تكوين مضيف سمعة الملف الثابت أو تجمع خادم سحابة سمعة الملف البديل على ESA

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز أمان البريد الإلكتروني من Cisco (ESA) للاتصال بمضيف ثابت أو تجمع خادم سحابة السمعة البديل للحصول على سمعة الملف باستخدام الحماية المتقدمة من البرامج الضارة (AMP) واستخدامها.

معلومات أساسية

يعتبر الاستعلام عن "سمعة الملفات" أول طبقتين من AMP على ESA. تقوم ميزة "سمعة الملفات" بالتقاط بصمة كل ملف عند إجتياز ESA وإرساله إلى شبكة الذكاء القائمة على سحابة AMP للحصول على حكم حول السمعة. بافتراض هذه النتائج، يمكن لمسؤولي ESA حظر الملفات الضارة تلقائيا وتطبيق السياسات التي يحددها المسؤول. تتم إستضافة خدمة سحابة "سمعة الملف" على خدمات الويب في Amazon (AWS). عند إجراء استعلامات DNS مقابل اسم المضيف (أسماء المضيف) الموضحة في هذا المستند، سترى "amazonaws.com." مدرجا.

أما الطبقة الثانية من بروتوكول AMP في ESA فهي ميزة تحليل الملفات. لا تتم تغطية ذلك في هذا المستند.

يستخدم اتصال SSL لحركة مرور سمعة الملف المنفذ 32137 بشكل افتراضي. في وقت تكوين الخدمة، قد يتم إستخدام المنفذ 443 كبديل. ارجع إلى قسم دليل مستخدم ESA، "تصفية سمعة الملفات وتحليل الملفات" للحصول على تفاصيل كاملة. قد يرغب مسؤولو ESA والشبكة في التحقق من الاتصال بالمجموعة لعنوان (عناوين) IP وموقع IP وكذلك إتصالات المنفذ (32137 مقابل 443) قبل المتابعة مع التكوين.

تجمع خادم سحابة السمعة الافتراضي للأمريكتين (القديم) (cloud-sa.amp.sourcefire.com)

بمجرد ترخيص "سمعة الملف" وتمكينها وتكوينها على ESA، سيتم تعيينها بشكل افتراضي لتجمع خوادم سحابة

السمعة هذا:

- الأمريكيتين (إرث) (cloud-sa.amp.sourcefire.com)

اسم المضيف "cloud-sa.amp.sourcefire.com" هو سجل الاسم القانوني ل CNAME. CNAME هو نوع سجل المورد في DNS المستخدم لتحديد اسم المجال كاسم مستعار لمجال آخر، وهو المجال "كانوني". قد تكون أسماء المضيف المقترنة في التجمع المرتبط بهذا الاسم مماثلة ل:

- (ec2-107-22-180-78.compute-1.amazonaws.com (107.22.180.78
- (ec2-54-225-142-100.compute-1.amazonaws.com (54.225.142.100
- (ec2-23-21-208-4.compute-1.amazonaws.com (23.21.208.4
- (ec2-54-83-195-228.compute-1.amazonaws.com (54.83.195.228

هناك خياران إضافيان لخوادم سمعة الملفات يمكن تحديدهما:

- الأمريكتان (cloud-sa.amp.cisco.com)
- أوروبا (cloud-sa.eu.amp.cisco.com)

تمت تغطية كلا الخادمين المذكورين في قسم "أسماء مضيف خادم سمعة الملف الثابت (.cisco.com)" في هذا المستند.

يمكنك التحقق من الأجهزة المضيفة المقترنة ب cloud-sa-amp.sourcefire.comCNAME من الشبكة الخاصة بك في أي وقت تقوم فيه بتشغيل استعلام **البحث** أو **البحث** هذا:

```
dig cloud-sa.amp.sourcefire.com +short $
.cloud-sa-589592150.us-east-1.elb.amazonaws.com
107.22.180.78
54.225.208.214
23.21.208.4
54.83.195.228

nslookup cloud-sa.amp.sourcefire.com $
Server: 208.67.222.222
Address: 208.67.222.222#53

:Non-authoritative answer
.cloud-sa.amp.sourcefire.com canonical name = cloud-sa-589592150.us-east-1.elb.amazonaws.com
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.225.208.214
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.83.195.228
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 107.22.180.78
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 23.21.208.4
```

ملاحظة: هذه الأجهزة المضيفة ليست ثابتة ومن المستحسن عدم تقييد حركة مرور "سمعة ملف ESA" استنادا إلى هذه الأجهزة المضيفة فقط. قد تختلف نتائج الاستعلام الخاص بك، حيث ستتغير البيئات المضيفة في التجمع دون إشعار.

