أستكشاف أخطاء الاتصال والتسجيل وإصلاحها باستخدام AMP على مركز إدارة FireSIGHT

المحتويات

المقدمة

يمكن أن يتصل مركز إدارة FireSIGHT في عملية النشر لديك بسحابة Cisco. بعد تكوين FireSIGHT Management Center للاتصال بالسحابة، يمكنك تلقي سجلات من عمليات الفحص والكشف البرامج الضارة والحجر الصحي. يتم تخزين السجلات في قاعدة بيانات أحداث برامج ضارة. ترسل السحابة بشكل افتراضي أحداث البرامج الضارة لجميع المجموعات داخل مؤسستك، ولكن يمكنك تقييدها حسب المجموعة عند تكوين الاتصال. يناقش هذا المستند العديد من المشاكل وخطوات أستكشاف الأخطاء وإصلاحها فيما يتعلق بميزة "الحماية المتقدمة من البرامج الضارة" (AMP) من مركز إدارة FireSIGHT.

المنفذ أو الخادم محظور في جدار الحماية

إذا لم يتمكن FireSIGHT Management Center من الاتصال بوحدة تحكم سحابة FireAMP، أو عدم تلقي أحداث برامج ضارة، فيجب عليك التحقق مما إذا كانت المنافذ المطلوبة قد تم تكبيرها بواسطة جدار الحماية. يستخدم مركز إدارة FireSIGHT المنفذ 443 لتلقي أحداث البرامج الضارة المستندة إلى نقطة النهاية من وحدة تحكم FireAMP. يتطلب المنفذ 32137 لأجهزة FirePOWER لإجراء عمليات البحث عن البرامج الضارة في Cisco Cloud.

لمعرفة المزيد حول أرقام المنافذ وعناوين الخوادم المطلوبة، أقرأ المستندات التالية:

- منافذ الاتصال المطلوبة لتشغيل نظام FireSIGHT
- الخوادم المطلوبة لتشغيل AMP

عنوان MAC قيد الاستخدام

عرض

عند محاولة تسجيل مركز إدارة FireSIGHT إلى سحابة خاصة وإجراء الاتصال الأولي، قد تتلقى رسالة تشير إلى أن عنوان MAC قيد الاستخدام بالفعل.

سبب

عند إستبدال مركز إدارة FireSIGHT بسبب عطل في الجهاز، ولم يتم إلغاء تسجيل الوحدة البديلة بشكل صحيح من مجموعة النظراء، فقد تواجه هذه المشكلة.

الحل

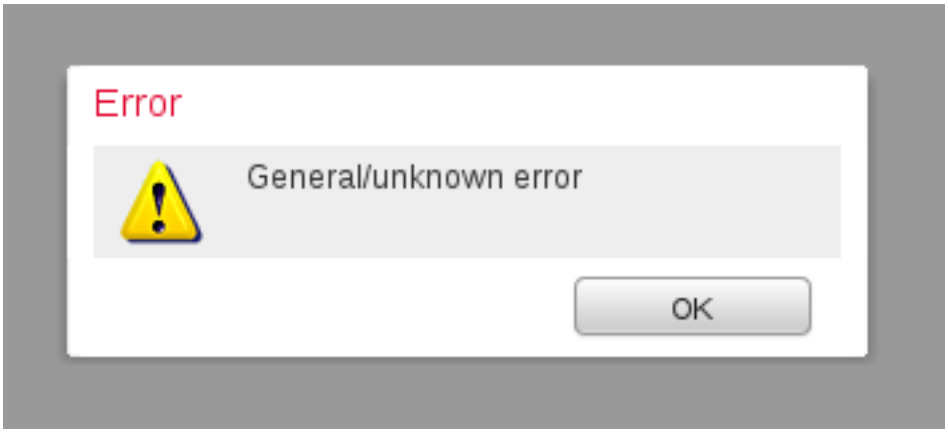
قبل إستبدال جهاز، يجب إلغاء تسجيل "مركز إدارة FireSIGHT" من السحابة FireAMP. يجب أيضا إزالة "مركز إدارة FireSIGHT" من سحابة FireAMP. يؤدي ذلك إلى منع التعرف على عنوان MAC على أنه قيد الاستخدام.

> **تلميح**: اقرأ هذا المستند للتعرف على العملية التفصيلية حول كيفية إلغاء تسجيل جهاز من سحابة FireAMP وحذف سحابة من مركز إدارة FireSIGHT.

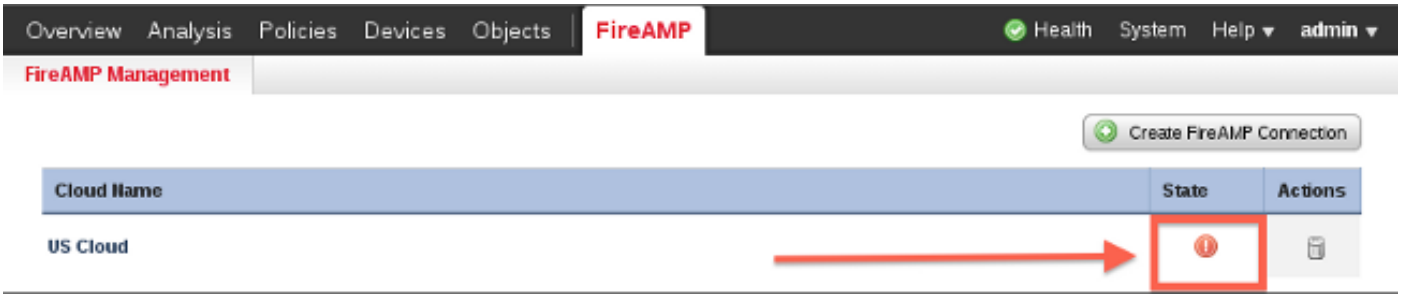
ظهور خطأ عام/غير معروف

عرض

عند توصيل FireSIGHT Management Center (مركز إدارة FireSIGHT) الذي تم تعويضه أو إستبداله بوحدة تحكم FireAMP، تظهر رسالة خطأ. يعرض خطأ عام/غير معروف.



