تكامل البيئة السحابية الافتراضية الخاصة بالحماية المتقدمة وشبكة التهديدات

المحتويات

المقدمة

يصف هذا المستند إجراء إكمال تكامل الشبكة الخاصة الظاهرية للحماية المتقدمة من البرامج الضارة (AMP) وجهاز شبكة الحماية من التهديدات. كما يوفر المستند خطوات استكشاف المشكلات المتعلقة بعملية التكامل وإصلاحها.

تمت المساهمة بواسطة أرمادن غارسيا، مهندس TAC من Cisco.

المتطلبات الأساسية
المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- العمل على شبكة AMP الخاصة الافتراضية وتشغيلها
- العمل وتشغيل شبكة تهديدات الحماية

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

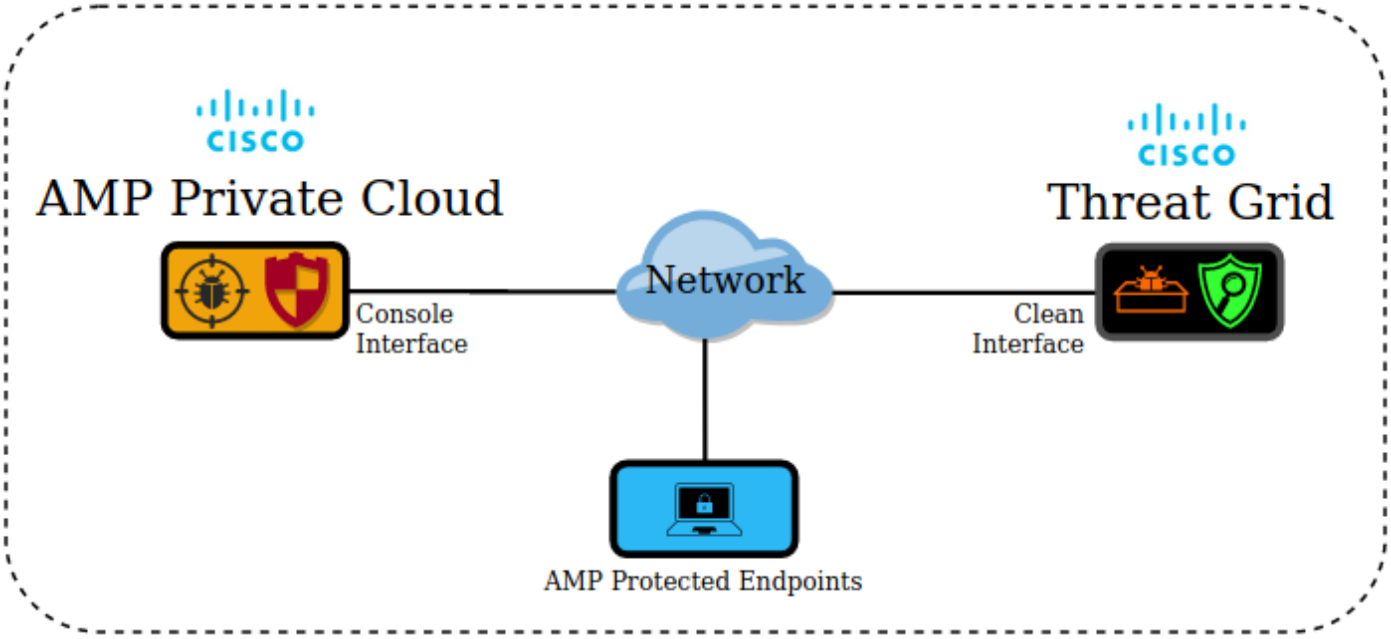
- AMP Private Cloud، الإصدار 3.2.0
- جهاز شبكة التهديدات 2.12.0.1

ملاحظة: تكون الوثائق صالحة لأجهزة شبكة التهديدات وأجهزة شبكة AMP الخاصة في الجهاز أو الإصدار الظاهري.

. (). .

معلومات أساسية

بنية التكامل



معلومات أساسية حول التكامل

- يحلل جهاز "شبكة التهديدات" العينات التي تم إرسالها بواسطة جهاز سحابة AMP الخاص.
- يمكن إرسال النماذج يدويا أو تلقائيا إلى جهاز شبكة التهديد.
- لا يتم تمكين التحليل التلقائي بشكل افتراضي في جهاز سحابة AMP الخاصة.
- يوفر جهاز شبكة التهديدات لجهاز سحابة AMP الخاص تقريرا ودرجة من تحليل العينة.

- وأ ديزت ةنيع يأ نع "ةكبش" زاهج مالعإب (poke) "ةيامحلا ةكبش" AMP الخاصة زاهج موقي ةجرد 95 يواست.
- إذا كانت النتيجة من التحليل أكبر من 95 وأ 95 يواست، يتم وضع علامة على العينة المأخوذة من بيانات AMP باللصق في الأشياء الضارة الموجودة في قاعدة بيانات AMP Private Cloud على العينات التي تحتوي على علامة أكبر من أو تساوي 95.

عارجإلا

الخطوة 1. قم بإعداد زاهج شبكة التحديثات والتكوين (لا يوجد دعم فني). تحقق من وجود رمز الأمان، إذا لزم الأمر، تثبيت وتحديث.

الخطوة 2. قم بإعداد وتكوين AMP للسحابة الخاصة بنقاط النهاية (لا يوجد دعم فني).

الخطوة 3. في واجهة مستخدم إدارة شبكة التحديثات، حدد علامة التبويب **التكوين** واختر **SSL**.

الخطوة 4. قم بتحميل شهادة SSL جديدة للواجهة النظيفة (PANDEM) وأنشئ أو

إعادة إنشاء شهادات SSL

يمكن إنشاء شهادة موقعة ذاتيا جديدة إذا لم يتطابق اسم المضيف للواجهة النظيفة مع الاسم البديل للموضوع (SAN) في الشهادة المثبتة حاليا في جهاز الواجهة النظيفة. يولد الجهاز شهادة جديدة للواجهة، مما يشكل اسم مضيف الواجهة الحالي في حقل SAN لشهادة التوقيع الذاتي.

الخطوة 4.1. من عمود الإجراءات حدد **(..)** ومن القائمة المنبثقة حدد **إنشاء شهادة جديدة**.

الخطوة 4.2. في واجهة مستخدم شبكة التهديد، حدد **عمليات**، في الشاشة التالية حدد **تنشيط** واختر **إعادة التكوين**.

ملاحظة: هذه الشهادة المنشأة موقعة ذاتيا.

تحميل شهادات SSL

في حالة وجود شهادة تم إنشاؤها بالفعل لواجهة تنظيف زاهج "شبكة التحديثات"، يمكن تحميل هذه الشهادة إلى الزاهج.

الخطوة 4.1. من عمود الإجراءات حدد **(..)** ومن القائمة المنبثقة حدد **تحميل شهادة جديدة**.

الخطوة 4.2. انسخ الشهادة والمفتاح الخاص المرادف بتنسيق PEM في مربعات النص التي تظهر على الشاشة وحدد **إضافة شهادة**.

الخطوة 4.3. في واجهة مستخدم شبكة التحديث، حدد **العمليات**، في الشاشة التالية حدد **إعادة التكوين** واختر **تنشيط**.

الخطوة 5. في واجهة مستخدم AMP Private Cloud Device Admin، حدد **إدارة الحساب** واختر **شبكة التحديثات**.

الخطوة 6. في تفاصيل تكوين شبكة التحديث، حدد **تحرير**.

الخطوة 7. في اسم المضيف لشبكة التهديدات، أدخل FQDN الخاص باواجهة النظيفة لجهاز شبكة التهديدات.

الخطوة 8. في شهادة SSL لشبكة التهديدات، أضف شهادة الواجهة النظيفة لجهاز شبكة التهديدات. (انظر الملاحظات أدناه)

الشهادة الموجودة في الواجهة النظيفة لجهاز شبكة التهديدات موقعة ذاتيا

الخطوة 8.1. في واجهة مستخدم "إدارة شبكة التهديدات"، حدد **التكوين واختر** SSL.

الخطوة 8.2. من عمود الإجراءات حدد **(..)** ومن القائمة المنبثقة حدد **تنزيل الشهادة**.

الخطوة 8.3. قم بالمتابعة لإضافة الملف الذي تم تنزيله إلى الجهاز الخاص الظاهري من AMP في صفحة تكامل شبكة التهديدات.

يتم توقيع الشهادة الموجودة في الواجهة النظيفة لجهاز شبكة التهديدات من قبل مرجع مصدق مؤسسي (CA)

الخطوة 8.1. انسخ في ملف نصي شهادة الواجهة النظيفة لجهاز شبكة الحماية وسلسلة شهادات CA الكاملة.

ملاحظة: يجب أن تكون الشهادات الموجودة في الملف النصي بتنسيق PEM.

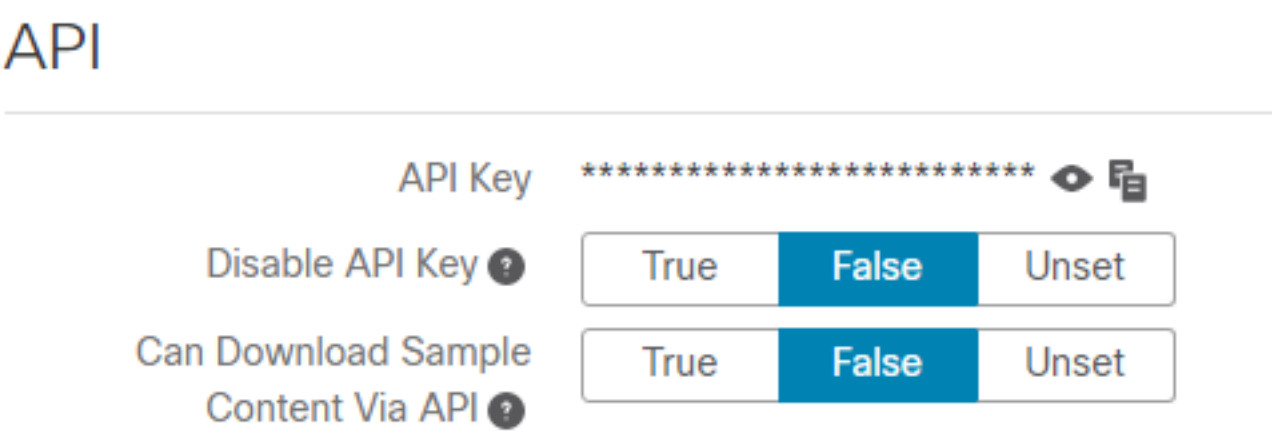
إذا كانت سلسلة الشهادات كاملة هي: شهادة ROOT_CA > شهادة THREAT_GRID_CLEAN_INTERFACE؛ في الملف النصي، كما هو موضح في الصورة.

```
-----BEGIN CERTIFICATE-----
Threat_Grid_Clean_Interface certificate PEM data
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
ROOT_CA certificate PEM data
-----END CERTIFICATE-----
```

إذا كانت سلسلة الشهادات كاملة هي: شهادة ROOT_CA > شهادة Sub_CA > شهادة THREAT_GRID_CLEAN_INTERFACE؛ في الملف النصي، كما هو موضح في الصورة.

```
-----BEGIN CERTIFICATE-----
Threat_Grid_Clean_Interface certificate PEM data
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sub_CA certificate PEM data
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
ROOT_CA certificate PEM data
-----END CERTIFICATE-----
```

9. (API) API .



