تثبيت الوحدة النمطية AMP وتكوينها من خلال أداة تمكين AnyConnect 4.x و AMP

المحتويات

المقدمة

يصف هذا المستند خطوات تثبيت وصل "الحماية المتقدمة من البرامج الضارة" (AMP) باستخدام AnyConnect.

يتم إستخدام أداة تمكين AnyConnect AMP كوسيط لنشر AMP لنقاط النهاية. كما أنها ال تملك أي قدرة على إدانة عملية التصرف في الملفات. وهو يدفع برنامج AMP لنقاط النهاية إلى نقطة نهاية من ASA. بمجرد تثبيت AMP، يستخدم سعة السحابة للتحقق من مصير الملفات. يمكن لخدمة AMP الإضافية إرسال الملفات إلى تحليل ديناميكي يسمى ThreatGrid، لتسجيل سلوك ملفات غير معروف. يمكن الحكم على هذه الملفات كملفات ضارة إذا تم الوفاء ببعض النتائج غير الدقيقة. وهذا مفيد على نطاق واسع لهجمات اليوم صفر.

المتطلبات الأساسية

المتطلبات

- AnyConnect Secure Mobility Client، الإصدار 4.x
- FireAMP / AMP لنقاط النهاية
- Adaptive Security Device Manager (ASDM)، الإصدار 7.3.2 أو إصدار أحدث

المكونات المستخدمة

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

- جهاز الأمان القابل للتكيف (ASA) 5525 مع إصدار البرنامج 9.5.1
- AnyConnect Secure Mobility Client 4.2.00096 على نظام التشغيل Microsoft Windows 7 Professional إصدار 64 بت
- ASDM الإصدار 7.5.1(112)

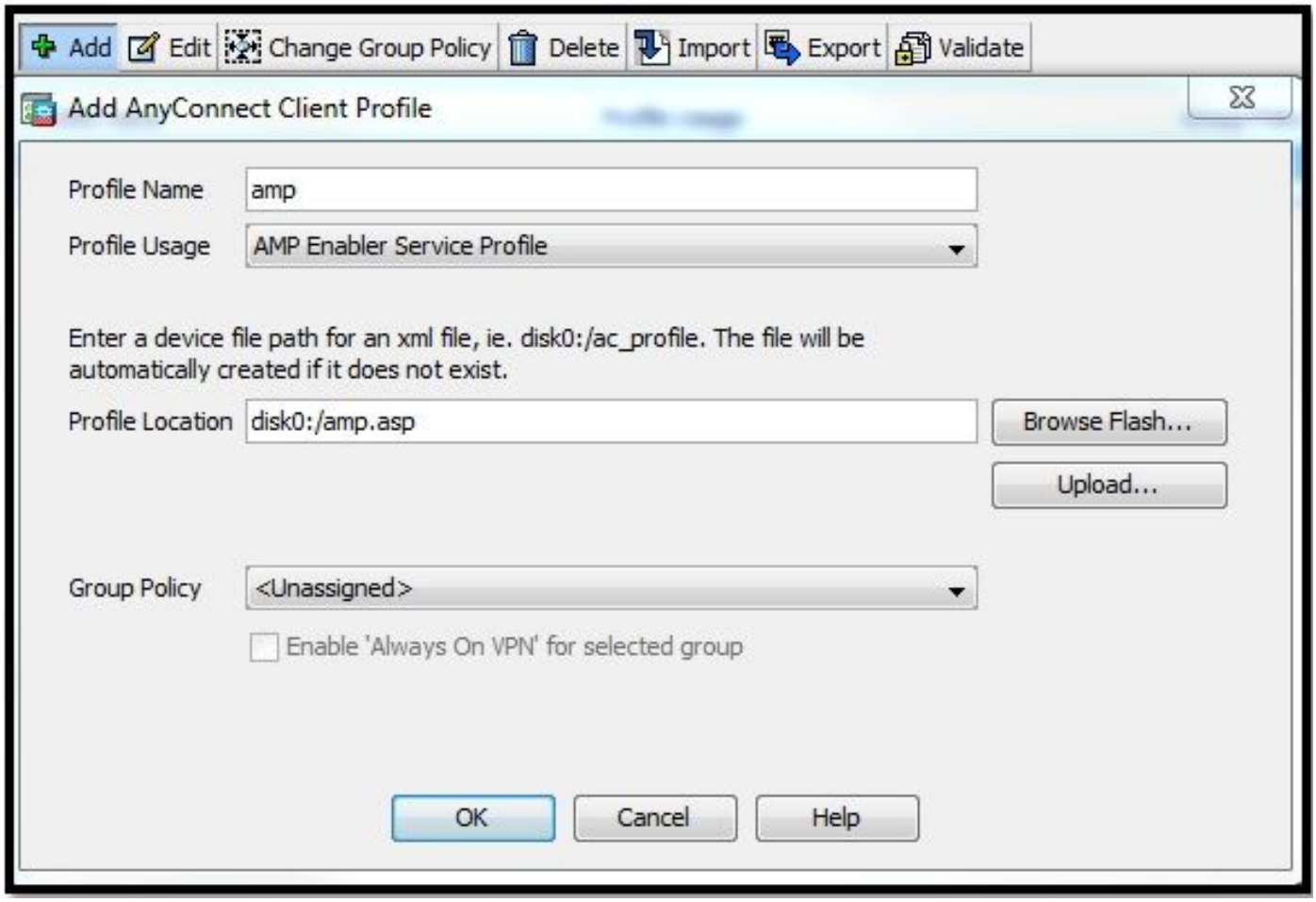
نشر AnyConnect ل AMP Enabler (أداة تمكين ASA)