يمكنك التحقق من موقع IP الجغرافي من أداة الطرف الثالث هذه:

- http://geoiplookup.net/ip/107.22.180.78
- http://geoiplookup.net/ip/54.225.208.214
- http://geoiplookup.net/ip/23.21.208.4
- http://geoiplookup.net/ip/54.83.195.228

أسماء مضيفات خادم سمعة الملف الثابت (cisco.com.)

بدأت Cisco في توفير أسماء المضيف المستندة إلى "cisco.com." لخدمة "سمعة الملف" ل AMP في عام 2016. هناك أسماء بيوت ثابتة وعناوين IP متاحة لسمعة الملف من هذا:

- cloud-sa.amp.cisco.com (أمريكا الشمالية - الولايات المتحدة الأمريكية)
- cloud-sa.eu.amp.cisco.com (أوروبا - جمهورية أيرلندا)
- cloud-sa.apjc.amp.cisco.com (منطقة آسيا والمحيط الهادئ - اليابان)

قد تقوم بالتحقق من الأجهزة المضيفة وعناوين IP المقترنة من شبكتك وتشغيل استعلام **تحويل** أو **بحث** NSLOOKUP:

أمريكا الشمالية (الولايات المتحدة):

```
dig cloud-sa.amp.cisco.com +short $
52.21.117.50
```

أوروبا (جمهورية أيرلندا):

```
nslookup cloud-sa.eu.amp.cisco.com $
Server: 208.67.222.222
Address: 208.67.222.222#53

:Non-authoritative answer
Name: cloud-sa.eu.amp.cisco.com
Address: 52.30.124.82
```

المحيط الهادئ (اليابان):

```
dig cloud-sa.apjc.amp.cisco.com +short $
52.69.39.127
```

يمكنك التحقق من موقع IP الجغرافي من أداة الطرف الثالث هذه:

- http://geoiplookup.net/ip/52.21.117.50
- http://geoiplookup.net/ip/52.30.124.82
- http://geoiplookup.net/ip/52.69.39.127

في هذا الوقت، لا توجد خطط لإلغاء تسمية المضيف "sourcefire.com.".

تجمع خادم سحابة السمعة الأوروبية البديل (cloud-sa.eu.amp.sourcefire.com)

بالنسبة للعملاء الموجودين في الاتحاد الأوروبي والمطالبين بإرسال حركة مرور معينة إلى الخوادم ومراكز البيانات الموجودة في الاتحاد الأوروبي فقط، يمكن للمسؤولين تكوين ESA للإشارة إما إلى المضيف الثابت للاتحاد الأوروبي أو إلى تجمع خوادم سحابة السمعة في الاتحاد الأوروبي:

- cloud-sa-eu.amp.cisco.com
- cloud-sa.eu.amp.sourcefire.com

مثل hostname الافتراضي "cloud-sa.amp.sourcefire.com"، فإن اسم المضيف "cloud-sa.eu.amp.sourcefire.com" هو أيضا CNAME. قد تكون أسماء المضيف المقترنة في التجمع المرتبط بهذا CNAME مماثلة ل:

- (54.217.245.97) ec2-54-217-245-97.eu-west-1.compute.amazonaws.com)
- (54.247.186.153) ec2-54-247-186-153.eu-west-1.compute.amazonaws.com)

- (ec2-176-34-122-245.eu-west-1.compute.amazonaws.com (176.34.122.245

يمكنك التحقق من الأجهزة المضيفة المقترنة ب CNAME cloud-sa.eu.amp.sourcefire.com من EUROPEAN الشبكة وتشغيل استعلام **dig** أو **nslookup**::

```
dig cloud-sa.eu.amp.sourcefire.com +short $
.cloud-sa-162723281.eu-west-1.elb.amazonaws.com
54.217.245.97
54.247.186.153
176.34.122.245

nslookup cloud-sa.eu.amp.sourcefire.com $
Server: 208.67.222.222
Address: 208.67.222.222#53

:Non-authoritative answer
.cloud-sa.eu.amp.sourcefire.com canonical name = cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.182.97
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 176.34.122.245
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.186.153
```