ملاحظة: في إعدادات الحساب من شبكة التهديدات، يؤكد المستخدم أن المعلمة **Disable API Key** غير معينة إلى True.

الخطوة 10. بعد اكتمال كافة التغييرات، حدد **حفظ**.

الخطوة 11. تطبيق عملية إعادة تكوين على جهاز السحابة الظاهري من AMP.

الخطوة 12. من واجهة مستخدم جهاز سحابة AMP الخاص، حدد **عمليات التكامل** واختر **شبكة التهديدات**.

الخطوة 13. من **التفاصيل** انسخ قيم عنوان URL لخدمة تحديث المصير النهائي، ومستخدم خدمة تحديث المصير النهائي، وكلمة مرور خدمة تحديث المصير النهائي. يتم إستخدام هذه المعلومات في الخطوة 17.

الخطوة 14. في واجهة مستخدم إدارة شبكة التهديد، حدد **تكوين** واختر **شهادات CA**.

الخطوة 15. حدد **إضافة شهادة** ونسخ بتنسيق PEM شهادة CA التي وقعت على شهادة خدمة

تحديث المصير النهائي للسحابة الخاصة ل AMP.

> **ملاحظة**: إذا كانت شهادة AMP التي وقعت على شهادة تحديث الترتيب السحابي الخاص ل CA هي شهادة CA مرجع مصدق فرعي، فكرر العملية حتى يتم تحميل جميع الشهادات المصدقة في السلسلة إلى **شهادات**.

الخطوة 16. في مدخل شبكة التهديدات، حدد إدارة وحدد إدارة تكامل سحابة AMP الخاصة.

الخطوة 17. في صفحة "خدمة مشاركة تحديث المصير النهائي"، أدخل المعلومات التي تم تجميعها في الخطوة 13

- URL الخاص باالخدمة: FQDN الخاص بخدمة تحديث المصير النهائي لجهاز السحابة الخاص ل AMP.
- المستخدم: المستخدم من خدمة تحديث المصير النهائي لجهاز السحابة الخاص ل AMP.
- كلمة المرور: كلمة مرور لخدمة تحديث المصير النهائي لجهاز سحابة AMP الخاص.

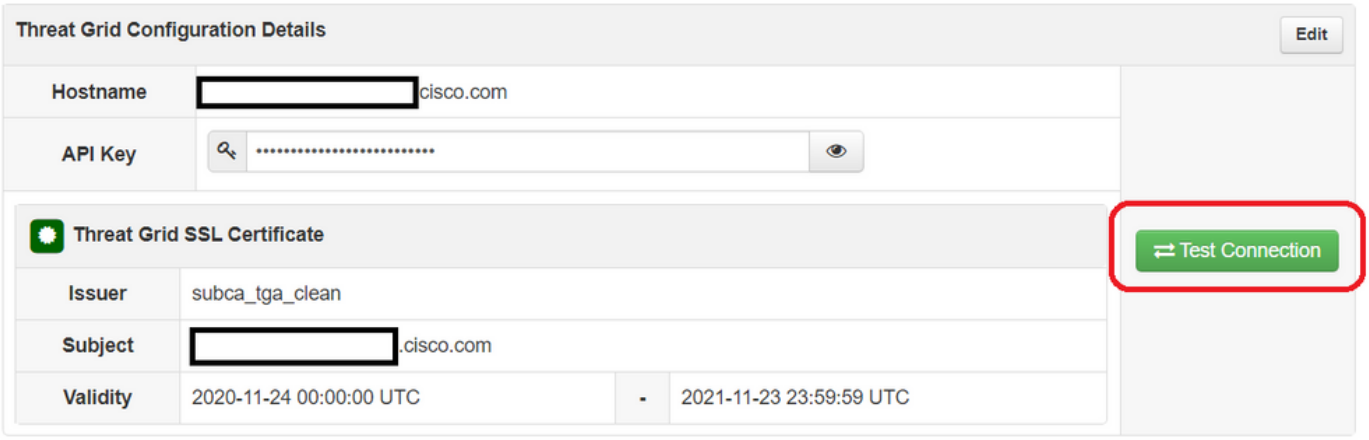
في هذه المرحلة، إذا تم تطبيق جميع الخطوات بشكل صحيح، يجب أن يعمل التكامل بنجاح.

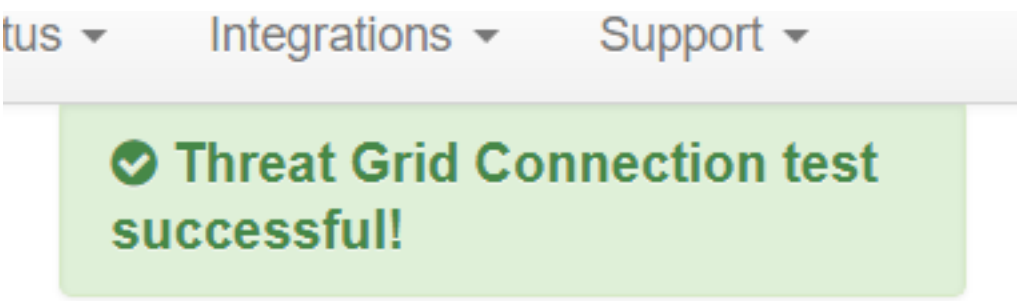
التحقق

" " .

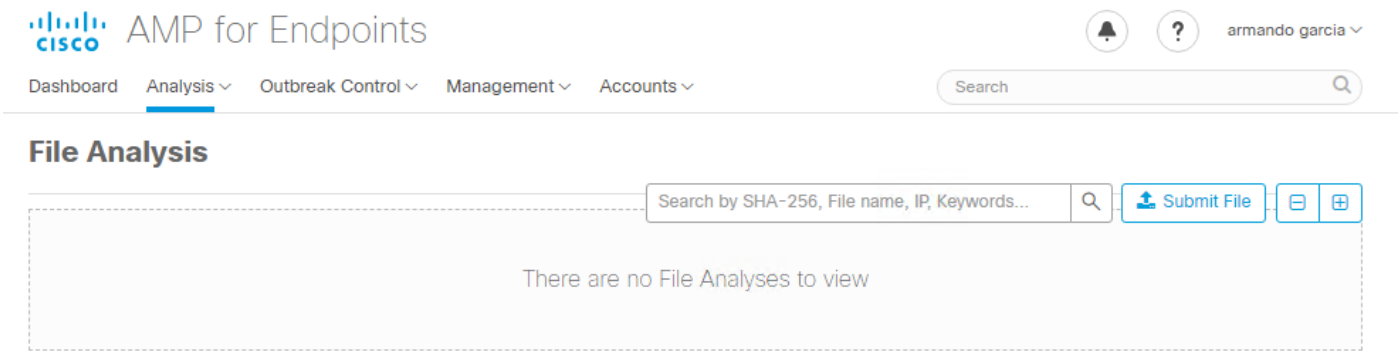
> **ملاحظة**: تكون الخطوات 1 و 2 و 3 و 4 طفق منانسبة للتطبيق في بيئة إنتاج الو لل لتحقق من التكامل. يتم توفير الخطوة 5 كمعلومات لمعرفة المزيد حول التكامل وما ينصح بتطبيقها في بيئة إنتاج.

1. AMP Private Cloud Device Admin UI > > Threat Grid ! .

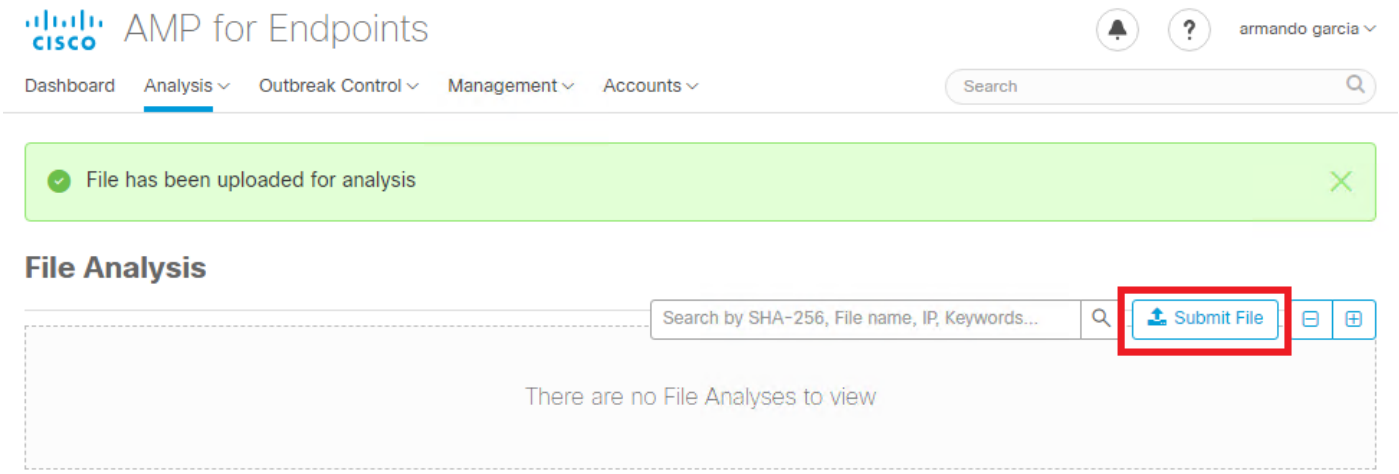


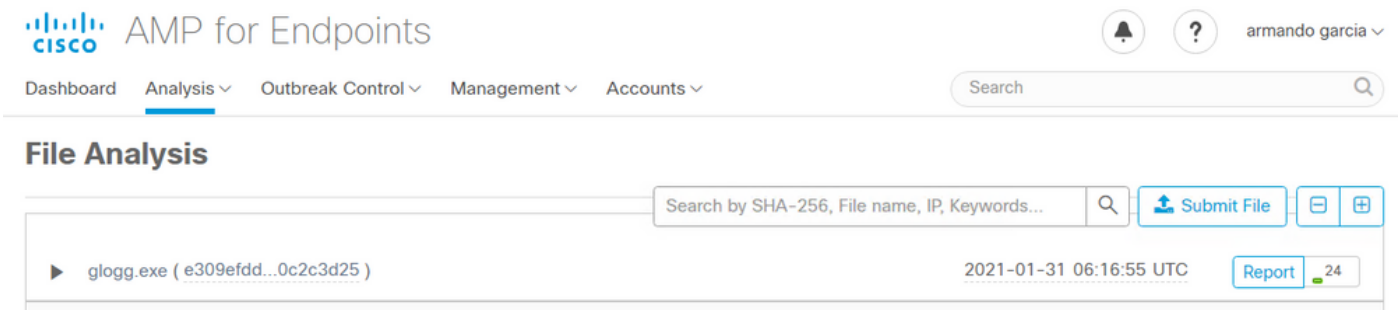


2. AMP .



الخطوة 3. تأكد من إدراك الملفات التي يتم إرسالها يدويا من **تحليل** وحدة تحكم السحابة الخاصة ل AMP > **تحليل الملفات** في جهاز "شبكة التهديدات"، ومن إرجاع تقرير بنقطة واحدة بواسطة جهاز "شبكة التهديدات".