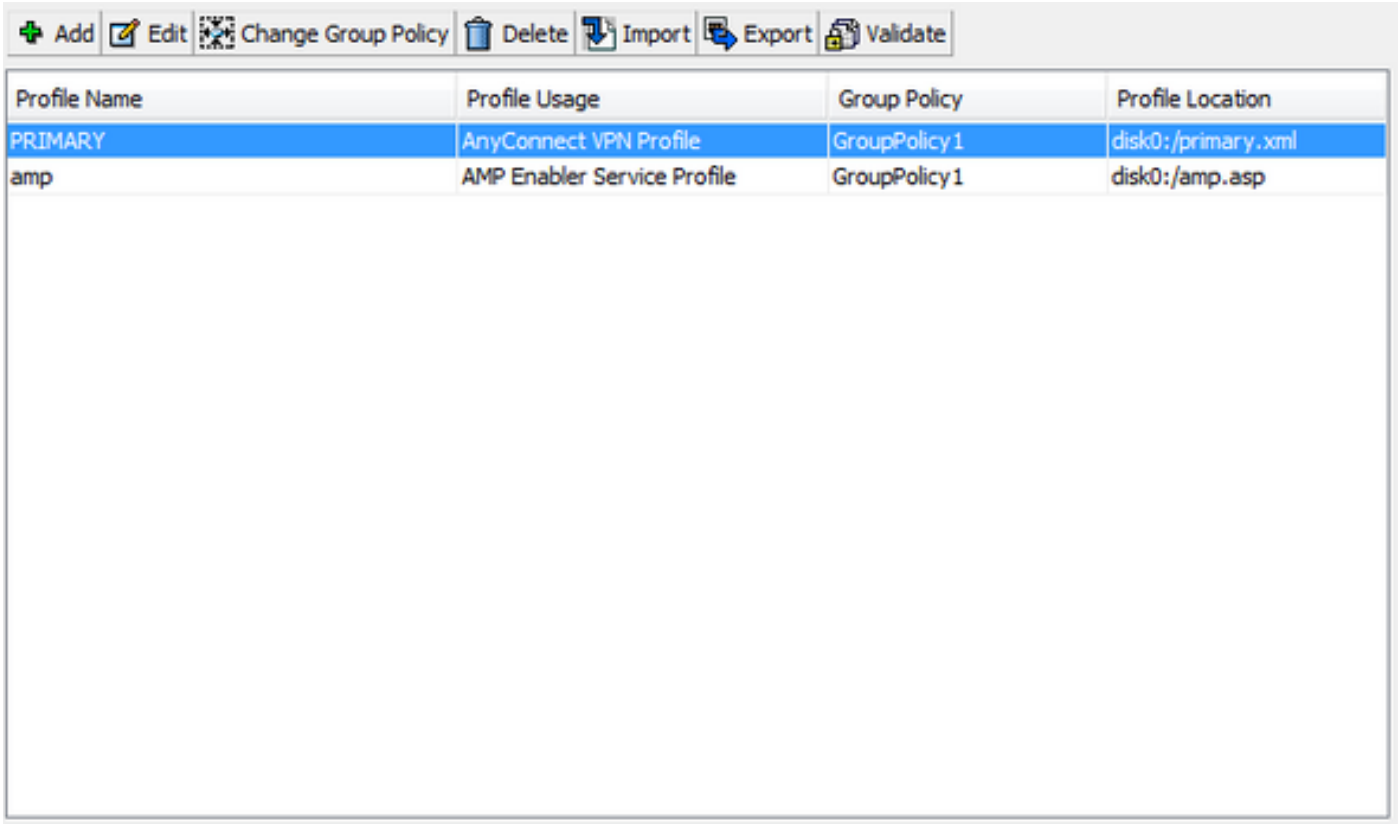
تكون الخطوات المعنية في التكوين كما يلي:

- تكوين ملف تعريف عميل AnyConnect AMP Enabler.
- قم بتحرير نهج مجموعة AnyConnect VPN وتنزيل ملف تعريف خدمة AMP Enabler.
- قم بتسجيل الدخول إلى لوحة معلومات AMP للحصول على إرتباط تنزيل URL الخاص بالموصل.
- تحقق من التثبيت على جهاز المستخدم.

الخطوة 1: تكوين ملف تعريف عميل AnyConnect AMP Enabler

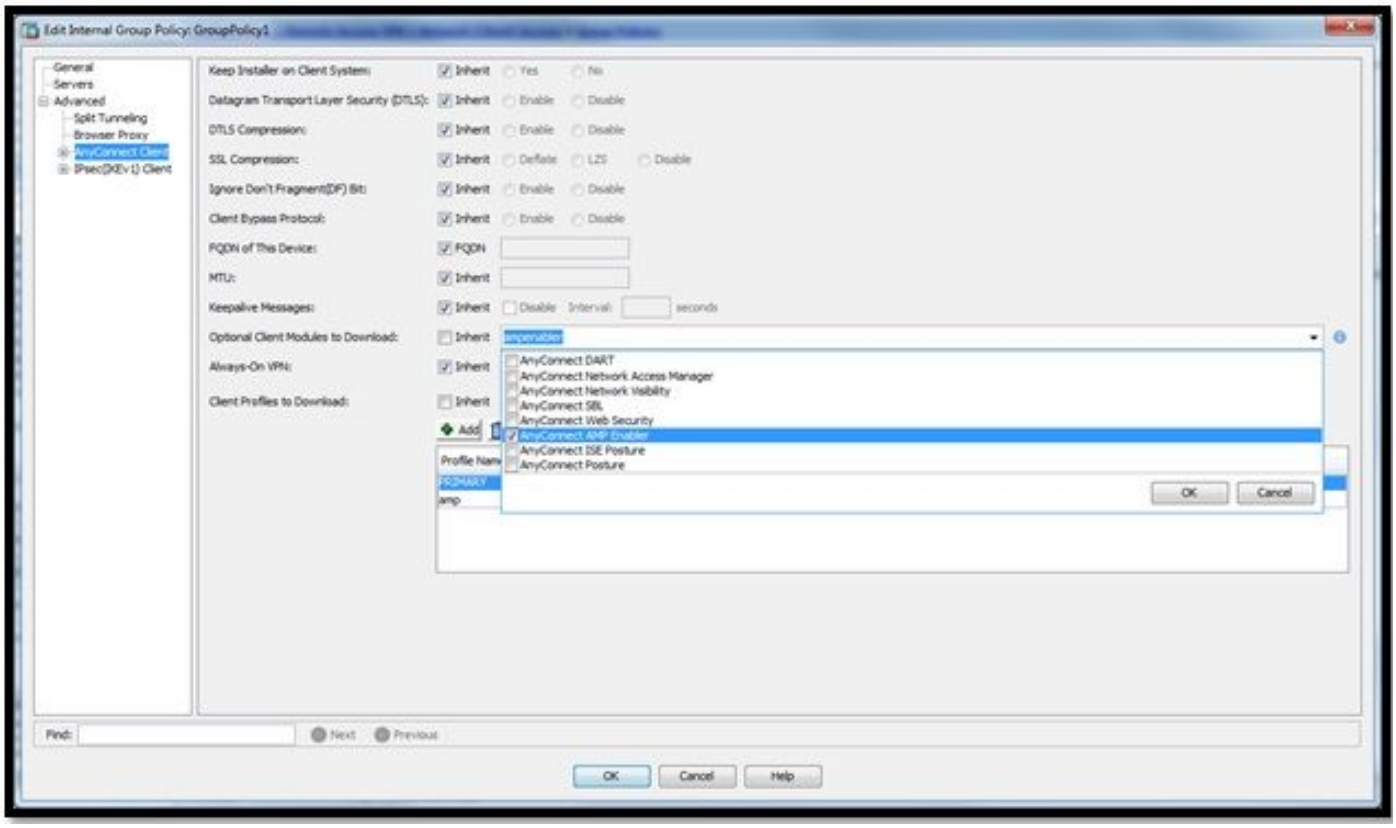
- انتقل إلى **التكوين > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > AnyConnect Client Profile**.
- إضافة **ملف تعريف خدمة تمكين AMP**.





