تتلقى ESA المزودة AMP خطأ "خدمة سمعة الملف غير قابلة للوصول"

المحتويات

المقدمة

يصف هذا المستند التنبيه المنسوب إلى جهاز أمان البريد الإلكتروني من Cisco (ESA) مع تمكين الحماية المتقدمة من البرامج الضارة (AMP)، حيث تكون الخدمة غير قادرة على الاتصال عبر المنفذ 32137 أو 443 للتعرف على الملف.

صححت الخطأ "خدمة سمعة الملف غير قابلة للوصول" الذي تم تلقيه ل AMP

تم إصدار AMP للاستخدام على ESA في الإصدار 8.5.5 من AsyncOS لأمان البريد الإلكتروني. يتلقى المسؤولون هذه الرسالة من خلال ترخيص AMP وتمكينه على ESA:

```
The Warning message is:

The File Reputation service is not reachable.

Last message occurred 2 times between Tue Jul 26 10:17:15 2015 and Tue Jul 26 10:18:16 2016.

Version: 12.5.0-066
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 07 Oct 2019 14:25:13 -0400
```

قد يتم تمكين خدمة AMP، ولكنها على الأرجح لا تتصل على الشبكة عبر المنفذ 32137 للتعرف على اسم الملف.

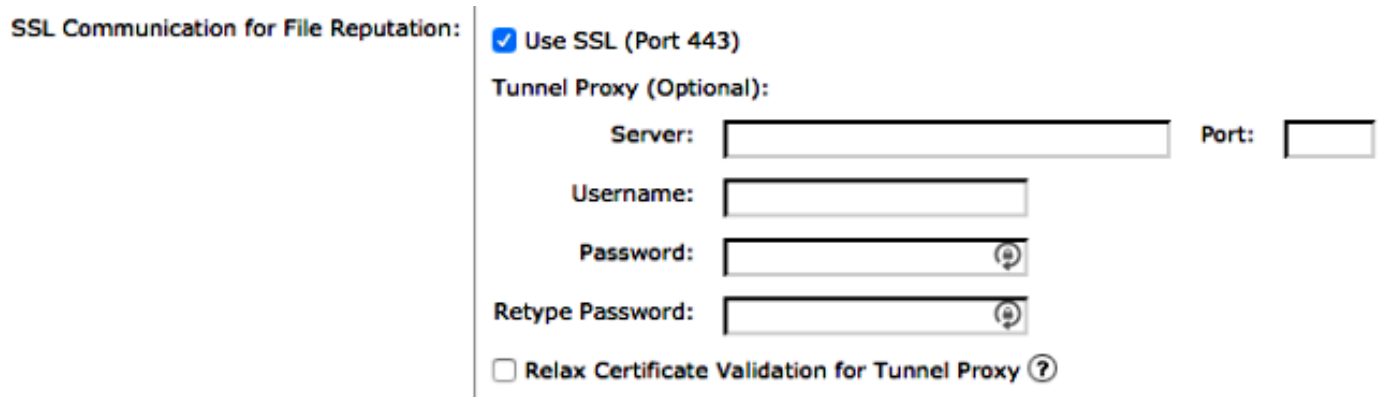
إذا كان هذا هو الحال، يمكن أن يختار مسؤول ESA أن يكون لديه اتصال "سمعة الملف" عبر المنفذ 443.

للقيام بذلك، قم بتشغيل **الأمر enableConfig > advanced** من واجهة سطر الأوامر وتأكد من تحديد Y ل *هل تريد تمكين اتصال SSL (المنفذ 443) لسمعة الملف؟ [N]>*:

```
(Cluster example.com)> ampconfig

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
```

```
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud
[1]>

Do you want use the recommended analysis threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

Do you want to suppress the verdict update alerts for all messages that are not delivered to the
recipient? [N]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. EUROPE (https://panacea.threatgrid.eu)
3. Private analysis cloud
[1]>
```

إذا كنت تستخدم واجهة المستخدم الرسومية، فأختر **خدمات الأمان > سمعة الملف وتحليله > تحرير الإعدادات العامة > إعدادات متقدمة (منسدلة)** وتأكد من تحديد خانة الاختيار **إستخدام SSL** كما هو موضح هنا:



قم بتطبيق أي وجميع التغييرات على التكوين.

وأخيرا، راجع سجل AMP الحالي للاطلاع على نجاح الخدمة والاتصال أو فشلها. يمكنك تحقيق ذلك من واجهة سطر الأوامر (CLI) باستخدام **أمبير الذيل**.

