أستكشاف الأخطاء وإصلاحها &t؛فشل تكوين السحابة"؛ على أجهزة FirePOWER

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

الرسم التخطيطي للشبكة

المشكلة

استكشاف الأخطاء وإصلاحها

الخيار 1. تكوين دجوي الى DNS

الخيار 2. تعذر على DNS الخاص بالعميل حل https://api-sse.cisco.com

المزيد من خيارات أستكشاف الأخطاء وإصلاحها

مشكلات معروفة

[فيديو] Firepower - تسجيل FMC في SSE

المقدمة

يصف هذا المستند السيناريوهات الشائعة التي يقوم فيها نظام FirePOWER بتشغيل التنبيه الصحي: تحديثات بيانات التهديد - تكوين السحابة من Cisco - الفشل.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة Firepower
- Firepower Threat Defense
- الوحدة النمطية لمستشعر Firepower
- تكامل السحابة
- دقة DNS واتصال الوكيل
- تكامل الاستجابة للتهديدات (CTR) من Cisco

المكونات المستخدمة

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

- مركز إدارة Firepower (FMC)، الإصدار 6.4.0 أو إصدار أحدث

- برنامج الدفاع عن تهديد Firepower (FTD) أو الوحدة النمطية لمستشعر FirePOWER (SFR) الإصدار 6.4.0 أو إصدار أحدث
- تبادل الخدمات الآمن (SSE) من Cisco
- بوابة الحساب الذكي من Cisco

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

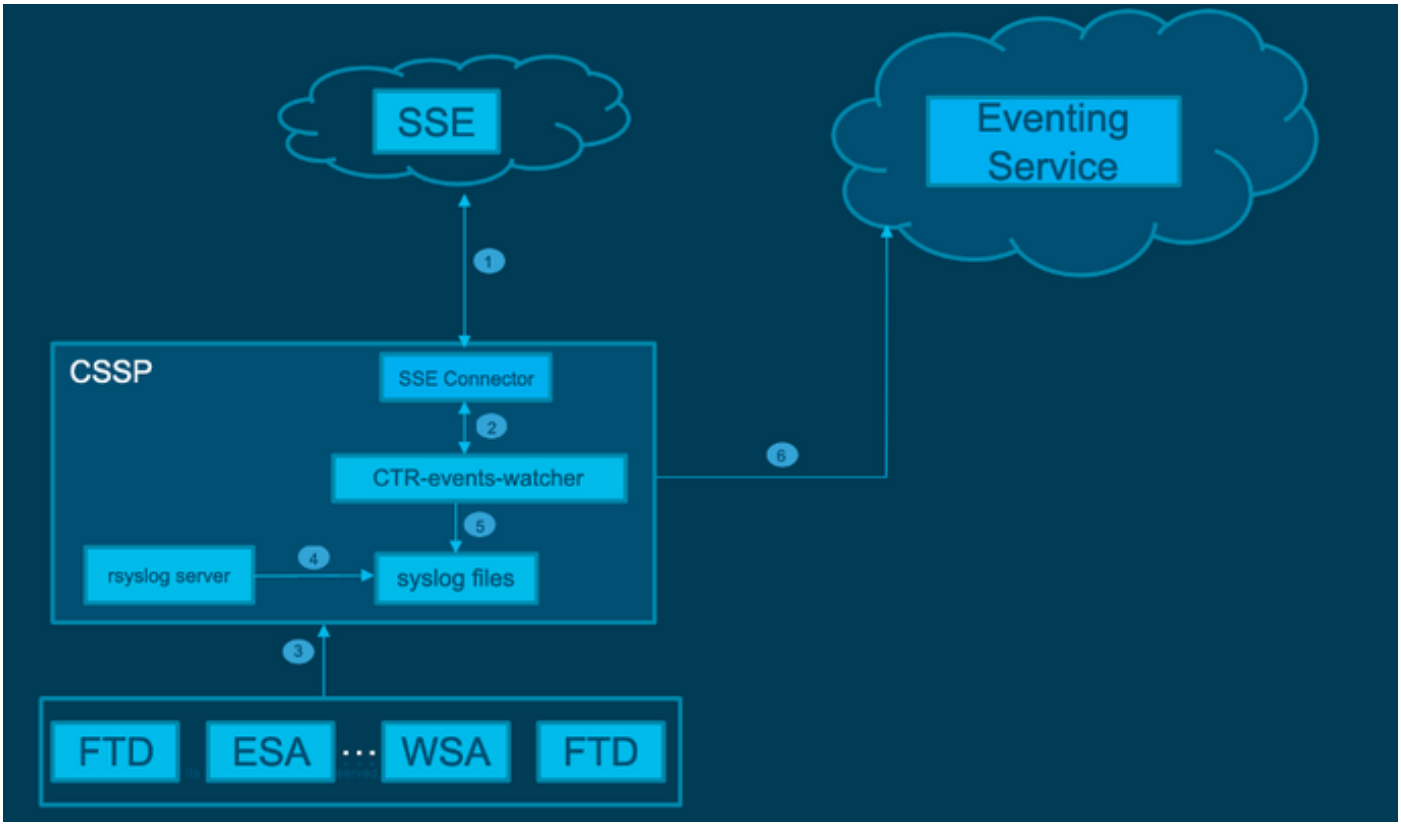
تمت ملاحظة خطأ تكوين السحابة لأن FTD غير قادر على الاتصال ب api-sse.cisco.com.