الخطوة 2: تحرير سياسة المجموعة لتنزيل AnyConnect AMP Enabler

- انتقل إلى التكوين > إزالة Access VPN > نهج المجموعة > تحرير.
- انتقل إلى خيارات متقدمة > AnyConnect Client (عميل AnyConnect) > وحدات العميل الاختيارية لتنزيلها.
- أختر أداة تمكين AnyConnect AMP.



الخطوة 3: تنزيل نهج FireAMP

ملاحظة: قبل المتابعة، تحقق مما إذا كان نظامك يفي بمتطلبات AMP لنقاط النهاية ل Windows Connector.

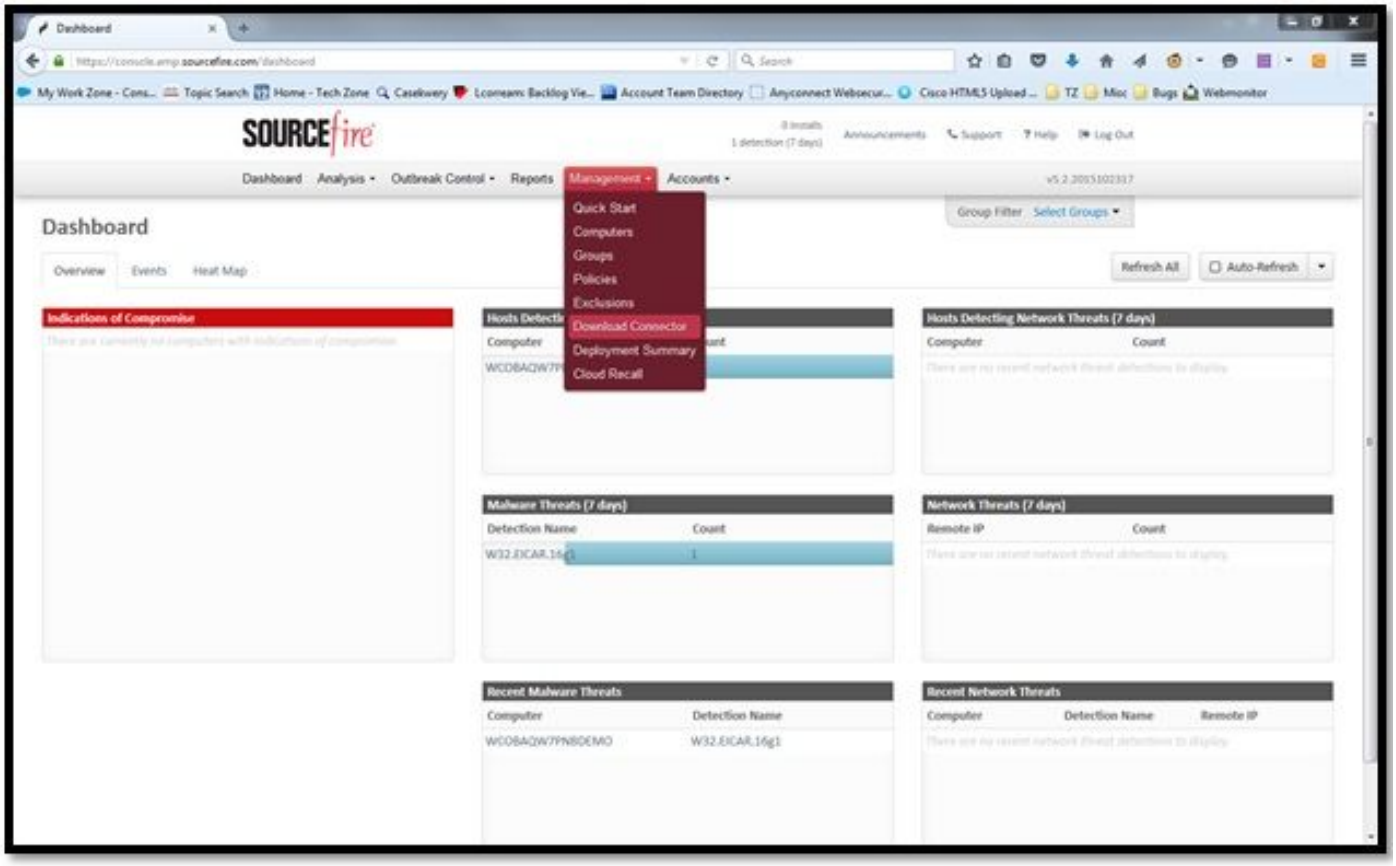
متطلبات النظام ل AMP لنقاط النهاية Windows Connector

هذه هي الحد الأدنى لمتطلبات النظام لموصل FireAMP استنادا إلى نظام التشغيل Windows. يدعم موصل FireAMP كل من الإصدارين 32 و 64 بت لأنظمة التشغيل هذه. يمكن العثور على أحدث وثائق AMP في نشر AMP