الخطوة 4. تأكد من تثبيت الشهادات المصدقة (CAs) الموقعة على شهادة خدمة تحديث المصير النهائي الخاصة بجهاز السحابة الخاص ل AMP في جهاز شبكة التهديدات في **جهات الترخيص**.

الخطوة 5. تأكد من أن أي عينة تم وضع علامة عليها بواسطة جهاز شبكة التهديد مع علامة >=95 يتم تسجيلها في قاعدة بيانات سحابة AMP الخاصة مع التعامل مع أية آثار ضارة بعد تقديم التقرير وعينة نقاط بواسطة جهاز شبكة التهديد.

ملاحظة: لا يعني تلقي التقرير النموذجي بنجاح وتسجيل <=95 عينة في وحدة تحكم السحابة الخاصة **من** AMP علامة التبويب **تحليل الملف** بالضرورة أنه تم تغييرها

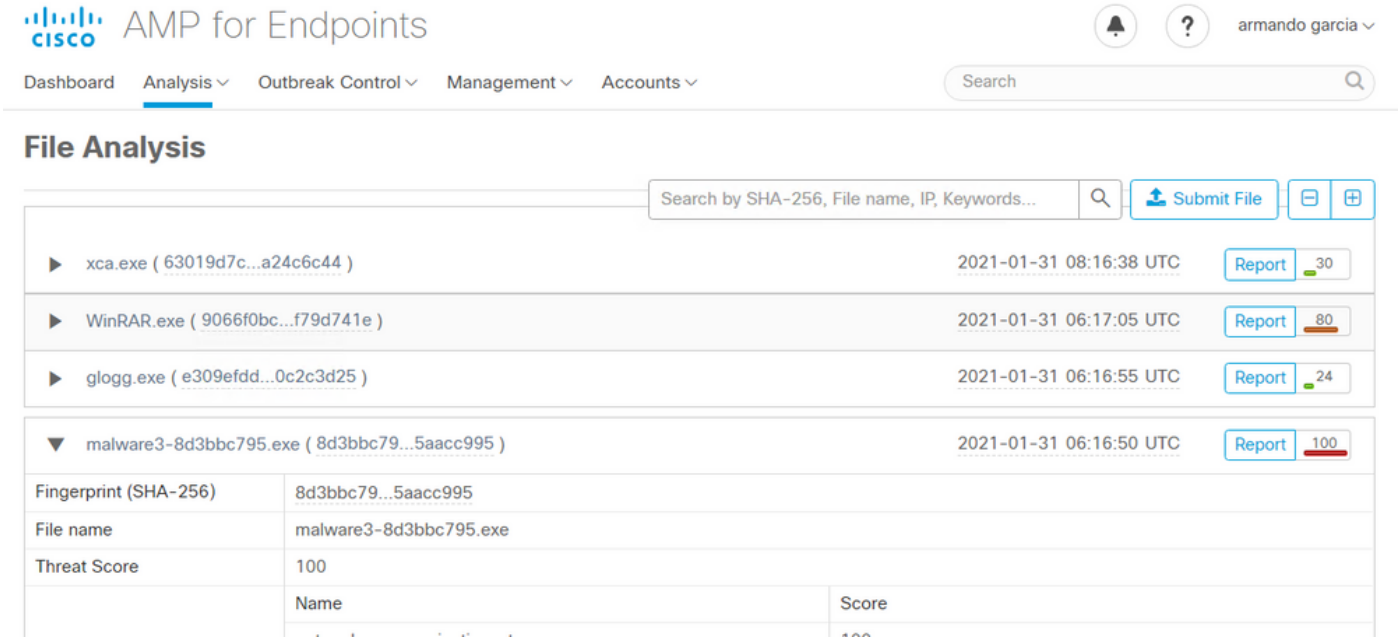
المصير النهائي للملف في قاعدة بيانات AMP. إذا لم يتم تثبيت CAs التي وقعت على شهادة خدمة تحديث المصير النهائي الخاصة بجهاز السحابة الخاص AMP في جهاز شبكة التهديدات في **هيئات الشهادات**، يتم تلقي التقارير والعينات بواسطة جهاز السحابة الخاص ل AMP، ولكن لا يتم تلقي أي رسائل من جهاز شبكة التهديدات.

تحذير: تم إكمال الاختبار التالي لتشغيل تغيير المصير النهائي للعينة في قاعدة بيانات AMP بعد أن قام جهاز Threat Grid بوضع علامة على ملف ذو علامة >=95. كان الغرض من هذا الاختبار توفير معلومات حول العمليات الداخلية في جهاز سحابة AMP الخاص عندما يوفر جهاز شبكة التهديدات عينة من >=95. لتشغيل عملية تغيير المصير النهائي، تم إنشاء ملف إختبار محاكاة البرامج الضارة باستخدام تطبيق Cisco الداخلي McWare.exe. عينة: خضار 3-419d23483.exeSHA256: 8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995.

تحذير: لا ينصح بتفجير أي ملف إختبار محاكاة برامج ضارة في بيئة إنتاج.

تأكيد تحديث المصير النهائي للعينة في قاعدة بيانات سحابة AMP الخاصة

" " AMP. 100 AMP Private Cloud Device Threat Grid. >=95 AMP . AMP >=95 .



إذا:

- تم إكمال التكامل بنجاح.
- يتم عرض نماذج التقارير والعينات في **تحليل الملفات** بعد إرسال الملفات يدويا.

ثم:

- لكل عينة يشير إليها جهاز شبكة الحماية بدرجة >=95، تتم إضافة إدخال إلى الملف /data/poked/poked.log في جهاز شبكة AMP الخاصة.
- يتم إنشاء الصفحة /data/poked/poked.log في جهاز الشبكة الخاصة بالحماية المتقدمة بعد أول علامة >=95 عينة يقدمها جهاز شبكة الحماية.
- تحمل قاعدة بيانات db_protect الموجودة في سحابة AMP الخاصة المصير النهائي الحالي للعينة. يمكن إستخدام هذه المعلومات للتأكد مما إذا كانت العينة تحتوي على

المصير النهائي على 3 بعد أن قام جهاز "شبكة التهديدات" بتوفير النتيجة.
إذا تم عرض تقرير النموذج ودرجة >=95 في **تحليل الملف** في وحدة تحكم السحابة الخاصة ل AMP، فقم بتطبيق الخطوات التالية:

الخطوة 1. سجل الدخول عبر SSH إلى جهاز سحابة AMP الخاص.

الخطوة 2. تأكد من وجود إدخال في /data/poked/poked.log للعينة.

تظهر قائمة الدليل /data/poked/ في جهاز سحابة AMP خاص الذي لم يستلم أبدا علامة >=95 عينة من جهاز شبكة تهديدات أن ملف poked.log لم يتم إنشاؤه في النظام.

إذا لم يستلم جهاز سحابة AMP الخاصة أي مكدس من جهاز شبكة تهديدات، فلن يتم العثور على ملف /data/poked/poked.log في الدليل، كما هو موضح في الصورة.

```
[root@fireamp ~]# ls /data/poked/
poked_error.log
[root@fireamp ~]#
```

تظهر قائمة الدليل /data/poked/ بعد إستلام أول علامة >=95، الملف الذي تم إنشاؤه.

بعد إستلام العينة الأولى بدرجة >=95.

```
[root@fireamp ~]# ls /data/poked/
poked_error.log  poked.log
[root@fireamp ~]#
[root@fireamp ~]# cat /data/poked/poked.log
Jan 30 18:25:18 fireamp poked[9557]: [9557]  info @0.004940 127.0.0.1 --
{"disposition":"malicious","force":0,"state":"local","name":"W32.8D3BBC795B-100.SBX.TG","ok":1,"time":1612031118,"hash":"8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995","engine":"sha256"
,"user":"-","mode":"tg","score":100}
[root@fireamp ~]#
```

عينة معلومة من الأداة يزود ب ال تهديد شبكة يمكن أن يفهم داخل ال poked.log مبرد.

الخطوة 3. **قم بتشغيل** هذا الأمر باستخدام نموذج SHA256 لاسترداد المصير النهائي الحالي من قاعدة بيانات جهاز سحابة AMP الخاص.

```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

مثال

ال يوفر استعلام قاعدة بيانات للحصول على المصير النهائي للعينة قبل تحميل العينة إلى "جهاز شبكة التهديدات" أية نتائج كما هو موضح في الصورة.

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
[root@fireamp ~]#
```

يظهر استعلام قاعدة بيانات للحصول على المصير النهائي للعينة بعد إستلام التقرير والعلامة من جهاز شبكة التهديدات، العينة التي لها المصير النهائي 3 والتي تعتبر ضارة.