ملاحظة: هذه الأجهزة المضيفة ليست ثابتة ومن المستحسن عدم تقييد حركة مرور "سمعة ملف ESA" استنادا إلى هذه الأجهزة المضيفة فقط. قد تختلف نتائج الاستعلام الخاص بك، حيث ستتغير البيئات المضيفة في التجمع دون إشعار.

يمكنك التحقق من موقع IP الجغرافي من أداة الطرف الثالث هذه:

- http://geoiplookup.net/ip/176.34.122.245
- http://geoiplookup.net/ip/54.247.186.153
- http://geoiplookup.net/ip/54.217.245.97

تكوين مضيف سمعة الملف الثابت أو تجمع خادم سحابة سمعة الملف البديل على ESA

يمكن تكوين سمعة الملف من واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI) على ESA. توضح خطوات التكوين المدرجة في هذا المستند تكوين CLI. ومع ذلك، يمكن تطبيق نفس الخطوات والمعلومات عبر واجهة المستخدم الرسومية (**خدمات الأمان > سمعة الملف وتحليله > تحرير الإعدادات العامة.. > إعدادات متقدمة لسمعة الملف**).

AsyncOS 10.x والإصدارات الأحدث

تتيح الميزات الجديدة لنظام التشغيل AsyncOS 10.x تكوين ESA لاستخدام سحابة السمعة الخاصة (خادم سمعة الملف الداخلي) أو خادم سمعة الملف المستند إلى السحابة. ومع هذا التغيير، لم يعد تكوين AMP يطالب باسم المضيف باستخدام الخطوة "إدخال سمعة تجمع خادم السحابة". يجب إختيار إعداد خادم سمعة الملف الإضافي كسحابة سمعة خاصة وتوفير المفتاح العام لاسم المضيف هذا.

بالنسبة إلى الإصدار x.10.0 والإصدارات الأحدث، عند تكوين خادم سمعة AMP بديل، قد يطلب منك إدخال مفتاح عام مرتبط باسم المضيف هذا.

تستخدم جميع خوادم سمعة AMP نفس المفتاح العام:

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
==WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g
-----END PUBLIC KEY-----
```

سيساعدك هذا المثال في إعداد خادم سمعة الملف البديل على cloud-sa.eu.amp.sourcefirce.com:

```
my11esa.local > ampconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
.((Machine 122.local

?What would you like to do
."Switch modes to edit at mode "Cluster Test_cluster .1
.(Start a new, empty configuration at the current mode (Machine 122.local .2
.(Copy settings from another cluster mode to the current mode (Machine 122.local .3
<[1]

File Reputation: Enabled
File Analysis: Enabled
:File types selected for File Analysis
(Adobe Portable Document Format (PDF
(Microsoft Office 2007+ (Open XML
(Microsoft Office 97-2004 (OLE
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


: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
.CLEARCACHE - Clears the local File Reputation cache -
.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
(AMERICAS (cloud-sa.amp.sourcefire.com .1
Private reputation cloud .2
<[2]

?Enter AMP reputation server hostname or IP address
cloud-sa.eu.amp.sourcefire.com <[]

Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
==WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g
-----END PUBLIC KEY-----
.
?Enter cloud domain
<[a.immunet.com]

<[Do you want use the recommended reputation threshold from cloud service? [Y
```

```
?Enter heartbeat interval
<[15]

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

Please make sure you have added the Amp onprem reputation server CA certificate in certconfig-
>CERTAUTHOROTIES->CUSTOM
:Proxy server detail
: Server
: Port
: User