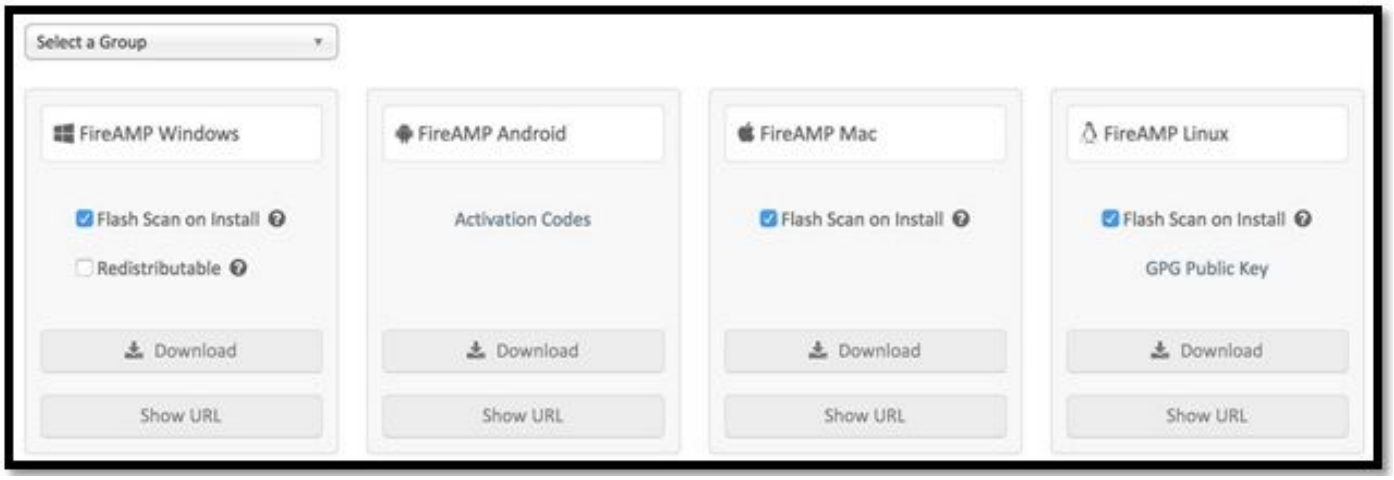
نظام تشغيل	المعالج	ذاكرة	مساحة القرص، وضع السحابة فقط	مساحة القرص
نظام التشغيل Microsoft Windows 7	معالج بسرعة 1 جيجاهرتز أو أسرع	وصول ذاكرة عشوائي (RAM) 1 جيجابايت	مساحة قرص متوفرة 150 ميجابايت - وضع السحابة فقط	مساحة قرص متوفرة 1 جيجابايت - Tetra
Microsoft Windows 8 و 8.1 (يتطلب موصل FireAMP 5.1.3 أو أحدث)	معالج بسرعة 1 جيجاهرتز أو أسرع	وصول ذاكرة عشوائي (RAM) 512 ميجابايت	مساحة قرص متوفرة 150 ميجابايت - وضع السحابة فقط	مساحة قرص متوفرة 1 جيجابايت - Tetra
نظام التشغيل Microsoft Windows Server 2003	معالج بسرعة 1 جيجاهرتز أو أسرع	وصول ذاكرة عشوائي (RAM) 512 ميجابايت	مساحة قرص متوفرة 150 ميجابايت - وضع السحابة فقط	مساحة قرص متوفرة 1 جيجابايت - Tetra
نظام التشغيل Microsoft Windows Server 2008	معالج بسرعة 2 جيجاهرتز أو أسرع	وصول ذاكرة عشوائي (RAM) 2 جيجابايت	مساحة قرص متوفرة 150 ميجابايت - وضع السحابة فقط	مساحة قرص متوفرة 1 جيجابايت - Tetra
Microsoft Windows Server 2012 (يتطلب FireAMP Connector 5.1.3 أو أحدث)	معالج بسرعة 2 جيجاهرتز أو أسرع	وصول ذاكرة عشوائي (RAM) 2 جيجابايت	مساحة قرص متوفرة 150 ميجابايت - وضع السحابة فقط	مساحة قرص متوفرة 1 صلب جيجابايت - Tetra

شائع للغاية وهو وضع أداة تثبيت AMP على خادم الويب الخاص بالمؤسسات.

لتنزيل الموصل، انتقل إلى **الإدارة > تنزيل الموصل**. ثم أختر الكتابة وقم **بتنزيل** FireAMP (Windows و Android و Mac و Linux).



تتيح لك صفحة "تنزيل الموصل" تنزيل حزم التثبيت لكل نوع من موصلات FireAMP. يمكن وضع هذه الحزمة على مشاركة أو توزيعها عبر برنامج الإدارة.



تحديد مجموعة

- **المراجعة فقط:** مراقبة النظام استنادا إلى SHA-256 المحسوب على كل ملف. لا يعمل وضع التدقيق هذا على عزل البرامج الضارة، ولكنه يرسل حدثا كتنبيه.
- **الحماية:** حماية الوضع باستخدام ملفات ضارة العزل. مراقبة نسخ الملفات ونقلها.
- **الفرز:** هذا للاستخدام على جهاز كمبيوتر به خلل/مصاب بالفعل.
- **الخادم:** مجموعة تثبيت لخادم Windows، حيث يتم تثبيت الموصل بدون محرك Tetra وبرنامج تشغيل DFC. تم تصميم هذه المجموعة باستخدام اسمها لخوادم وحدات التحكم غير بالمجال.
- **وحدة التحكم بالمجال:** تم تعيين النهج الافتراضي لهذه المجموعة على وضع التدقيق كما هو الحال في مجموعة الخوادم. قم بإقران كافة خوادم Active Directory في هذه المجموعة، مما يعني أن الموصل سيتم تشغيله على وحدة التحكم بالمجال ل Windows.

هذا ويتمتع هذا الجهاز بميزة تدعى تيترا وهي محرك مضاد للفيروسات بالكامل. هذا الخيار إختياري لكل من.

الميزات

- **ميزة المسح الضوئي عند التثبيت:** يتم تشغيل عملية المسح الضوئي أثناء التثبيت. وهو سريع نسبيا في التنفيذ ويوصى بتشغيله مرة واحدة فقط.
- **قابل لإعادة التوزيع:** يجب تنزيل حزمة واحدة واحدة، تحتوي على مثبتات 32 بت و 64 بت. بدلا من أداة تمهيد تشغيل الكمبيوتر، والتي تكون متوفرة لتترك هذا الخيار غير محدد وتنزيل ملفات أداة التثبيت، بمجرد تنفيذها.

ملاحظة: يمكنك إنشاء مجموعتك الخاصة وتكوين النهج المقترن بها. الغرض هو وضع كافة خوادم Active Directory على سبيل المثال في مجموعة واحدة، حيث يكون النهج في وضع التدقيق.
يتم policy.xml على ملف bootstrapper و redistribution كما يحتوي كل من أداة تثبيت إستخدامه كملف تكوين لموصل AMP.