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
+------------------------------------------------------------------+---------------+
| hex(fingerprint)                                                 | disposition_id |
+------------------------------------------------------------------+---------------+
| 8D3BBC795BB47447984BF2842D3A0119BAC0D79A15A59686951E1F7C5AACC995 |             3 |
+------------------------------------------------------------------+---------------+
[root@fireamp ~]#
```

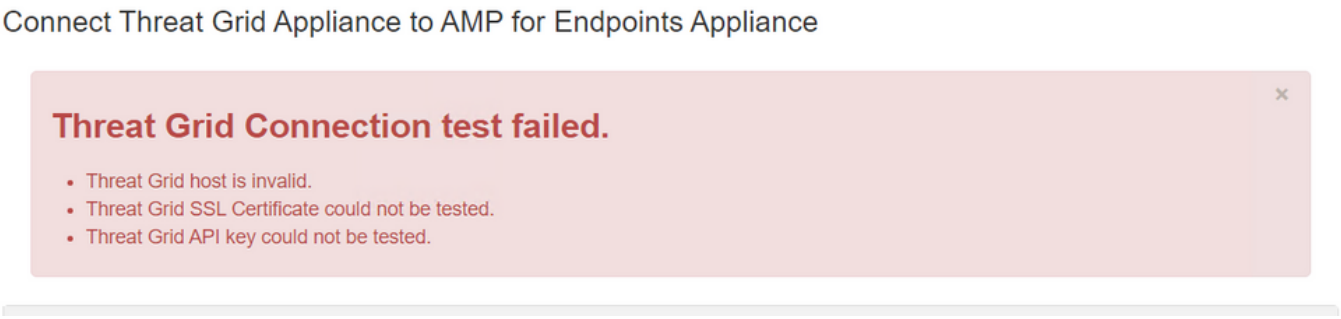
استكشاف الأخطاء وإصلاحها

وفي عملية التكامل، يمكن النظر إلى القضايا المحتملة. وفي هذه الجزء من الوثيقة، يجري تناول بعض أكثر المسائل شيوعا.

تحذير في جهاز السحابة الخاص ل AMP حول المضيف غير صالح، لم يتم إختبار الشهادة، لم يتم إختبار مفتاح API

عرض

رسالة التحذير: مضيف شبكة التهديدات غير صالح، تعذر إختبار شهادة SSL لشبكة التهديدات، تعذر إختبار مفتاح API لشبكة التهديدات، تم إستلامه في جهاز شبكة AMP الخاصة بعد تحديد **زر إختبار الاتصال** في **عمليات التكامل > شبكة التهديدات**.



هناك مشكلة على مستوى الشبكة في التكامل.

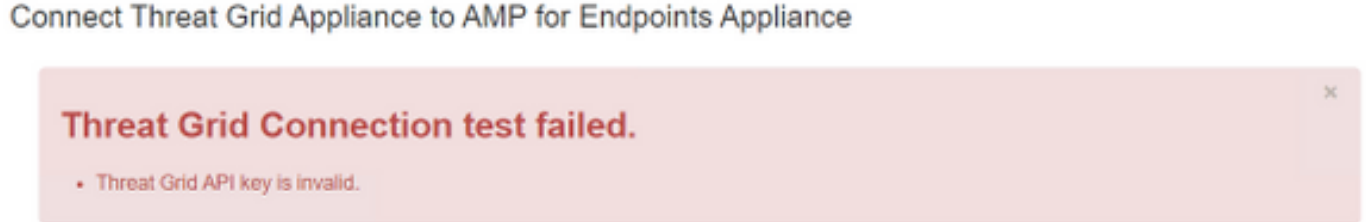
الخطوات الموصى بها:

- تأكيد إمكانية وصول واجهة وحدة تحكم جهاز السحابة الخاص ل AMP إلى الواجهة النظيفة لجهاز شبكة التهديدات.
- تأكيد أن جهاز سحابة AMP الخاص يمكنه حل FQDN الخاص بواجهة تنظيف جهاز شبكة التهديدات.
- تأكد من عدم وجود جهاز تصفية في مسار الشبكة لجهاز سحابة AMP الخاص وجهاز شبكة التهديدات.

AMP API

عرض

رسالة التحذير: فشل إختبار اتصال شبكة التهديدات، API الخاص بشبكة التهديدات غير صالح، يتم إستلامه في جهاز سحابة AMP الخاص بعد تحديد زر **إختبار الاتصال** في **عمليات التكامل > شبكة التهديدات**.

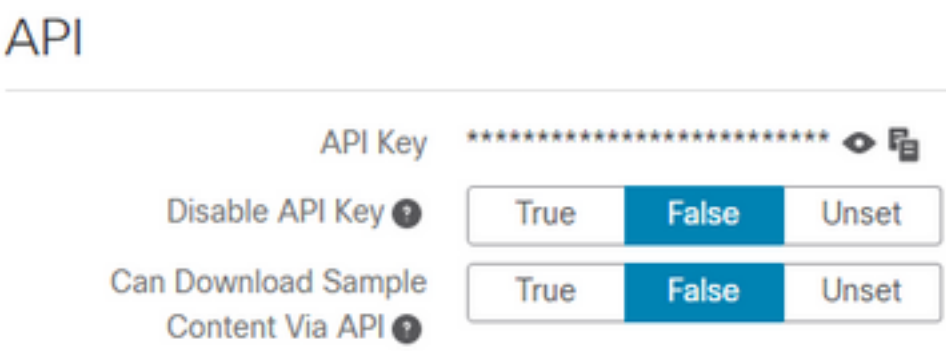


API AMP .

الخطوات الموصى بها:

- تأكيد في إعدادات الحساب الخاصة بمستخدم جهاز شبكة التهديدات، لم يتم تعيين

المعلمة Disable API Key إلى True.
- يجب تعيين المعلمة Disable API Key على: false أو unset.



- تأكيد مفتاح API لشبكة التهديدات الذي تم تكوينه في **عملياتك المالية** بوابة إدارة سحابة AMP الخاصة > **شبكة التهديدات**، وهو نفس مفتاح API في إعدادات المستخدم في جهاز شبكة التهديدات.
- تأكيد ما إذا كان يتم حفظ مفتاح واجهة برمجة التطبيقات (API) لشبكة التهديدات الصحيحة في قاعدة بيانات جهاز سحابة AMP الخاص.

من سطر أوامر جهاز سحابة AMP الخاص، يمكن تأكيد مفتاح API لشبكة التهديدات الحالية الذي تم تكوينه في جهاز AMP. قم بتسجيل الدخول إلى جهاز الشبكة الخاص لـ AMP عبر SSH وقم بتشغيل هذا الأمر لاسترداد مفتاح API لمستخدم شبكة التهديدات الحالية:

```
mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
```

هذا إدخال صحيح في قاعدة البيانات الخاصة بجهاز سحابة AMP الخاص لمفتاح واجهة برمجة التطبيقات (API) لجهاز شبكة التهديدات.

```
[root@fireamp ~]#  mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
+--------------------------+----------------------+----------------------+
| tg_api_key               | tg_login             | api_client_id        |
+--------------------------+----------------------+----------------------+
| mirt1if[redacted]nnjae7 | argarci2_samples-user | de4c23c64d3e36034bb7 |
+--------------------------+----------------------+----------------------+
[root@fireamp ~]#
```

على الرغم من أن اسم مستخدم شبكة التهديد لم يتم تكوينه مباشرة في جهاز السحابة الخاصة لـ AMP في أي خطوة من التكامل، إلا أن اسم مستخدم شبكة التهديدات يتم إدراكه في المعلمة tg_login في قاعدة بيانات AMP إذا تم تطبيق مفتاح API لشبكة التهديدات بشكل صحيح.

هذا إدخال خاطئ في قاعدة بيانات AMP لمفتاح واجهة برمجة التطبيقات (API) لشبكة التهديدات.

```
[root@fireamp ~]# mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
+-------------------------+----------+----------------------+
| tg_api_key              | tg_login | api_client_id        |
+-------------------------+----------+----------------------+
| thisisanwrongapikey     | NULL     | de4c23c64d3e36034bb7 |
+-------------------------+----------+----------------------+
[root@fireamp ~]#
```

tg_login NULL. AMP .

يتم إستلام نماذج النتائج >=95 بواسطة جهاز الشبكة الخاص بالحماية المتقدمة (AMP)، ولكن لا يتم ملاحظة أي تغيير في المصير النهائي للعينة

عرض

يتم تلقي التقارير و >=95 عينة من العلامات بنجاح من جهاز "شبكة التهديدات" بعد إرسال عينة، ولكن لا يتم إدراك أي تغيير في المصير النهائي للعينة في جهاز شبكة AMP الخاصة.

الخطوات الموصى بها:

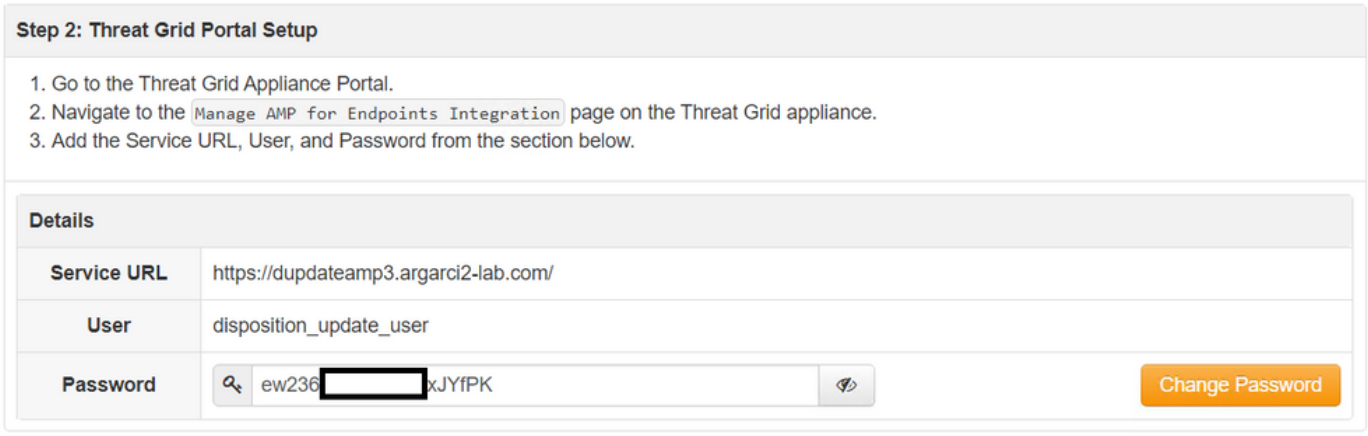
- تأكد في جهاز سحابة AMP الخاص إذا كانت العينة SHA256 في محتوى /data/poked/poked.log.

إذا تم العثور على SHA256 في /data/poked/poked.log، فقم بتشغيل هذا الأمر لتأكيد المصير النهائي للعينة الحالي في قاعدة بيانات AMP.

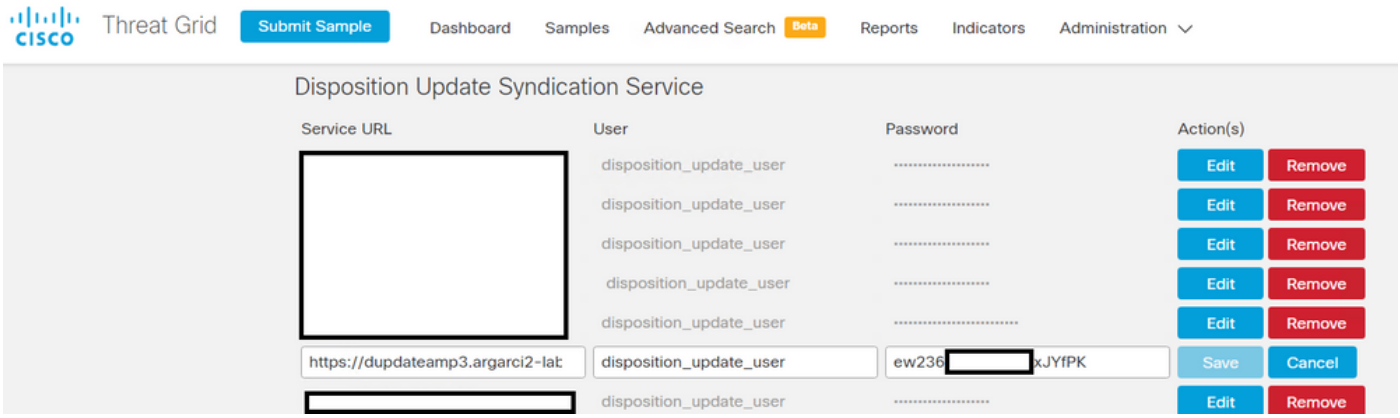
```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

- تأكد من إضافة كلمة مرور تكامل البيئة السحابية الخاصة ل AMP الصحيحة إلى مدخل إدارة جهاز شبكة التهديدات في **الإدارة > إدارة تكامل البيئة السحابية الخاصة ل AMP**.