<[Do you want to change proxy detail [N

:Choose a file analysis server
(AMERICAS (https://panacea.threatgrid.com .1
Private analysis cloud .2
<[1]
```

قم بتنفيذ أي تغييرات في التكوين.

AsyncOS 9.7.x والإصدارات الأقدم

سيساعدك هذا المثال على AsyncOS 9.7.2-065 لأمان البريد الإلكتروني على ترقية تجمع خوادم سحابة السمعة البديل إلى cloud-sa.eu.amp.sourcefirce.com:

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
:File types selected for File Analysis
(Adobe Portable Document Format (PDF
(Microsoft Office 2007+ (Open XML
(Microsoft Office 97-2004 (OLE
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


: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
.CLEARCACHE - Clears the local File Reputation cache -
advanced <[]

?Enter cloud query timeout
<[15]

?Enter cloud domain
<[a.immunet.com]

?Enter reputation cloud server pool
cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com]

<[Do you want use the recommended reputation threshold from cloud service? [Y

:Choose a file analysis server
(AMERICAS (https://panacea.threatgrid.com .1
```

```
Private Cloud .2
<[1]

?Enter heartbeat interval
<[15]

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

:Proxy server detail
: Server
: Port
: User

<[Do you want to change proxy detail [N
```

قم بتنفيذ أي تغييرات في التكوين.

خادم سمعة الملف المحلي (FireAMP Private Cloud)

تم تقديم إستخدام خادم سمعة الملفات المحلي، المعروف أيضا باسم سحابة FireAMP الخاصة، والذي يبدأ ب AsyncOS 10.x لأمان البريد الإلكتروني.

إذا قمت بنشر جهاز سحابة افتراضي خاص بالحماية المتقدمة من البرامج الضارة من Cisco على شبكتك، فيمكنك الآن الاستعلام عن سمعة الملف الخاص بمرفقات الرسائل دون إرسالها إلى سحابة السمعة العامة. لتكوين الجهاز الخاص بك لاستخدام خادم سمعة الملفات المحلي، راجع الفصل "تصفية سمعة الملفات وتحليلها" في دليل مستخدم ESA أو التعليمات عبر الإنترنت.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

in order to رأيت ملف سمعة حركة مرور يمر إلي ال يشكل مضيف ساكن إستاتيكي أو سمعة سحابة نادل بركة، أنجزت ربط التقاط من ال ESA مع يعين مرشح أن على قبض ميناء 32137 أو ميناء 443 حركة مرور.

على سبيل المثال، أستخدم تجمع خوادم السحابة cloud-sa.eu.amp.sourcefire.com واتصالات SSL باستخدام المنفذ 443...

تم تسجيل هذا الأمر إلى ESA في سجلات AMP:

```
Sun Mar 26 21:17:45 2017 Info: File reputation query initiating. File Name =
'contract_604418.doc', MID = 463, File Size = 139816 bytes, File Type = application/msword
Sun Mar 26 21:17:46 2017 Info: Response received for file reputation query from Cloud. File Name
= 'contract_604418.doc', MID = 463, Disposition = MALICIOUS, Malware = W32.8A78D308C9-95.SBX.TG,
Reputation Score = 99, sha256 =
8a78d308c96ff5c7158ea1d6ca25f3546fae8515d305cd699eab2d2ef3c08745, upload_action = 2
```