الخطوة 4: تنزيل ملف تعريف عميل أمان الويب

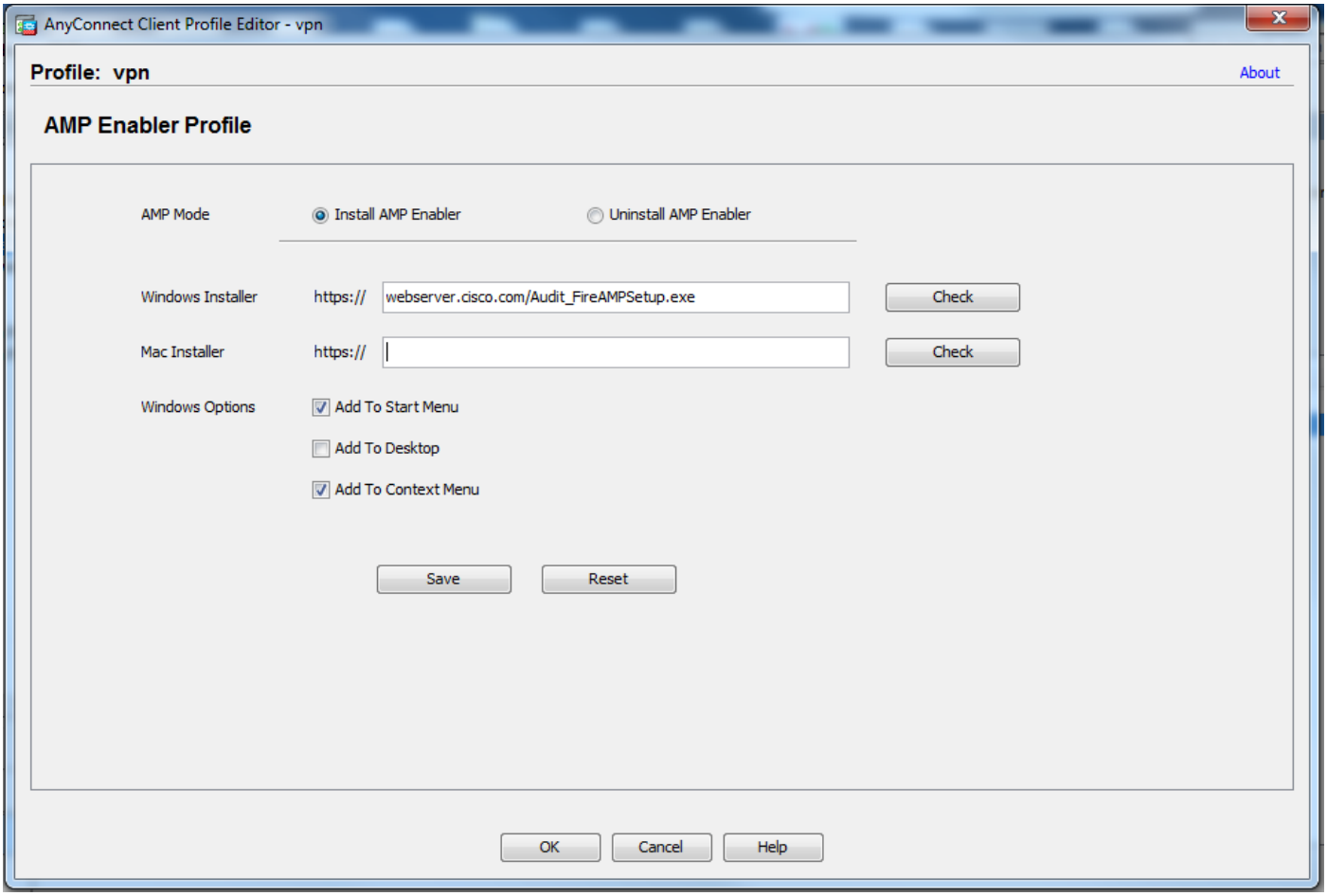
تحديد خادم ويب للشركة أو مشاركة شبكة مع أداة تثبيت AMP. وهو شائع الاستخدام في جميع الشركات لتوفير النطاق الترددي ووضع المثبتات الموثوقة في موقع مركزي.

الرجاء التأكد من أنه يمكن الوصول إلى إرتباط HTTPS على نقاط النهاية بدون أي خطأ في الشهادة وأن الشهادة الأساسية مثبتة في مخزن الأجهزة.

العودة إلى ملف تعريف AMP الذي تم إنشاؤه من قبل على ASA (الخطوة 1) وتحرير **ملف تعريف أداة تمكين AMP**:

1. بالنسبة لوضع AMP، انقر فوق الزر **تثبيت** أداة تمكين AMP Radio.
2. في حقل **Windows Installer**، قم بإضافة IP لخادم الويب والملف ل FireAMP.
3. خيارات نظام التشغيل Windows إختيارية.

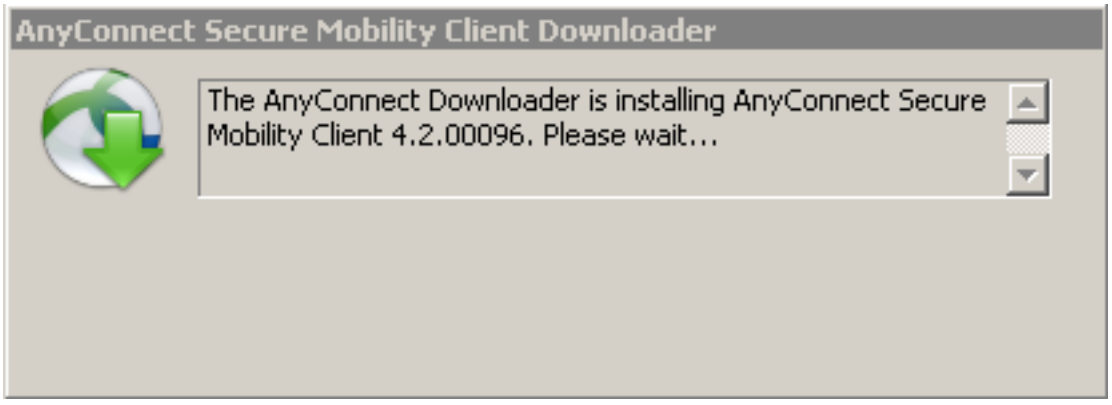
طقطقة **ok** وطبق التغييرات.