بوابة إدارة سحابة AMP الخاصة.



بوابة وحدة التحكم في جهاز شبكة الحماية.

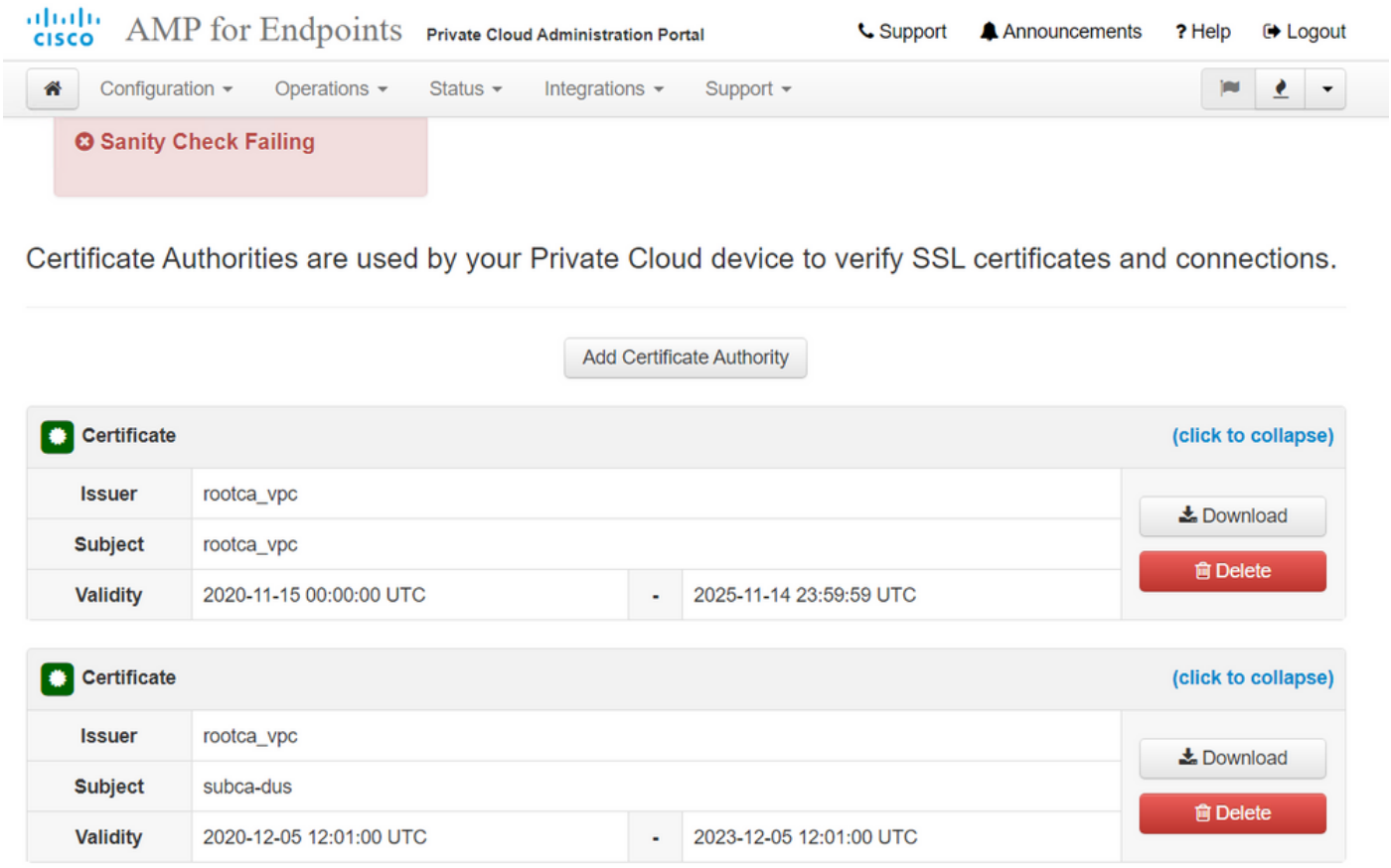


- تأكيد تثبيت الشهادات المصدقة (CAs) الموقعة على شهادة خدمة تحديث مصير أجهزة السحابة الخاصة من AMP في مدخل إدارة أجهزة شبكة التهديدات في **شهادات CA**.

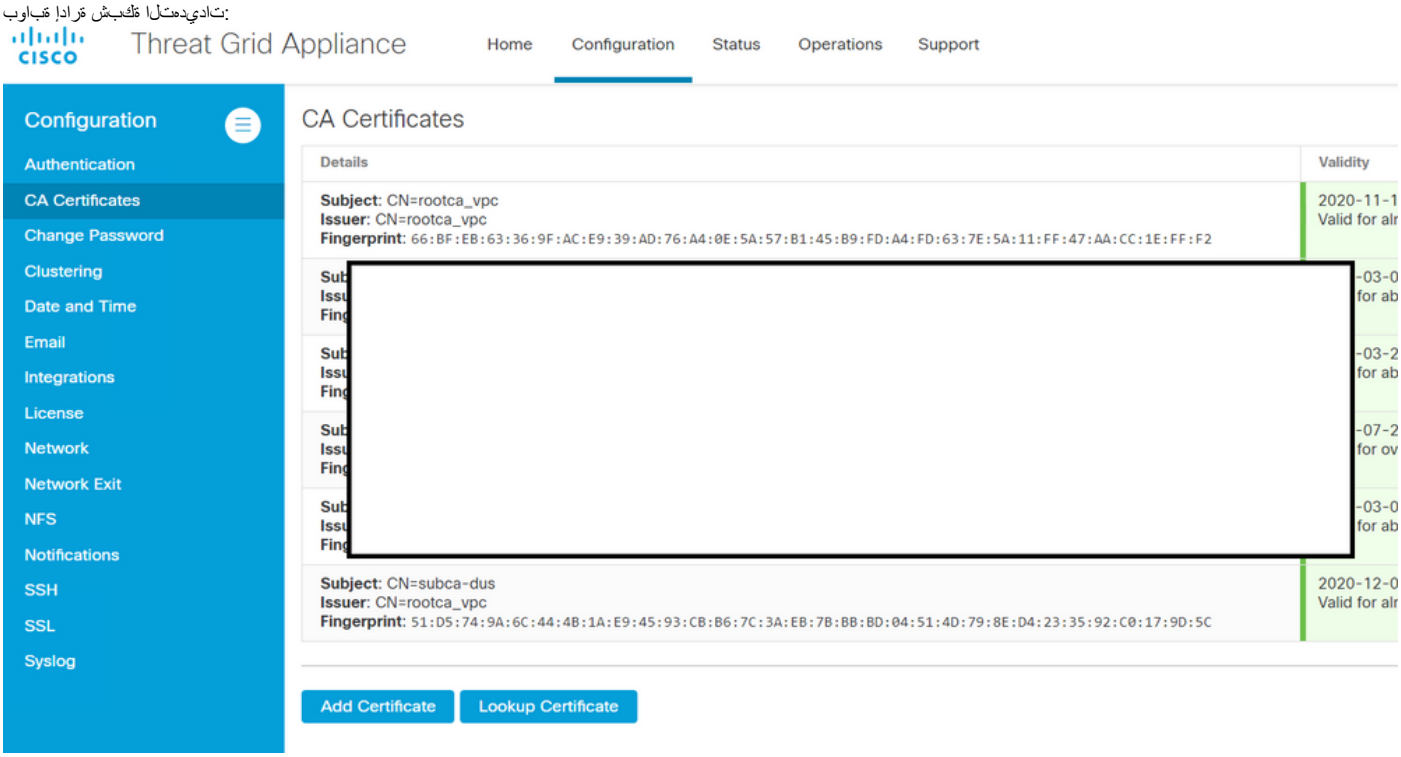
في المثال التالي، يجب تثبيت سلسلة الشهادات الخاصة بشهادة خدمة تحديث مصير الجهاز السحابي الخاص ل AMP على **ROOT_CA > Sub_CA > DISPOSITION_UPDATE_SERVICE**.

وبالتالي، يجب تثبيت RootCA و Sub_CA في **شهادات CA** في جهاز شبكة التهديد.

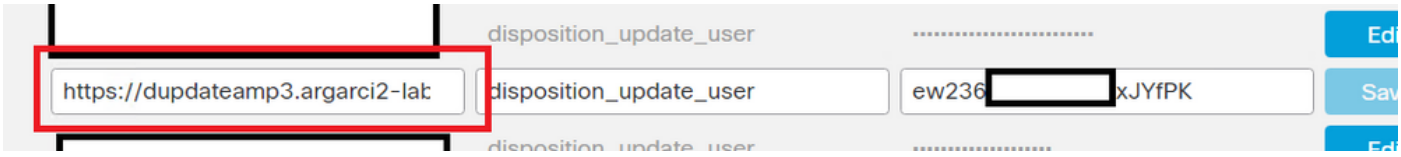
سلطات الشهادات في مدخل إدارة سحابة AMP الخاصة.



