FireSIGHT Management Center での AMP の接続および登録に関する問題のトラブルシューティング

目次

概要

展開内の FireSIGHT Management Center は、シスコのクラウドに接続できます。 クラウドに接続するように FireSIGHT Management Center を設定すると、スキャン、マルウェア検出、検疫のレコードを受信できるようになります。 これらのレコードは、FireSIGHT Management Center データベースにマルウェア イベントとして格納されます。 デフォルトで、クラウドは組織内のすべてのグループに関するマルウェア イベントを送信しますが、接続を設定するときにグループごとに制限できます。 このドキュメントでは、FireSIGHT Management Center の高度なマルウェア防御（AMP）機能に関するさまざまな問題とトラブルシューティング手順について説明します。

ポートまたはサーバがファイアウォールでブロックされる

FireSIGHT Management Center が FireAMP Cloud コンソールに接続できないか、またはマルウェア イベントを受信していない場合は、必要なポートがファイアウォールでブロックされているかどうかを確認する必要があります。 FireSIGHT Management Center は、ポート 443 を使用して FireAMP コンソールからエンドポイント ベースのマルウェア イベントを受信します。 FirePOWER アプライアンスがシスコのクラウド内でマルウェア検索を実行するには、ポート 32137 が必要です。

必要なポート番号とサーバ アドレスの詳細については、次のドキュメントを参照してください。

- FireSIGHT システムの動作に必要な通信ポート
- AMP の動作に必要なサーバ

使用中の MAC アドレス

症状

FireSIGHT Management Center をプライベート クラウドに登録し、初めて接続しようとすると、MAC アドレスがすでに使用中であることを示すメッセージを受信することがあります。

原因

ハードウェア障害のために FireSIGHT Management Center が交換され、交換ユニットがクラウドから正しく登録解除されていないときに、この問題が発生することがあります。

解決策

アプライアンスを交換する前に、FireAMP クラウドから FireSIGHT Management Center を登録解除する必要があります。 さらに、FireAMP クラウドから FireSIGHT Management Center を削除する必要があります。 これにより、MAC アドレスが使用中として認識されなくなります。

> **ヒント**： FireAMP クラウドからアプライアンスを登録解除し、FireSIGHT Management Center からクラウドを削除する詳しいプロセスについては、このドキュメントを参照してください。

General/unknown error が表示される

症状

再イメージ化または交換された FireSIGHT Management Center を FireAMP コンソールに接続すると、エラー メッセージが表示されます。 General/unknown error が表示されます。

General/unknown error メッセージが表示されると、FireSIGHT Management Center の FireAMP 接続のステータスがクリティカルになります。 Web インターフェイスに赤いアイコンが表示されます。

原因

この問題は、再イメージ化または交換された FireSIGHT Management Center の MAC アドレスが FireAMP コンソールに登録されたままになっているときに発生します。

解決策

アプライアンスを再イメージ化または交換する前に、FireAMP クラウドから FireSIGHT Management Center を登録解除する必要があります。 さらに、FireAMP クラウドから FireSIGHT Management Center を削除する必要があります。 これにより、MAC アドレスが使用中として認識されなくなります。

> **ヒント**： FireAMP クラウドからアプライアンスを登録解除し、FireSIGHT Management Center からクラウドを削除する詳しいプロセスについては、このドキュメントを参照してください。

クラウドを選択できない

症状

FireSIGHT Management Center から FireAMP Cloud コンソールへの接続を作成するときに、米国または EU のクラウドに対応するドロップ ダウン オプションが表示されません。

原因

この問題は、FireSIGHT Management Center がホスト名 api.amp.sourcefire.com を解決できないときに発生します。

この問題を検証するには、FireSIGHT Management Center の CLI で nslookup を実行します。 FireSIGHT Management Center で DNS が正しく設定されているかどうかを確認します。

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

FireSIGHT Management Center で DNS がホスト名を解決できないときは、次の出力が表示されます。

```
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
```

FireSIGHT Management Center で DNS が正しく解決されたときは、次の出力が表示されます。

```
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
```

解決策

- FireSIGHT Management Center がホスト名を解決できない場合は、Management Center の DNS 設定が正しいかどうかを検証する必要があります。
- FireSIGHT Management Center はホスト名は解決できるものの、ファイアウォールを介して api.amp.sourcefire.com にアクセスできない場合は、ファイアウォールのルールと設定を確認します。

接続の作成中に FireSIGHT Management Center がホスト名を解決できない場合は、httpsd_error_log に次のエラー メッセージが記録されます。

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

たとえば、次のログ出力は Defense Center が api.amp.sourcefire.com に対して curl コマンドを実行できなかったことを示しています。

```
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/
```

接続の作成中に、エラーなしで httpsd_error_log に次のメッセージが記録された場合は、FireSIGHT Management Center がホスト名を解決できたことを示しています。

```
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/

たとえば、次の出力は Management Center が api.amp.sourcefire.com に curl コマンドを実行できたことを示しています。

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/