الخطوة 5: اتصل ب AnyConnect وتحقق من تثبيت الوحدة النمطية

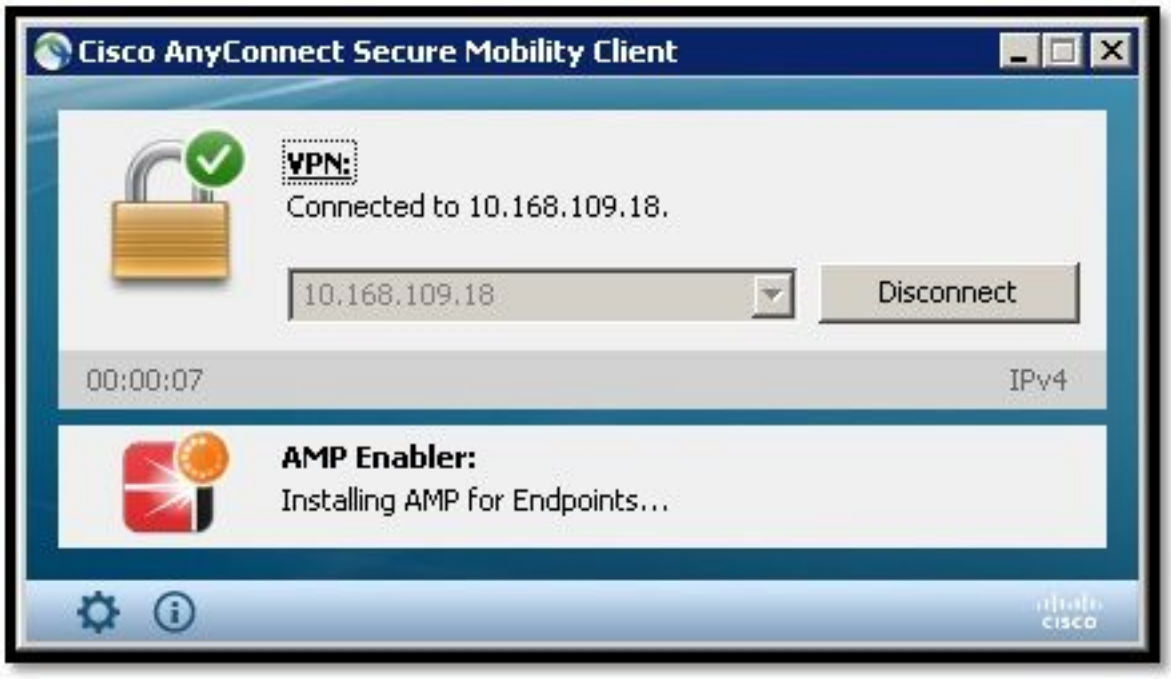
عند اتصال مستخدمي AnyConnect VPN، يقوم ASA بدفع وحدة تمكين AnyConnect AMP من خلال الشبكة الخاصة الظاهرية (VPN). بالنسبة للمستخدمين الذين تم تسجيل دخولهم بالفعل، يوصى بتسجيل الخروج ثم تسجيل الدخول مرة أخرى لتمكين الوظيفة.

```
10:08:29 AM    Establishing VPN session...
10:08:29 AM    The AnyConnect Downloader is performing update checks...
10:08:29 AM    Checking for profile updates...
10:08:29 AM    Checking for product updates...
10:08:31 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 48%
10:08:32 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 91%
10:08:33 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 100%
```



الخطوة 6: أداة تمكين تثبيت اتصال VPN من Start و AMP موصل

ام إن يضغط أنت الزر يربط أن يبدأ ال VPN، وه ينزل الجديد تنزيل وحدة نمطية. سيتضمن هذا أداة تمكين AMP ويقوم بتنزيل حزمة AMP من مسار عنوان URL الذي حددته قبل خطوتين.




```
If you look at the event viewer:

AMP enabler install:
Date         : 04/24/2017
Time         : 10:08:34
Type         : Information
Source       : acvpndownloader

Description : Cisco AnyConnect Secure Mobility Client Downloader (2) exiting, version 4.4.01054
, return code 0 [0x00000000]
```

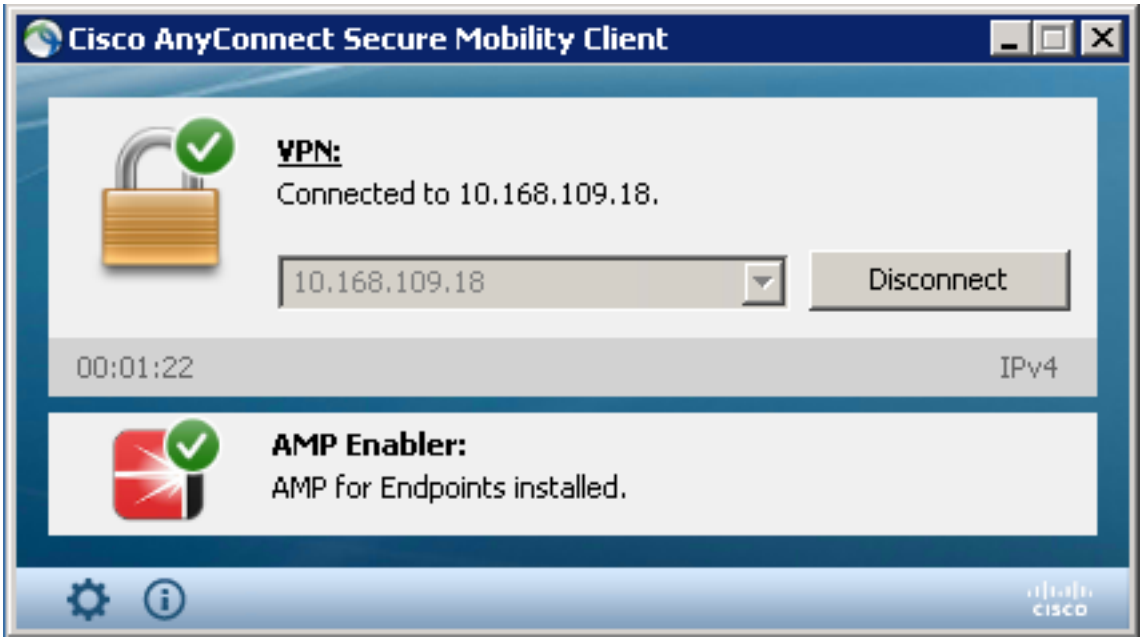
الخطوة 7: تحقق من AnyConnect وتحقق من تثبيت كل شيء

بمجرد توصيل الشبكة الخاصة الظاهرية (VPN) وتثبيت تكوين خادم الويب، تحقق من AnyConnect وتحقق من تثبيت كل شيء بشكل صحيح.