بوابة إدارة شبكة التهديدات:



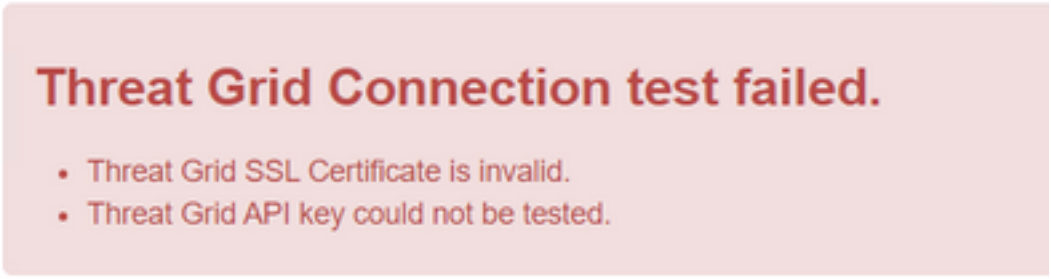
- AMP > **AMP**. IP AMP FQDN.



تحذير في جهاز السحابة الخاص ل AMP حول شهادة SSL لشبكة تهديدات غير صالحة

عرض

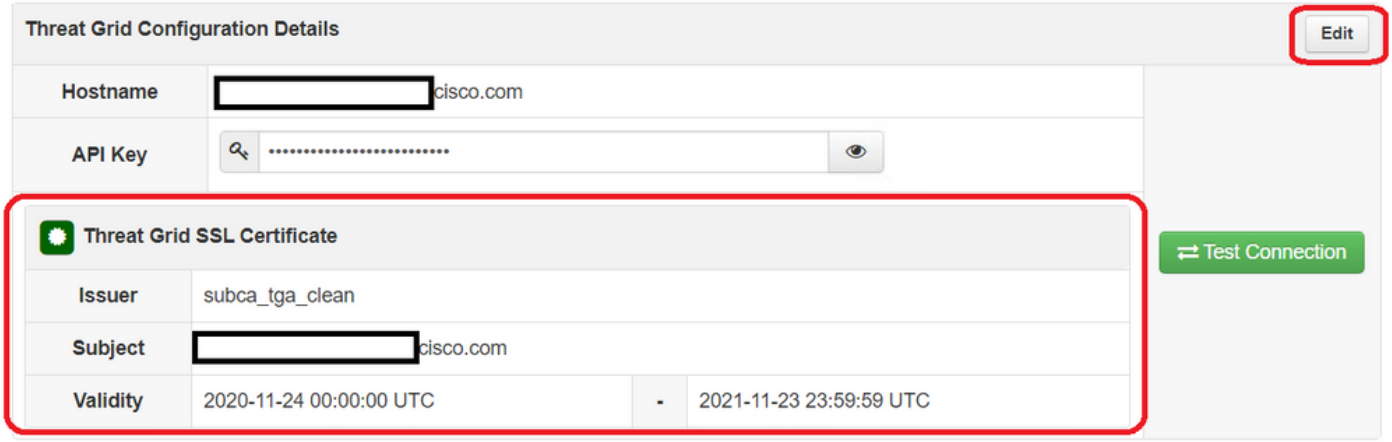
يتم تلقي رسالة التحذير: "شهادة SSL لشبكة التهديدات غير صالحة"، في جهاز السحابة الخاص ل AMP بعد تحديد زر **إختبار الاتصال** في **عمليات التكامل > شبكة التهديدات**.



الخطوات الموصى بها:

- تأكيد ما إذا كانت الشهادة المثبتة في واجهة Threat Grid التي تم توقيعها من قبل مرجع مصدق مؤسسي.

إذا تم توقيعها بواسطة CA، فيجب إضافة سلسلة الشهادات الكاملة داخل ملف إلى عمليات **تكامل** بوابة إدارة أجهزة سحابة AMP الخاصة > **شبكة التهديدات** في **شهادة SSL لشبكة التهديدات**.



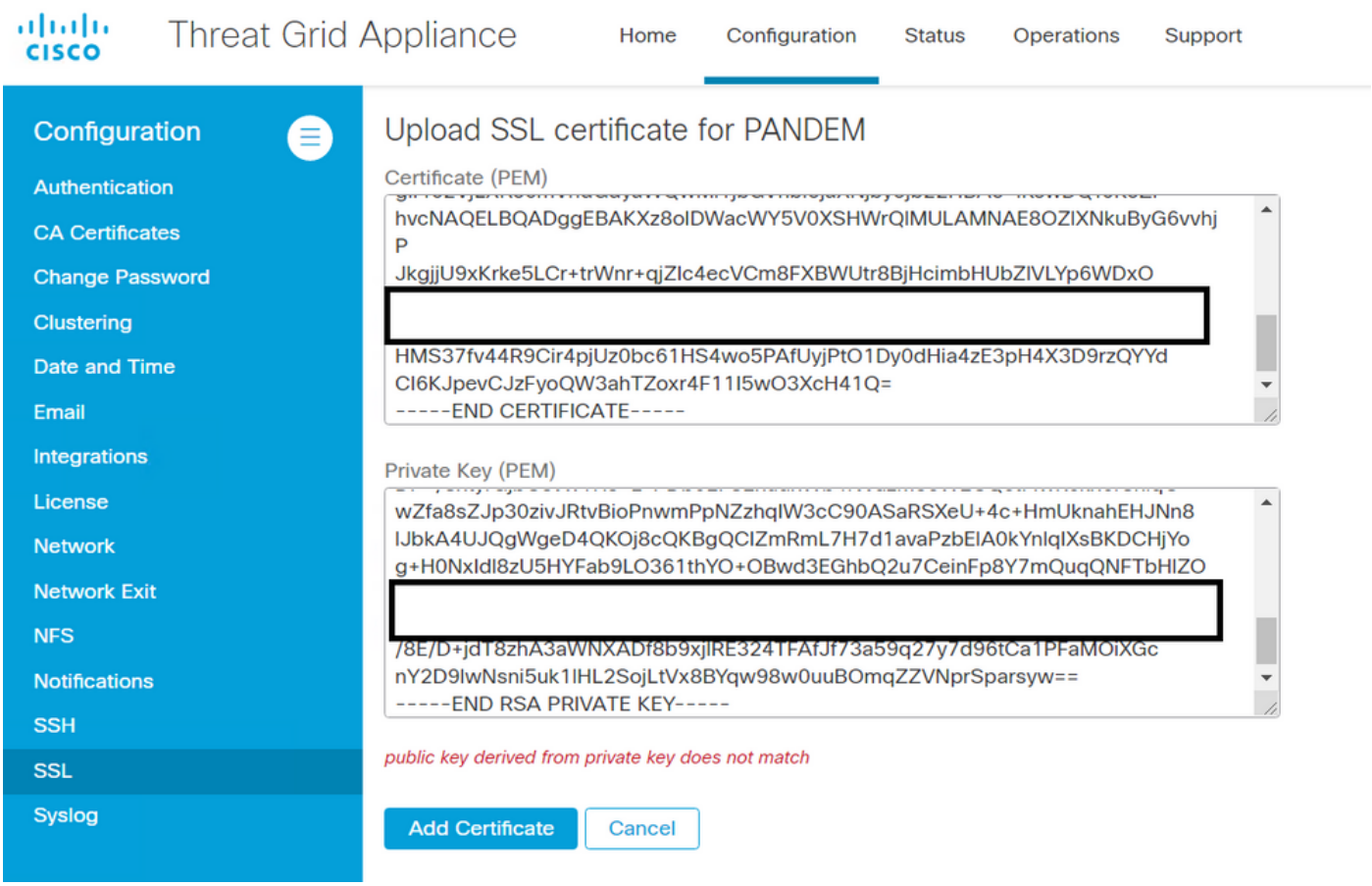
في جهاز AMP Private Cloud، يمكن العثور على شهادات جهاز شبكة الحماية المثبتة حاليا في: /opt/fire/etc/ssl/threat_grid.crt .

التحذيرات الموجودة في جهاز شبكة التهديد المتعلقة بالشهادات

رسالة تحذير - المفتاح العام المستمد من مفتاح خاص غير متطابق

عرض

رسالة التحذير: المفتاح العام المستمد من مفتاح خاص غير مطابق، يتم إستلامه في جهاز شبكة التهديد بعد محاولة إضافة شهادة إلى واجهة.



المفتاح العام المصدر من المفتاح الخاص لا يتطابق مع المفتاح العام المكون في الشهادة.

الخطوات الموصى بها:

- تأكيد ما إذا كان المفتاح الخاص يطابق المفتاح العام في الشهادة.

إذا كان المفتاح الخاص يطابق المفتاح العام في الشهادة، فيجب أن يكون المعامل والأس العام نفس الشيء. لذا التحليل، يكفي تأكيد ما إذا كان المعامل له نفس القيمة في المفتاح الخاص والمفتاح العام في الشهادة.

الخطوة 1. أستخدم أداة OpenSSL لمقارنة الوحدات النمطية في المفتاح الخاص والمفتاح العام الذي تم تكوينه في الشهادة.

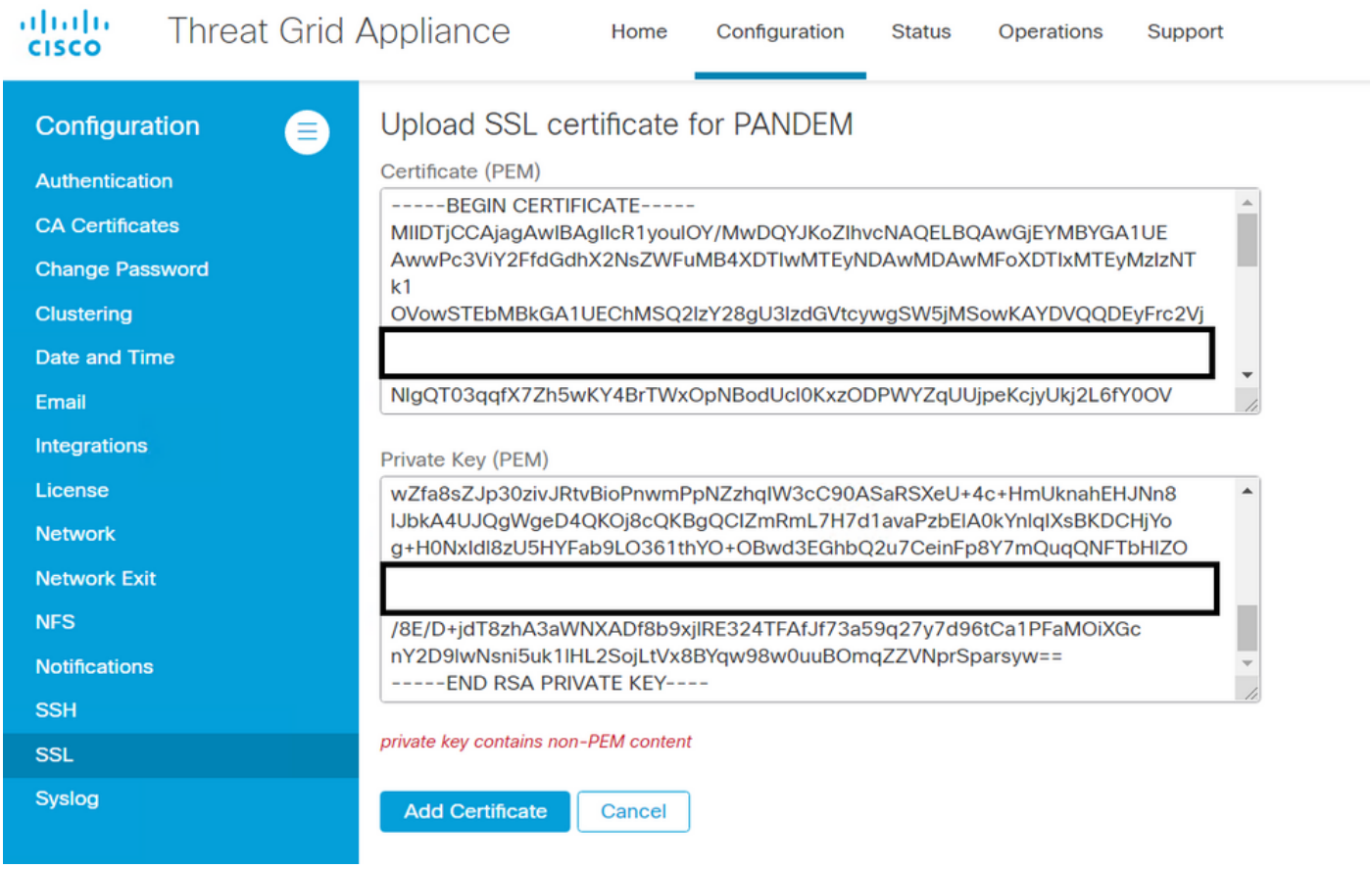
```
openssl x509 -noout -modulus -in
```
مثال. تطابق إجمالي المفتاح الخاص والمفتاح العام تم تكوينهما في الشهادة.

```
$ openssl x509 -noout -in certificate.cert | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
$
$
$ openssl rsa -noout -in private-key.key | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
```