عندما تظهر رسالة الخطأ العام/غير المعروف، تصبح حالة اتصال FireAMP على FireSIGHT Management Center حرجة. تعرض واجهة الويب أيقونة حمراء.



سبب

تحدث هذه المشكلة عندما يكون عنوان MAC الخاص بمركز إدارة FireSIGHT، والذي تم تعويضه أو إستبداله للتو ال يزال قيد التسجيل في وحدة تحكم FireAMP.

الحل

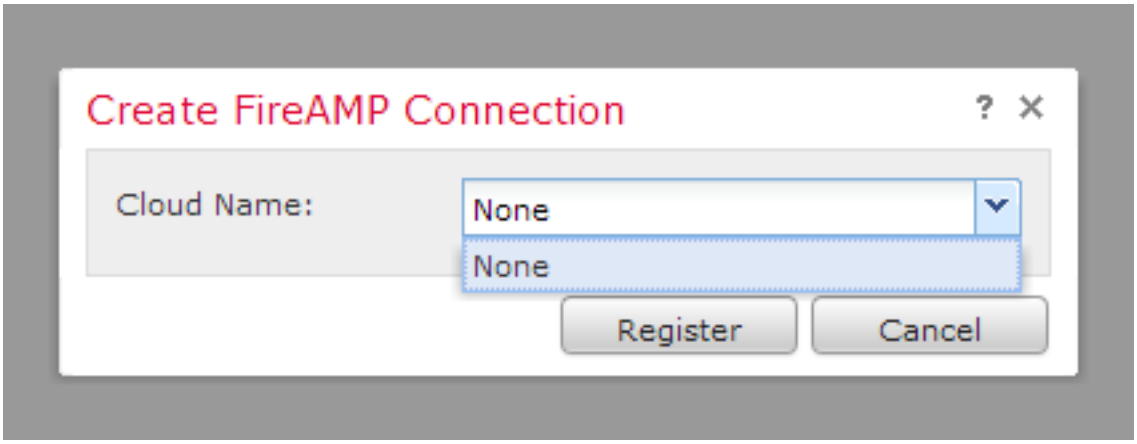
قبل إعادة تكوين جهاز أو إستبداله، يجب إلغاء تسجيل FireSIGHT Management Center من السحابة FireAMP. يجب أيضا إزالة "مركز إدارة FireSIGHT" من سحابة FireAMP. يؤدي ذلك إلى منع التعرف على عنوان MAC على أنه قيد الاستخدام.

> **تلميح**: اقرأ هذا المستند للتعرف على العملية التفصيلية حول كيفية إلغاء تسجيل جهاز من سحابة FireAMP وحذف سحابة من مركز إدارة FireSIGHT.

تعذر تحديد مجموعة النظراء

عرض

عند إنشاء اتصال من FireSIGHT Management Center بوحدة تحكم السحابة FireAMP، ال توجد خيارات منسدلة لسحابة الولايات المتحدة أو شبكة الاتحاد الأوروبي.



سبب

تحدث هذه المشكلة عندما يكون FireSIGHT Management Center غير قادر على حل hostname api.amp.sourcefire.com.

للتحقق من المشكلة، قم بإجراء بحث على واجهة سطر الأوامر (CLI) الخاصة بمركز إدارة FireSIGHT. تحقق مما إذا تم تكوين إعدادات DNS بشكل صحيح على مركز إدارة FireSIGHT:

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

ةرادإ زكرم يف فيضملا مسا لح DNS ىلع رذعتي امدنع يلاتلا جارخإلا ضرع متي 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
```

ةرادإ زكرم ىلع حيحص لكشب DNS لح مت اذإ جرخملا يلي اميف 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
```

الحل

- اذإ رذعت ىلع FireSIGHT Management Center لح مسا فيضملا، تنأف ةجاحب ىلإ ققحتلا نم ةحص تادادعإ DNS ىلع زكرم ةرادإلا.
- اذإ ناك زكرم ةرادإ FireSIGHT ارداق ىلع لح مسا فيضملا، هنكلو ريغ رداق ىلع لوصولا ىلإ api.amp.sourcefire.com نم للاخ رادج ةيامح، ققحتف نم دعاوق تادادعإو رادج ةيامحلا.

اذإ رذعت ىلع "زكرم ةرادإ FireSIGHT" لح مسا فيضملا، متي ءاشنإ ةيلمع ءانثأ لاصتالا ليجست ةلاسر أطخلا ةيلاتلا يف httpsd_error_log:

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

ىلع لاثملا ليبس ىلع ،يلاتلا لجسلا جارخإ حضوي "عافدلا زكرم" لشف يف لامكإ رمألا curl ىلإ 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/
```

أثناء عملية إنشاء الاتصال، إذا تم تسجيل الرسالة التالية في httpsd_error_log دون خطأ، فإنها تشير إلى أن مركز إدارة FireSIGHT قادر على حل اسم المضيف:

```
getCloudData completed
```

على سبيل المثال، يوضح الإخراج التالي أن مركز الإدارة يقوم بإكمال رمز curl إلى 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/
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).