قام تتبع حزمة ESA الجاري تشغيله بتصوير هذه المحادثة:

```
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 74 51391  28.504624 1060
443 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=64 SACK_PERM=1 TSval=198653388 TSecr=0
ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 74 443  28.594265 1072
51391 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=142397924
TSecr=198653388 WS=256
```

```
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.594289 1073
                          443 [ACK] Seq=1 Ack=1 Win=16384 Len=0 TSval=198653478 TSecr=142397924
      my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com SSL 502 28.595264 1074
                                                                                  Client Hello
  ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443  28.685554 1085
                       51391 [ACK] Seq=1 Ack=437 Win=30208 Len=0 TSval=142397947 TSecr=198653478
   ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 1434 28.687344 1086
                                                                                  Server Hello
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.687378 1087
                       443 [ACK] Seq=437 Ack=1369 Win=15040 Len=0 TSval=198653568 TSecr=142397947
 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 146 [TCP 28.687381 1088
                                                                    [segment of a reassembled PDU
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.687400 1089
                       443 [ACK] Seq=437 Ack=1449 Win=14912 Len=0 TSval=198653568 TSecr=142397947
ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 1434 [TCP 28.687461 1090
                                                                    [segment of a reassembled PDU
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.687475 1091
                       443 [ACK] Seq=437 Ack=2817 Win=13568 Len=0 TSval=198653568 TSecr=142397947
ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 1346 [TCP 28.687479 1092
                                                                    [segment of a reassembled PDU
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.687491 1093
                       443 [ACK] Seq=437 Ack=4097 Win=12288 Len=0 TSval=198653568 TSecr=142397947
  my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 [TCP 28.687614 1094
Window Update] 51391  443 [ACK] Seq=437 Ack=4097 Win=16384 Len=0 TSval=198653568 TSecr=142397947
   ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 1120 28.711945 1096
                                                                                  Certificate
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.711973 1097
                       443 [ACK] Seq=437 Ack=5151 Win=15360 Len=0 TSval=198653594 TSecr=142397953
    my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 392 28.753074 1098
                             Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 348 New 28.855886 1099
                                  Session Ticket, Change Cipher Spec, Encrypted Handshake Message
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.855934 1100
                       443 [ACK] Seq=763 Ack=5433 Win=16128 Len=0 TSval=198653740 TSecr=142397989
    my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 252 28.856555 1101
                                                          Application Data, Application Data
    ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 252 28.952344 1104
                                                          Application Data, Application Data
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  28.952419 1105
                       443 [ACK] Seq=949 Ack=5619 Win=16192 Len=0 TSval=198653837 TSecr=142398013
    my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 300 28.958953 1106
                                                          Application Data, Application Data
    ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 268 29.070057 1107
                                                          Application Data, Application Data
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  29.070117 1108
                      443 [ACK] Seq=1183 Ack=5821 Win=16192 Len=0 TSval=198653951 TSecr=142398043
    ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 103 59.971986 1279
                                                                                  Encrypted Alert
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  59.972030 1280
                      443 [ACK] Seq=1183 Ack=5858 Win=16320 Len=0 TSval=198684848 TSecr=142405768
  ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443  59.972034 1281
               51391 [FIN, ACK] Seq=5858 Ack=1183 Win=33280 Len=0 TSval=142405768 TSecr=198653951
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  59.972044 1282
                      443 [ACK] Seq=1183 Ack=5859 Win=16320 Len=0 TSval=198684848 TSecr=142405768
    my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 103 59.972392 1283
                                                                                  Encrypted Alert
my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391  59.972528 1284
                 443 [FIN, ACK] Seq=1220 Ack=5859 Win=16384 Len=0 TSval=198684848 TSecr=142405768
  ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443  60.062083 1285
                    51391 [ACK] Seq=5859 Ack=1221 Win=33280 Len=0 TSval=142405791 TSecr=198684848
```

أنت ترى أن الحركة مرور يتصل عبر ميناء 443. من موقع ESA الخاص بنا (my11esa.local)، فإنه يتصل بالعنوان hostname ec2-176-34-122-245.eu-west-1.compute.amazonaws.com. اسم المضيف هذا مرتبط بعنوان IP: 176.34.122.245

```
dig ec2-176-34-122-245.eu-west-1.compute.amazonaws.com +short $
176.34.122.245
```

عنوان 176.34.122.245 IP هو عضو تجمع في الاسم ل cloud-sa.eu.amp.sourcefire.com:

```
dig cloud-sa.eu.amp.sourcefire.com +short $
.cloud-sa-162723281.eu-west-1.elb.amazonaws.com
54.217.245.200
54.247.186.153
176.34.122.245
```

على سبيل المثال، تم توجيه الاتصال وقبوله بواسطة تجمع خوادم سحابة السمعة الذي تم تكوينه، cloud-sa.eu.amp.sourcefire.com.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إستخدام Telnet لاختبار الاتصال

للتحقق من الاتصال على مستوى المنفذ بسحابة "سمعة الملف"، أستخدم اسم المضيف لتجمع خوادم سحابة السمعة التي تم تكوينها، واختبر مع **telnet** إلى المنفذ 32137، أو المنفذ 443، كما تم تكوينها.

```
my97esa.local> telnet cloud-sa.amp.sourcefire.com 443

...Trying 23.21.208.4
.Connected to ec2-23-21-208-4.compute-1.amazonaws.com
.'[^' Escape character is
[^
telnet> quit
.Connection closed
```