رسالة تحذير - يحتوي المفتاح الخاص على محتوى غير PEM

عرض

رسالة التحذير: يحتوي المفتاح الخاص على محتوى غير PEM، ويتم إستالمه في جهاز شبكة التهديد بعد محاولة إضافة شهادة إلى واجهة.



بيانات PEM داخل ملف المفتاح الخاص تالفة.

الخطوات الموصى بها:

- .

الخطوة 1. أستخدم أداة OpenSSL للتحقق من سالمة المفتاح الخاص.

```
openssl rsa -check -noout -in
```

. PEM PEM.

```
$ openssl rsa -check -noout -in wrong-private-key.key
unable to load Private Key
140333463315776:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:


$ openssl rsa -check -noout -in correct-private-key.key
RSA key ok
```

إذا لم يكن إخراج الأمر OpenSSL هو **مفتاح RSA OK**، فهذا يعني أنه تم العثور على مشكل مع بيانات PEM داخل المفتاح.

إذا تم العثور على مشكل في الأمر OpenSSL، فعندئذ:

- تأكيد ما إذا كانت بيانات PEM داخل المفتاح الخاص مفقودة أم ال.

يتم عرض بيانات PEM داخل ملف المفتاح الخاص في الأسطر المكونة من 64 حرف. يمكن أن يظهر الفحص البصري السريع لبيانات PEM داخل الملف ما إذا كانت البيانات مفقودة. السطر ذو البيانات المفقودة ال تتم محاذاته مع الأسطر الأخرى في الملف.

- تأكيد أن السطر الأول في المفتاح الخاص يبدأ ب 5 واصلة، **وتبدأ** الكلمات **مفتاح خاص،** وينتهي ب 5 واصلة.

مثال.

—بدء المفتاح الخاص—

- تأكيد السطر الأخير في المفتاح الخاص يبدأ ب 5 واصلة، كلمات **إنهاء المفتاح الخاص،** وينتهي ب 5 واصلة.

مثال.

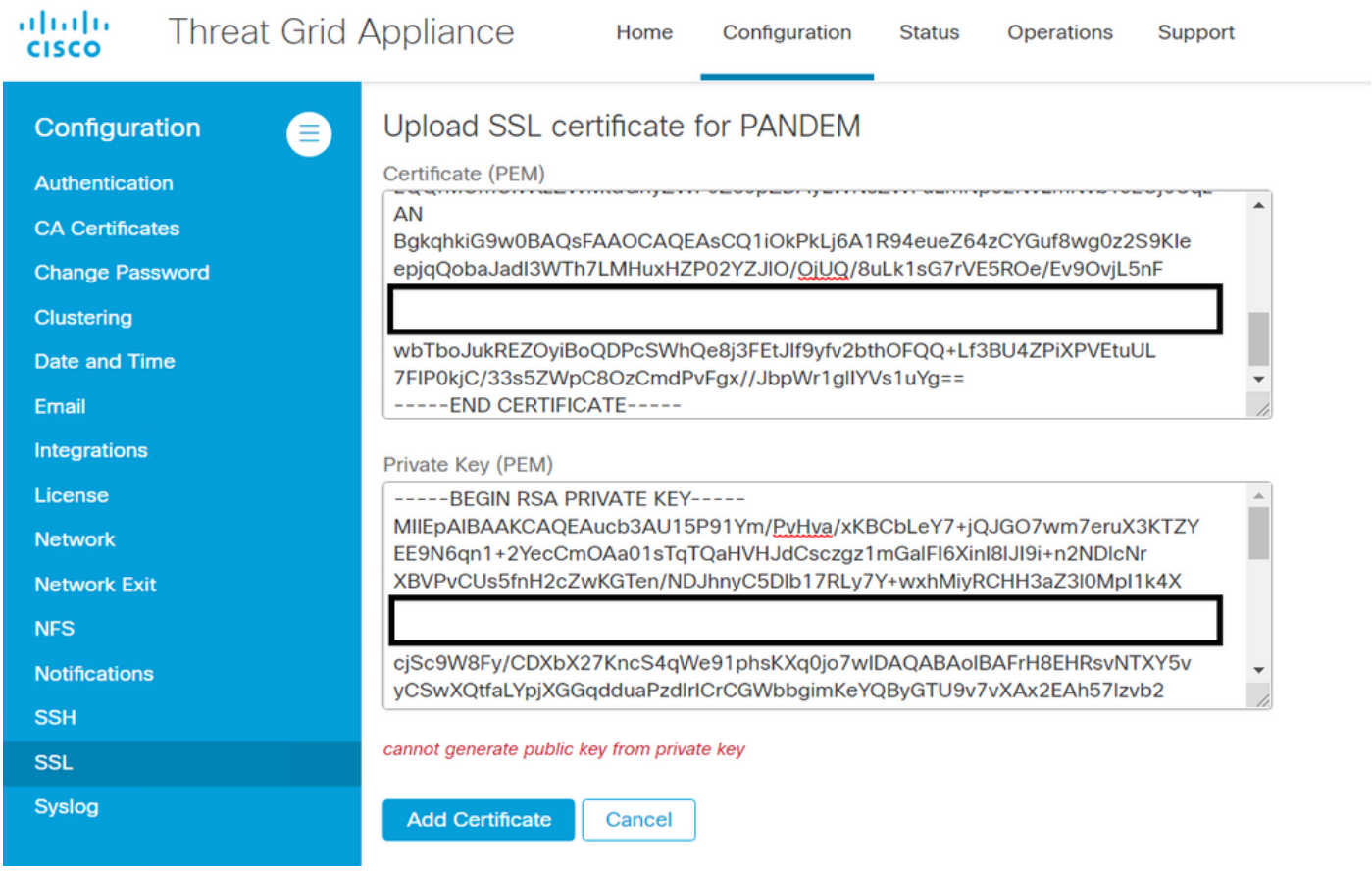
—مفتاح النهاية الخاص—

مثال. تصحيح تنسيق PEM والبيانات الموجودة داخل مفتاح خاص.

رسالة تحذير - لا يمكن إنشاء مفتاح عام من المفتاح الخاص

عرض

رسالة التحذير: لا يمكن إنشاء مفتاح عام من المفتاح الخاص، تم تلقيها في جهاز شبكة التهديد بعد محاولة إضافة شهادة إلى واجهة.



ال يمكن إنشاء المفاتيح العام من بيانات PEM الحالية داخل ملف المفاتيح الخاص.

الخطوات الموصى بها:

- .

1. OpenSSL .

```
openssl rsa -check -noout -in
```

إذا لم يكن إخراج الأمر OpenSSL هو **مفاتيح RSA OK**، فهذا يعني أنه تم العثور على مشكل مع بيانات PEM داخل المفاتيح.

الخطوة 2. أستخدم أداة OpenSSL للتحقق من إمكانية تصدير المفاتيح العام من المفاتيح الخاص.

```
openssl rsa -in
```

مثال. فشل تصدير المفاتيح العام وتصدير مفاتيح عام ناجح.