في services.msc يمكنك العثور على خدمة جديدة تسمى CiscoAMP_5.1.3. في أمر PowerShell نرى:

```
PS C:\Users\winUser348> Get-Service -name "*CiscoAMP*"

Status   Name               DisplayName
------   ----               -----------
Running  CiscoAMP_5.1.3     Cisco AMP for Endpoints Connector 5...
```



يضيف مثبت AMP برامج تشغيل جديدة إلى نظام التشغيل Windows. قد تستخدم الأمر driveQuery لسرد المرادفات.

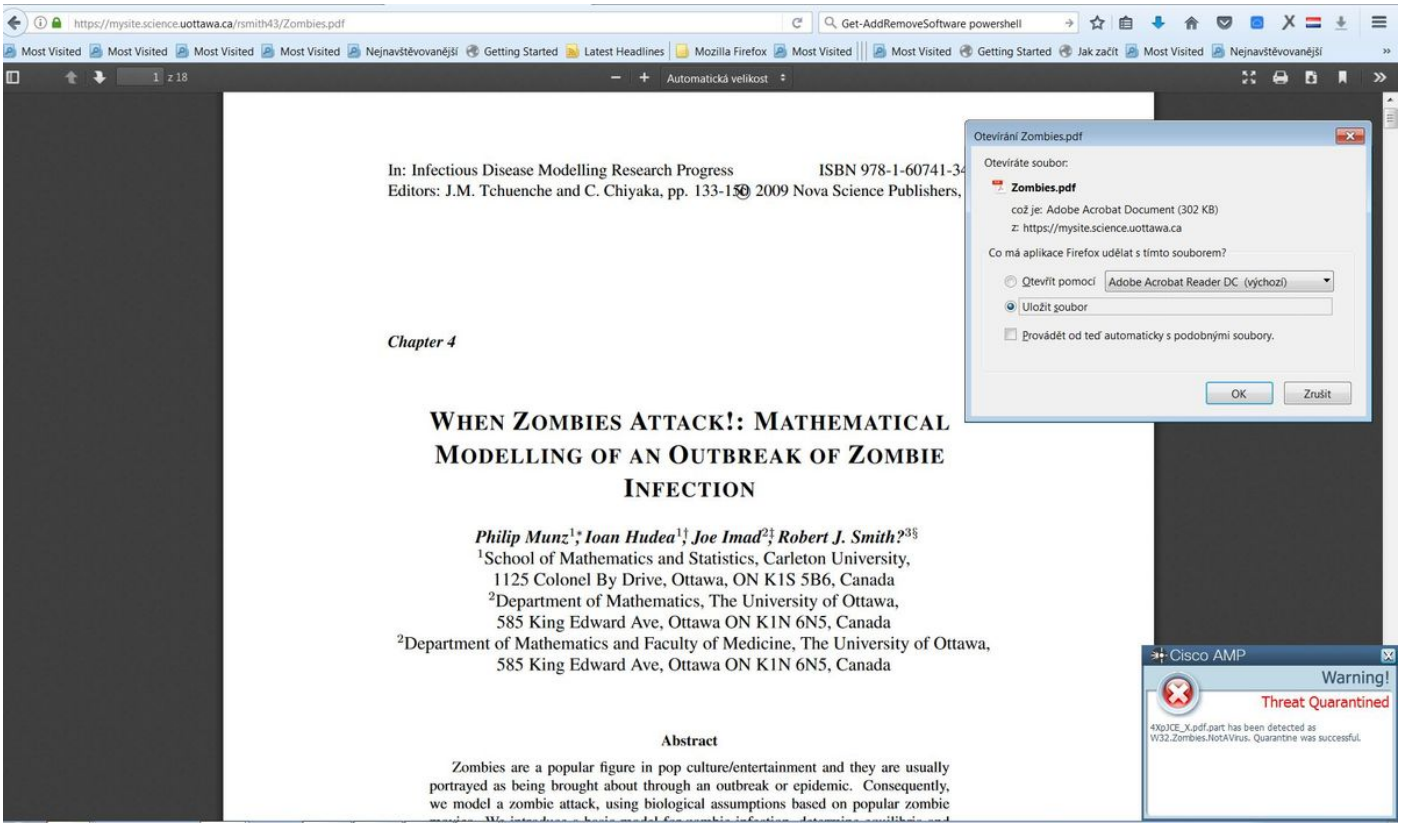
```
C:\Windows\System32>driverquery /v | findstr immunet

ImmunetProte ImmunetProtectDriver   ImmunetProtectDriver   File System   System     Running
OK           TRUE         FA
LSE          4,096       69,632      0       3/17/2017 5:04:20 PM
\??\C:\WINDOWS\System32\Drivers\immunetprotect.s 8,192

ImmunetSelfP ImmunetSelfProtectDriv ImmunetSelfProtectDriv File System   System     Running
OK           TRUE         FA
LSE          4,096       28,672      0       3/17/2017 5:04:08 PM
\??\C:\WINDOWS\System32\Drivers\immunetselfprote 8,192
```

