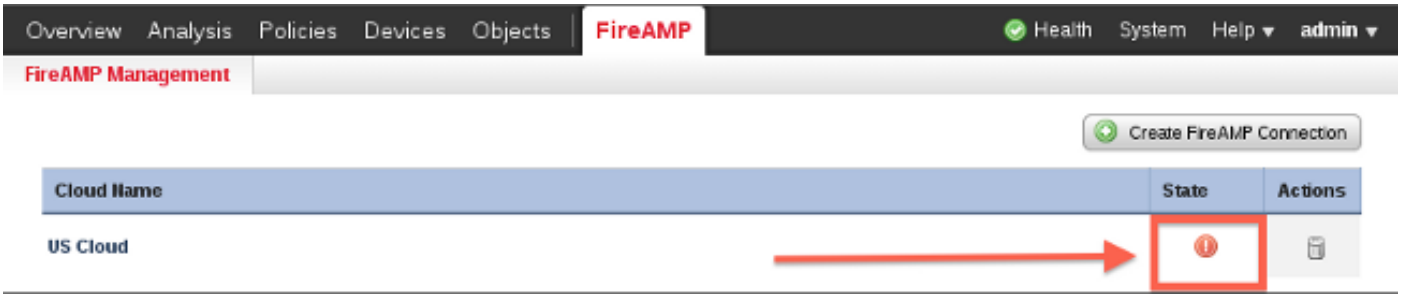
Erro geral/desconhecido é exibido

Sintoma

Ao conectar um FireSIGHT Management Center recriado ou substituto a um FireAMP Console, uma mensagem de erro é exibida. Ele exibe um erro geral/desconhecido.



Quando a mensagem de erro geral/desconhecido é exibida, o estado da conexão do FireAMP no FireSIGHT Management Center se torna crítico. A interface da Web exibe um ícone vermelho.



Razão

Esse problema ocorre quando um endereço MAC de um FireSIGHT Management Center, que acaba de ser recriado ou substituído, ainda está sendo registrado em um FireAMP Console.

Solução

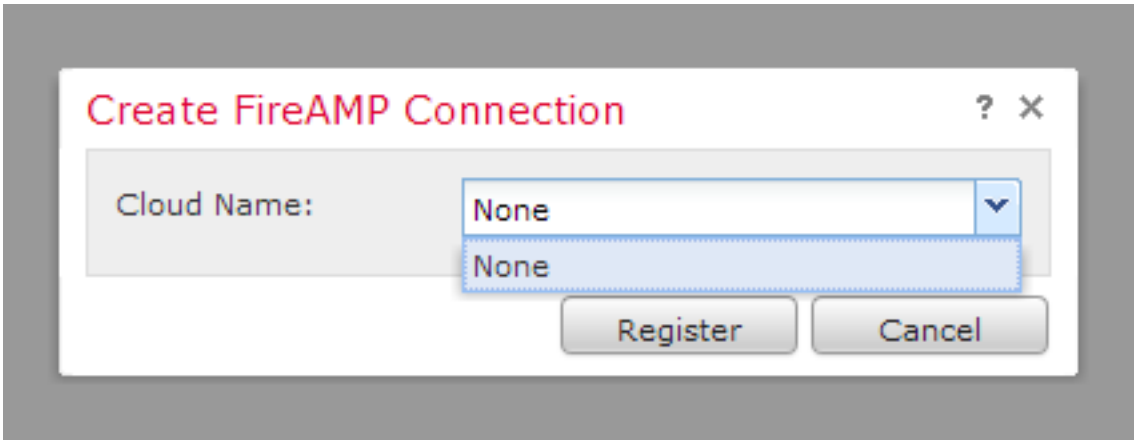
Antes de recriar ou substituir um dispositivo, você deve cancelar o registro do FireSIGHT Management Center da nuvem do FireAMP. Você também deve remover o FireSIGHT Management Center da nuvem do FireAMP. Isso evita que um endereço MAC seja percebido como sendo usado.

> **Tip**: Leia este documento para saber mais sobre como cancelar o registro de um dispositivo da nuvem do FireAMP e excluir uma nuvem do FireSIGHT Management Center.

Não é possível selecionar uma nuvem

Sintoma

Ao criar uma conexão de um FireSIGHT Management Center para o FireAMP Cloud Console, não há opções suspensas encontradas para a nuvem dos EUA ou para a nuvem da UE.



Razão

Esse problema ocorre quando um FireSIGHT Management Center é incapaz de resolver o nome de host api.amp.sourcefire.com.

Para verificar o problema, execute uma nslookup no CLI do FireSIGHT Management Center. Verifique se as configurações de DNS estão configuradas corretamente no FireSIGHT

Management Center:

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

A seguinte saída é exibida quando o DNS não consegue resolver o nome do host no 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
```

Abaixo está a saída se o DNS for resolvido corretamente no 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
```

Solução

- Se um FireSIGHT Management Center não puder resolver o nome do host, verifique se as configurações de DNS no Management Center estão corretas.
- Se um FireSIGHT Management Center for capaz de resolver o nome do host, mas não puder acessar api.amp.sourcefire.com por meio de um firewall, verifique as regras e configurações do firewall.

Durante o processo de criação da conexão, se um FireSIGHT Management Center não puder resolver o nome do host, a seguinte mensagem de erro será registrada no httpsd_error_log:

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

Por exemplo, a seguinte saída de registro mostra que o Defense Center não concluiu o comando curl para 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 de criação da conexão, se a seguinte mensagem estiver registrada no httpsd_error_log sem um erro, ela indica que o FireSIGHT Management Center é capaz de resolver o nome do host:

```
getCloudData completed
```

Por exemplo, a saída a seguir mostra que um Management Center completa um comando curl para 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/
```