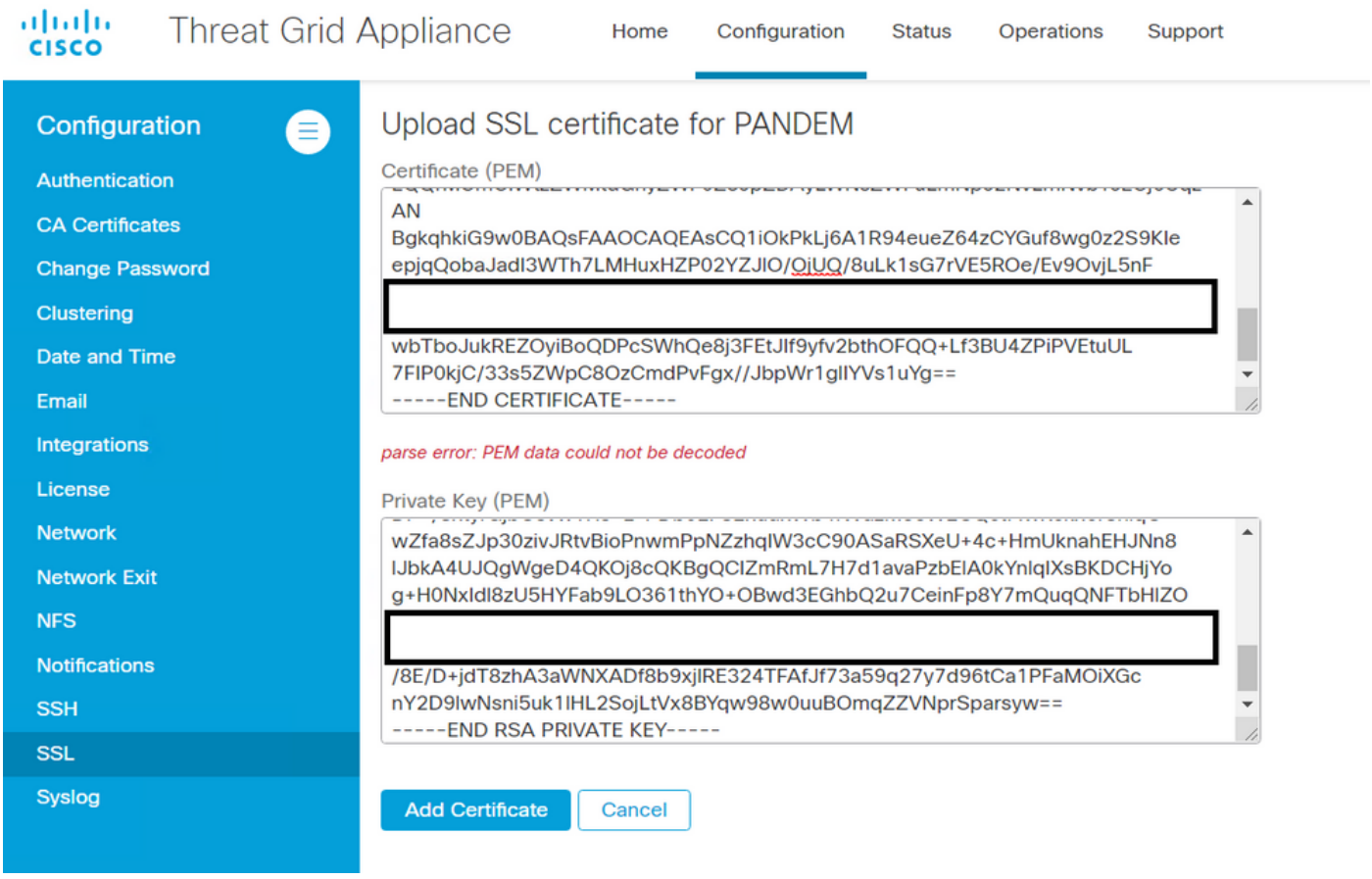
```
$ openssl rsa -in wrong-private-key.key -pubout
unable to load Private Key
140195161523520:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ openssl rsa -in correct-private-key.key -pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr3yMrcJH/VCHOQ5bivT0
2yrw60oYJ/Pwnp/cFxFAyATWoZRYmb8GW/+RS/iNa8vz9FiiTIl0YS0OdmNKKIEL
Lg08O/TKGusV2CyqtT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBsWjijNHNwBICv6WAO2gr/xj+qxpB3
P1YjNTU7llSFnSHC4E1Fzg3hy40yHCNqv7x/4jlniIAL9dGhrgQjnoFQ1DcDoD8m
N1yPIOx3C0lWeVForZmx+Dg6l+J4uIjytkVceBwOv1bDNdDRyk+BIb0pLFl2VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

رسالة تحذير - خطأ في التحليل: تعذر فك ترميز بيانات PEM

عرض

رسالة التحذير: خطأ في التحليل: تعذر فك ترميز بيانات PEM، تم تلقيها في جهاز "شبكة التهديد" بعد محاولة إضافة شهادة إلى واجهة.



يتعذر فك ترميز الشهادة من بيانات PEM الحالية الموجودة في ملف الشهادة. بيانات PEM داخل ملف الشهادة تالفة.

- تأكيد ما إذا كان يمكن إستردادا معلومات الشهادة من بيانات PEM داخل ملف الشهادة.

الخطوة 1. أستخدم أداة OpenSSL لعرض معلومات الترخيص من ملف بيانات PEM.

```
openssl x509 -in
```

إذا كانت بيانات PEM تالفة، فسيظهر خطأ عندما تحاول أداة OpenSSL تحميل معلومات الشهادة.

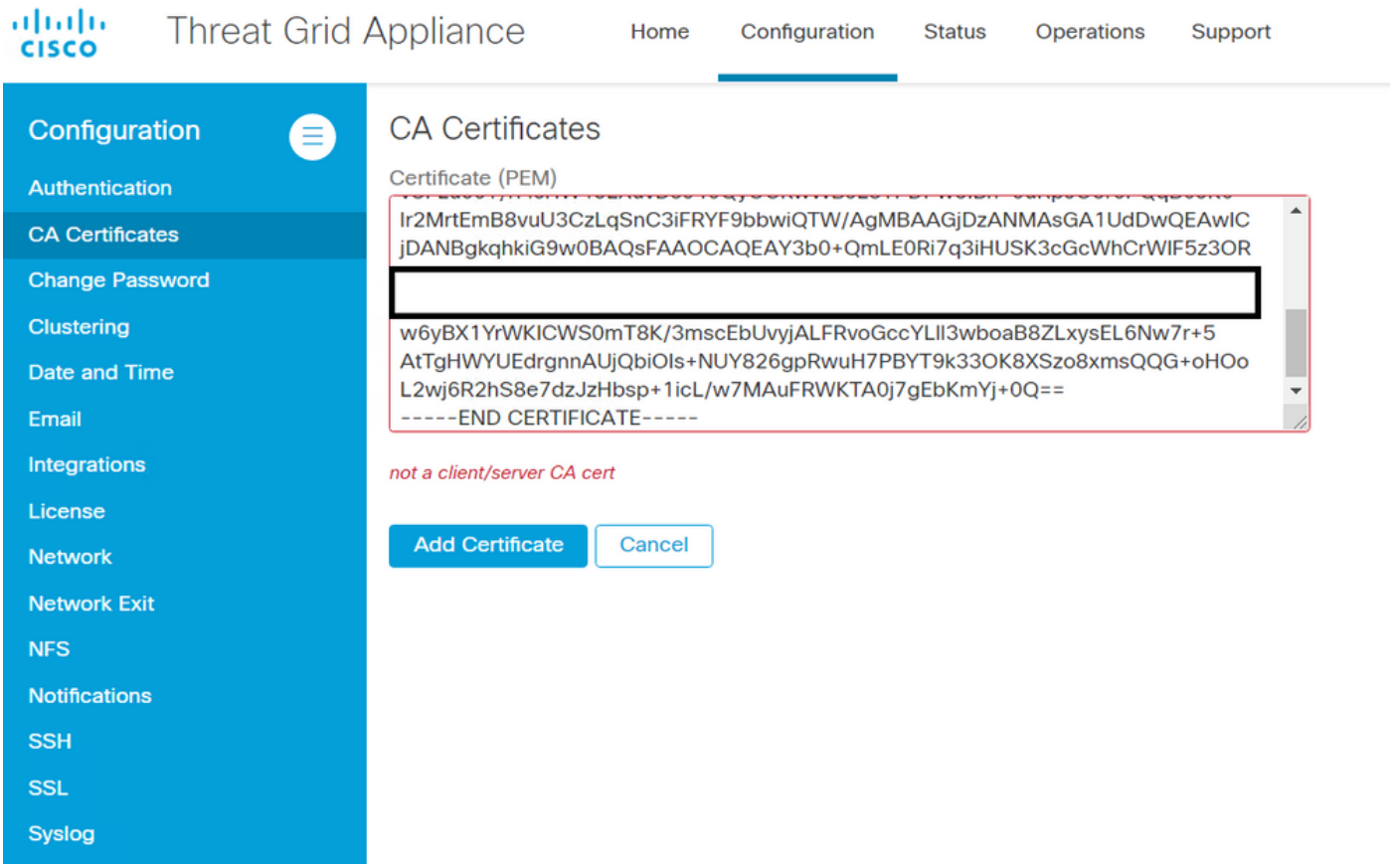
مثال. فشلت محاولة تحميل معلومات الشهادة بسبب تلف بيانات PEM في ملف الشهادة.

```
$ openssl x509 -in wrong-certificate.cert -text -noout
unable to load certificate
140159319831872:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:
```

رسالة تحذير - ليست شهادة مرجع مصدق للعميل/الخادم

عرض

رسالة التحذير: خطأ في التحليل: ليس شهادة مرجع تصديق عميل/خادم، يتم إستالمها في جهاز "شبكة التهديد" بعد محاولة إضافة شهادة مرجع مصدق إلى **التكوين > شهادات المرجع المصدق**.



لم يتم تعريف قيمة الملحق "القيود الأساسية" في شهادة CA ك CA: صحيح.

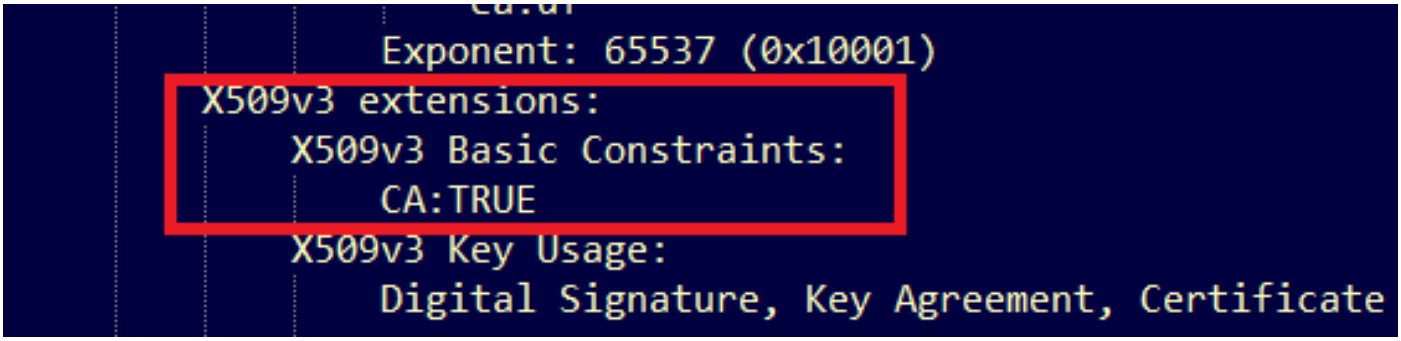
التأكيد باستخدام أداة OpenSSL إذا تم تعيين قيمة ملحق القيود الأساسية على CA: صحيح في شهادة CA.

الخطوة 1. أستخدم أداة OpenSSL لعرض معلومات الترخيص من ملف بيانات PEM.

```
openssl x509 -in
```

الخطوة 2. ابحث في معلومات الشهادة عن القيمة الحالية لملحق **القيود الأساسية**.

مثال. قيمة القيد الأساسية ل CA مقبول بواسطة جهاز شبكة التهديدات.



معلومات ذات صلة

- جهاز شبكة الحماية - أدلة التكوين
- الأداة السحابية الافتراضية الخاصة بالحماية المتقدمة من البرامج الضارة من Cisco - أمثلة التكوين والملاحظات الفنية
- الدعم التقني والمستندات - Cisco Systems

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).