قبل إجراء التغييرات على **amconfig > متقدم**، كنت سترى هذا في سجلات AMP:

```
Mon Jan 26 10:11:16 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:12:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:13:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
```

بعد إجراء التغيير على **amconfig > متقدم**، يمكنك مشاهدة ذلك في سجلات AMP:

```
Mon Jan 26 10:19:19 2015 Info: amp stunnel process started pid [3725]
Mon Jan 26 10:19:22 2015 Info: amp The File Reputation service in the cloud
is reachable.
Mon Jan 26 10:19:22 2015 Info: amp File reputation service initialized
successfully
Mon Jan 26 10:19:22 2015 Info: amp File Analysis service initialized
successfully
Mon Jan 26 10:19:23 2015 Info: amp The File Analysis server is reachable
Mon Jan 26 10:20:24 2015 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Jan 26 10:20:24 2015 Info: amp Response received for file reputation query
from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown,
Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977
fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

سيتم تشغيل ملف **amp_watchdog.txt** كما هو موضح في المثال السابق كل 10 دقائق ويتم تتبعه في سجل AMP. يعد هذا الملف جزءا من AMP.

سيكون أي استعلام عادي في سجل AMP مقابل رسالة من نوع (أنواع) الملفات التي تم تكوينها لسمعة الملف وتحليل الملف مماثلا لهذه الرسالة:

```
Wed Jan 14 15:33:01 2015 Info: File reputation query initiating. File Name =
'securedoc_20150112T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Wed Jan 14 15:33:02 2015 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20150112T114401.html', MID = 703, Disposition = file
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

باستخدام معلومات السجل هذه، يجب أن يكون المسؤول قادرا على ربط معرف الرسالة (MID) في سجلات البريد.

استكشاف الأخطاء وإصلاحها

راجع إعدادات جدار الحماية والشبكة لضمان فتح اتصال SSL لهذه:

المنفذ	البروتوكول	الدخول/الخروج	اسم المضيف	الوصف
443	TCP	خارج	كما هو مكون في خدمات الأمان > سمعة الملف وتحليله، قسم متقدم.	الوصول إلى خدمات السحابة لتحليل الملفات.
32137	TCP	خارج	كما هو مكون في خدمات الأمان > سمعة الملف وتحليله، المقطع المتقدم، المقطع المتقدم، معلمة تجمع خوادم السحابة.	الوصول إلى خدمات السحابة للحصول على سمعة الملف.

يمكنك إختبار الاتصال الأساسي من ESA لديك إلى خدمة السحابة عبر برنامج Telnet عبر

برنامج Telnet لضمان إمكانية وصول الجهاز لديك إلى خدمات AMP وسمعة الملفات وتحليل الملفات بنجاح.

ملاحظة: يتم تكوين العناوين الخاصة بسمعة الملف وتحليل الملفات على واجهة المستخدم الرسومية (GUI) عم **خدمات الأمان > سمعة الملف وتحليله > تحرير الإعدادات العامة > إعدادات متقدمة (منسدلة)**.

ملاحظة: إذا كنت تستخدم وكيل نفق بين ESA وخادم (خوادم) سمعة الملف، فقد يطلب منك تمكين خيار تخفيف عملية التحقق من صحة الشهادة لوكيل النفق. يتم توفير هذا الخيار لتخطي التحقق من صحة الشهادة القياسية إذا لم يتم توقيع شهادة خادم وكيل النفق من قبل مرجع جذر موثوق به من قبل ESA. على سبيل المثال، حدد هذا الخيار إذا كنت تستخدم شهادة موقعة ذاتيا على خادم وكيل نفق داخلي موثوق به.

مثال سمعة الملف:

```
10.0.0-125.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.199.158...
Connected to ec2-23-21-199-158.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

مثال تحليل الملف:

```
10.0.0-125.local> telnet panacea.threatgrid.com 443

Trying 69.55.5.244...
Connected to 69.55.5.244.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

إذا كان ESA قادرا على إرسال برنامج Telnet إلى خادم سمعة الملف، ولا يوجد وكيل للتفويض، فقد يلزم إعادة تسجيل التطبيق باستخدام شبكة التشفير الاتصال، كما هو موضح في التعليمات. على واجهة سطر أوامر (CLI) ESA هناك أمر مخفي:

```
10.0.0-125.local> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> ampregister

AMP registration initiated.
```

معلومات ذات صلة

- اختبار ESA للحماية المتقدمة من البرامج الضارة (AMP)
- أدلة مستخدم ESA
- الأسئلة المتداولة حول ESA: ما هو معرف الرسالة (MID) أو معرف اتصال الحقن (ICID) أو معرف اتصال التسليم (DCID)؟
- كيف يمكنني البحث وعرض سجلات البريد على ESA؟
- 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).