هذا هو الموقع الذي تحتاج أجهزة FirePOWER إلى الوصول إليه للتكامل مع خدمات SecureX والسحابة.

يعد هذا التنبيه جزءا من ميزة إحتواء التهديدات السريعة (RTC). يتم تمكين هذه الميزة بشكل افتراضي على إصدارات FirePOWER الجديدة، حيث يحتاج FTD إلى أن يكون قادرا على التحدث إلى api-sse.cisco.com على الإنترنت.

إذا لم يتوفر هذا الاتصال، فإن وحدة مراقبة صحة FTD تعرض رسالة الخطأ هذه: تحديثات بيانات التهديد - تكوين السحابة من Cisco - الفشل

الرسم التخطيطي للشبكة



المشكلة

يوضح مع عرف تصحيح الأخطاء من Cisco CSCvr46845 أنه عندما يقوم نظام FirePOWER بتشغيل التنبيه الصحي تكوين سحابة Cisco - الفشل، غالبا ما تكون المشكلة مرتبطة بالاتصال بين FTD وapi-sse.cisco.com.

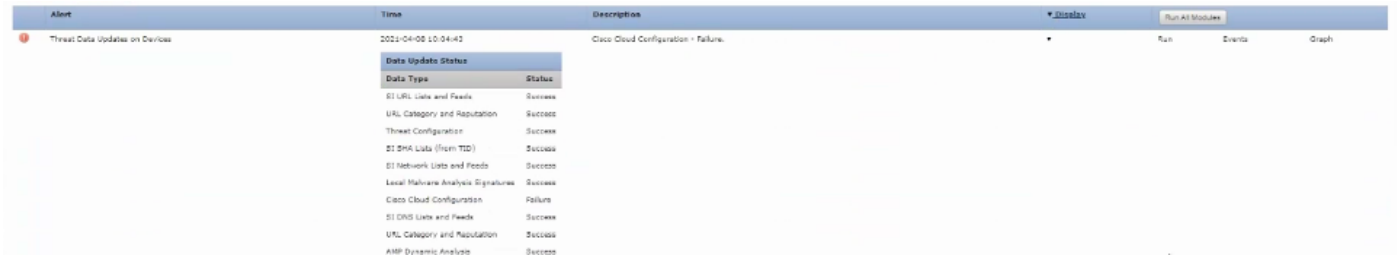
ومع ذلك، فإن التنبيه عام جدا ويمكن أن يشير إلى مشاكل متنوعة، حتى وإن كان ال يزال حول الاتصال، ولكن في سياق مختلف.

هناك سيناريوهان محتملان:

السيناريو الأول. في حالة عدم تمكين تكامل السحابة، من المتوقع أن يكون هذا التنبيه بسبب عدم السماح بالاتصال بمدخل السحابة.

السيناريو 2. في الحالة التي يتم فيها تمكين تكامل السحابة، من الضروري إجراء تحليل أكثر تفصيال لإزالة الظروف التي تنطوي على فشل الاتصال.

يتم عرض مثال تنبيه فشل الصحة في الصورة التالية:



مثال تنبيه فشل الصحة

استكشاف الأخطاء وإصالحها

حل سيناريو 1. تمت مالحظة خطأ تكوين السحابة ألن FTD غير قادر على االتصال ب https://api-sse.cisco.com/

لتعطيل تنبيه تكوين سحابة Cisco-العطل، انتقل إلى نظام > الصحة > السياسة > تحرير السياسة > تحديثات بيانات التحديد على الأجهزة. أختر تمكين (إيقاف)، احفظ النهج وانهاء.

فيما يلي الإرشادات المرجعية للتكوين الداخلي.

حل سيناريو 2. عندما يجب تمكين تكامل السحابة.

أوامر مفيدة الستكشاف الأخطاء وإصالحها:

<#root>

```
curl -v -k https://api-sse.cisco.com
```

```
 <-- To verify connection with the external site
```

```
nslookup api-sse.cisco.com
```

```
 <-- To dicard any DNS error
```

```
/ngfw/etc/sf/connector.properties
```

```
 <-- To verify is configure properly the FQDN settings

lsof -i | grep conn

 <-- To verify the outbound connection to the cloud on port 8989/tcp is ESTABLISHED
```

الخيار 1. الا يوجد تكوين DNS

الخطوة 1. تحقق من تكوين DNS على FTD. في حالة عدم وجود تكوينات DNS، فعليك المتابعة كما يلي:

```
> show network
```

الخطوة 2. إضافة DNS باستخدام الأمر:

```
> configure network dns servers dns_ip_addresses
```

بعد تكوين DNS، يتم إصلاح تنبيه الصحة ويتم عرض الجهاز كجهاز سليم. تكون هذه الفترة الزمنية قصيرة قبل أن يعكس التغيير تكوين خوادم DNS المناسبة.