اتصال فعلي بالاتحاد الأوروبي، ناجح عبر المنفذ 443:

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 443

...Trying 176.34.113.72
.Connected to ec2-176-34-113-72.eu-west-1.compute.amazonaws.com
.'[^' Escape character is
[^
telnet> quit
.Connection closed
```

اتصال فعلي بالاتحاد الأوروبي، غير قادر على الاتصال عبر المنفذ 32137:

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

...Trying 176.34.113.72
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```

يمكنك إختبار Telnet إلى IP المباشر أو أسماء المضيف خلف CNAME لتجمع خوادم سحابة السمعة باستخدام طريقة إختبار Telnet نفسها، مع إستخدام المنفذ 32137 أو المنفذ 443. إذا لم تكن قادرا على توصيل Telnet بنجاح باسم المضيف والمنفذ، فقد تحتاج إلى التحقق من اتصال الشبكة وإعدادات جدار الحماية خارج ESA.

سيتم التحقق من صلاحية برنامج Telnet لخادم سمعة الملفات المحلي بواسطة العملية نفسها كما هو موضح.

إدخال المفتاح العام

عند إدخال المفتاح العام على ESA الذي يشغل نظام التشغيل AsyncOS 10.x والإصدارات الأحدث، تأكد من أنك نجحت في لصق المفتاح العام أو تحميله. سيتم عرض أي أخطاء في المفتاح العام لمخرج التكوين:

```
Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MEAwEAYHKoZIzj0CAQYFK4EEAAEDLAAEAIHPMkqCH057gxeQK6aUKqmpqk+1AW0u
vxOkpuI+gtfLICRijTx3Vh45
-----END PUBLIC KEY-----
.
Failed to save public key
```

إذا تلقيت خطأ، فأعد محاولة التكوين. بالنسبة للأخطاء المتواصلة، اتصل بدعم Cisco.

مراجعة سجلات AMP

عندما تقوم بعرض سجل AMP الموجود على ESA، تأكد من أنك ترى "استعلام سمعة الملف من السحابة" المحدد في وقت استعلام سمعة الملف:

```
Sun Mar 26 11:28:13 2017 Info: File reputation query initiating. File Name =
'billing_fax_271934.doc', MID = 458, File Size = 143872 bytes, File Type = application/msword
Sun Mar 26 11:28:14 2017 Info: Response received for file reputation query from Cloud. File Name
= 'billing_fax_271934.doc', MID = 458, Disposition = MALICIOUS, Malware = W32.50944E2888-
100.SBX.TG, Reputation Score = 0, sha256 =
50944e2888b551f41f3de2fc76b4b57cb3cd28e718c9265c43128568916fe70f, upload_action = 2
```

إذا رأيت هذا، فإن الاستعلام سحب الاستجابة من ذاكرة التخزين المؤقت المحلية ل ESA و NOT من مجموعة خوادم سحابة السمعة التي تم تكوينها :

```
Sun Mar 26 11:30:18 2017 Info: File reputation query initiating. File Name =
'billing_fax_271934.doc', MID = 459, File Size = 143872 bytes, File Type = application/msword
Sun Mar 26 11:30:18 2017 Info: Response received for file reputation query from Cache. File Name
= 'billing_fax_271934.doc', MID = 459, Disposition = MALICIOUS, Malware = W32.50944E2888-
100.SBX.TG, Reputation Score = 0, sha256 =
50944e2888b551f41f3de2fc76b4b57cb3cd28e718c9265c43128568916fe70f, upload_action = 2
```

أخطاء وتنبيهات إضافية

قد يتلقى مسؤول ESA هذا الإشعار. إذا تم تلقي هذا الأمر، فعليك بإعادة التقدم خلال عملية التكوين والتحقق.

```
:The Warning message is

amp The previously selected regional server cloud-sa.eu.amp.sourcefire.com is unavailable.
.Server cloud-sa.amp.sourcefire.com has been selected as default

Version: 11.0.0-028
Serial Number: 1111CEE15FF3A9F9A1111-1AAA2CF4A1A1
Timestamp: 26 Mar 2017 11:09:29 -0400
```

معلومات ذات صلة

- عناوين الخادم المطلوبة لعمليات AMP المناسبة
- 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).