الخطوة 8: اختبر باستخدام سلسلة eicar المتضمنة في ملف Zombies PDF

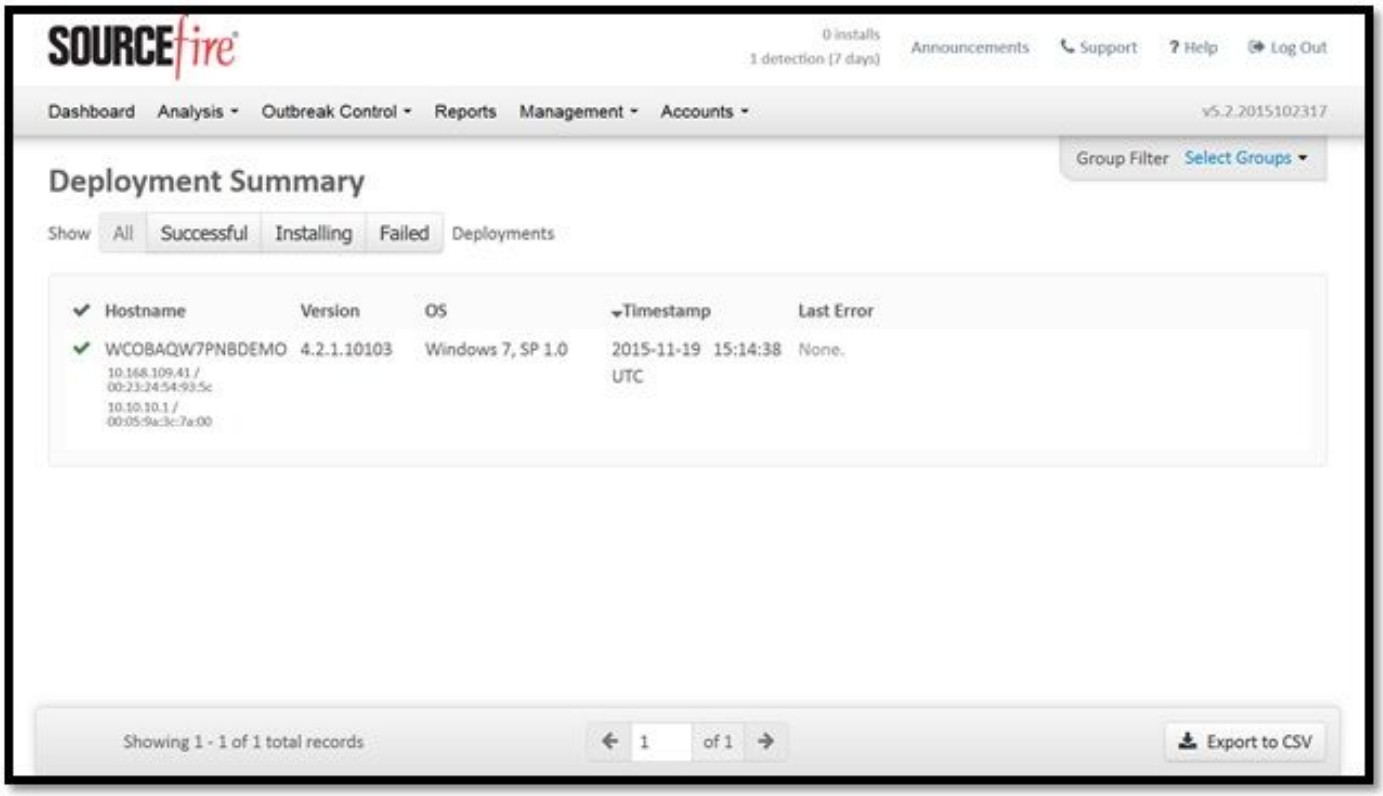
قم بالاختبار باستخدام سلسلة إيكار موجودة في ملف Zombies PDF في حاسب إختباري للتحقق من عزل الملف الضار.



يحتوي Zombies.pdf على سلسلة إيكار

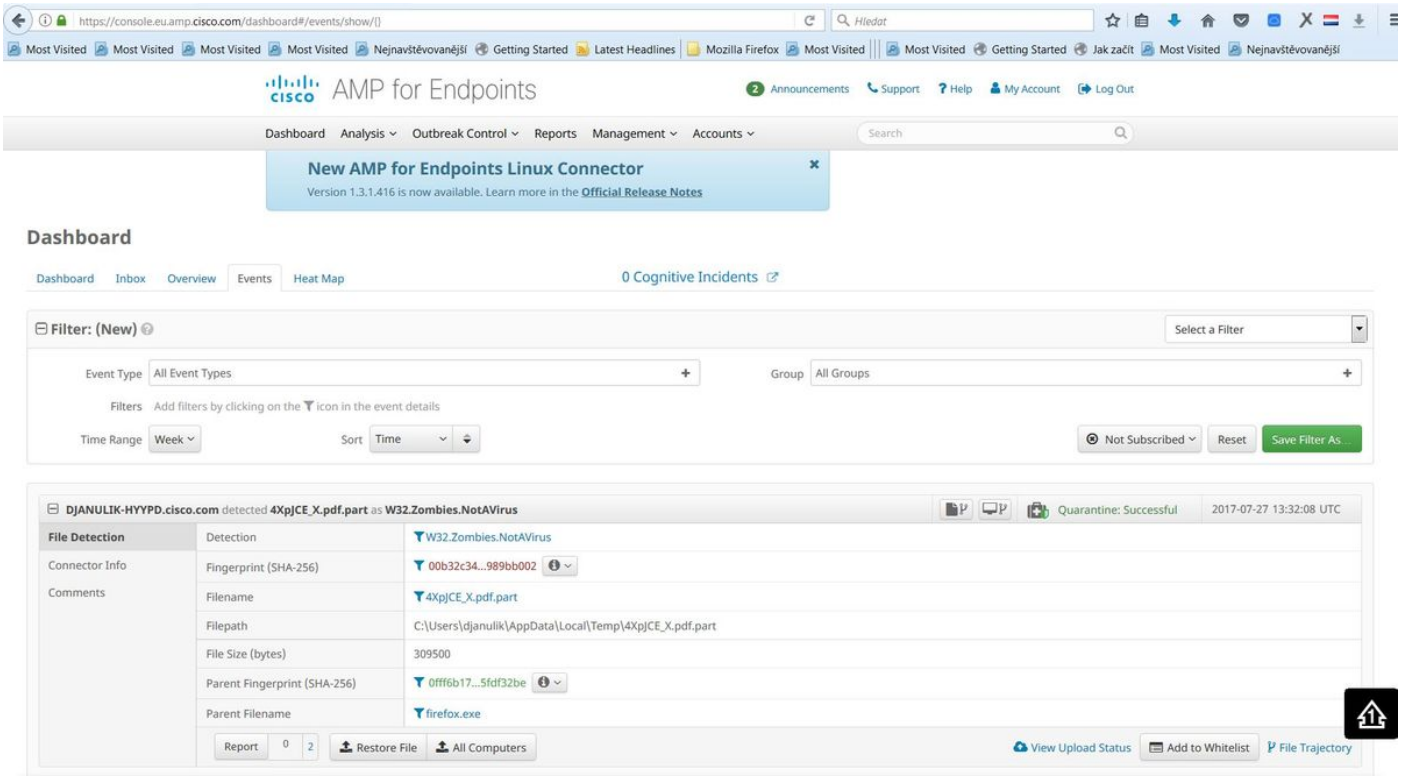
الخطوة 9: ملخص النشر

تظهر لك هذه الصفحة قائمة بعمليات تثبيت موصلات FireAMP الناجحة والفاشلة بالإضافة إلى تلك قيد التقدم حاليا. يمكنك الانتقال إلى **الإدارة > ملخص النشر**.



الخطوة 10: التحقق من اكتشاف مؤشرات التراب

قام Zombies.pdf بتشغيل حدث عزل، قم بإرسال إلى لوحة معلومات AMP.



حدث العزل

معلومات إضافية

للحصول على حساب AMP الخاص بك، يمكنك التسجيل في جامعة ATS. يمنحك هذه نظرة عامة على وظائف AMP في Lab.

معلومات ذات صلة

- تكوين أداة تمكين AMP
- 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).