الخيار 2. تعذر على DNS الخاص بالعميل حل https://api-sse.cisco.com

قم بالاختبار باستخدام الأمر curl. إذا تعذر على الجهاز الوصول إلى موقع السحابة، فهناك إخراج مشابه لهذا المثال.

<#root>

```
FTD01:/home/ldap/abbac#

curl -v -k

https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6)

Couldn't resolve host 'api-sse.cisco.com'
```

تلميح: ابدأ بنفس الطريقة لاستكشاف الأخطاء وإصلاحها كما هو الحال في الخيار 1. تحقق أولا من تعيين تكوين DNS بشكل صحيح. يمكنك ملاحظة مشكلة DNS بعد أن يقوم بتشغيل الأمر curl.

يجب أن يكون إخراج Curl الصحيح كما يلي:

<#root>

```
root@fp:/home/admin# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 10.6.187.110...
* Connected to api-sse.cisco.com (10.6.187.110) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api-sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 30 Dec 2020 21:41:15 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5fb40950-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src https: ;
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< X-Frame-Options: SAMEORIGIN
< Strict-Transport-Security: max-age=31536000; includeSubDomains
<

* Connection #0 to host api-sse.cisco.com left intact


Forbidden
```

قم بالرجوع إلى اسم المضيف للخادم.

<#root>

#

curl -v -k

https://cloud-sa.amp.cisco.com
*   Trying 10.21.117.50...
* TCP_NODELAY set
* Connected to cloud-sa.amp.cisco.com (10.21.117.50) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):

أستخدم أدوات الاتصال الأساسية مثل أوامر NSLOOKUP وtelnet وping للتحقق من دقة DNS الصحيحة لموقع سحابة Cisco.

ملاحظة: يجب أن يكون لخدمات سحابة Firepower اتصال صادر بالسحابة على المنفذ 8989/tcp.

تطبيق NSLOOKUP على أسماء مضيف الخادم.

```
# nslookup cloud-sa.amp.sourcefire.com
# nslookup cloud-sa.amp.cisco.com
# nslookup api.amp.sourcefire.com
# nslookup panacea.threatgrid.com
```

<#root>

root@fp:/home/admin#

nslookup api-sse.cisco.com

Server: 10.25.0.1
Address: 10.25.0.1#53

Non-authoritative answer:
api-sse.cisco.com canonical name = api-sse.cisco.com.akadns.net.
Name: api-sse.cisco.com.akadns.net
Address: 10.6.187.110
Name: api-sse.cisco.com.akadns.net
Address: 10.234.20.16

قد تكون مشاكل الاتصال بسحابة AMP ناجمة عن تحليل DNS. تحقق من إعدادات DNS أو قم بالبحث من FMC.

```
nslookup api.amp.sourcefire.com
```

Telnet

<#root>

```
root@fp:/home/admin#
```

telnet api-sse.cisco.com 8989

```
root@fp:/home/admin#
```

telnet api-sse.cisco.com 443

```
root@fp:/home/admin#
```

telnet cloud-sa.amp.cisco.com 443

بينغ

<#root>

```
root@fp:/home/admin#
```

ping api-sse.cisco.com

المزيد من خيارات أستكشاف الأخطاء وإصلاحها

تحقق من خصائص الموصل ضمن /ngfw/etc/sf/connector.properties. يجب أن ترى هذا الإخراج مع عنوان URL الصحيح connector_fqdn و (8989) منفذ الموصل الصحيح.

<#root>

```
root@Firepower-module1:sf#
```

cat /ngfw/etc/sf/connector.properties

```
registration_interval=180
```

connector_port=8989

```
region_discovery_endpoint=https://api-sse.cisco.com/providers/sse/api/v1/regions
```

```
connector_fqdn=api-sse.cisco.com
```

لمزيد من المعلومات، ارجع إلى دليل تكوين Firepower.

مشكلات معروفة

معرف تصحيح الأخطاء من Cisco CSCvs05084 FTD Cisco Cloud Configuration Failure بسبب الوكيل

معرف تصحيح الأخطاء من Cisco CSCvp56922 أستخدم Update-context sse-connector API لتحديث اسم مضيف الجهاز وإصداره

معرف تصحيح الأخطاء من Cisco CSCvu02123 DOC Bug: تحديث URL الذي يمكن الوصول إليه من أجهزة FirePOWER إلى SSE في دليل تكوين CTR

معرف تصحيح الأخطاء من Cisco CSCvr46845 ENH: تكوين رسالة الصحة Cisco Cloud - الفشل يحتاج إلى تحسين

[فيديو] Firepower - تسجيل FMC في SSE

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).