Instalación y configuración del módulo AMP a través de AnyConnect 4.x y del Enabler AMP

Contenido

Introducción

Este documento pasa con los pasos instalar el conector avanzado de la protección de Malware (AMP) con AnyConnect.

El Enabler de AnyConnect AMP se utiliza como media para desplegar el AMP para las puntos finales. Sí mismo no tiene ninguna capacidad para condenar la disposición del fichero. Empuja el AMP para el software de las puntos finales a una punto final del ASA. Una vez que el AMP está instalado utiliza la capacidad de la nube de controlar para saber si hay disposición de los ficheros. El servicio adicional AMP puede someter los ficheros a ThreatGrid llamado análisis dinámico, para anotar el comportamiento de los ficheros el desconocido. Estos ficheros se pueden condenar como malévolos si se resuelven ciertos artefactos. Esto es extensamente útil para los ataques del zero-day.

Prerrequisitos

Requisitos

- Versión de cliente segura 4.x de la movilidad de AnyConnect
- FireAMP/AMP para las puntos finales
- Versión 7.3.2 o posterior adaptante del Administrador de dispositivos de seguridad (ASDM)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad adaptante (ASA) 5525 con la versión de software 9.5.1
- Cliente seguro 4.2.00096 de la movilidad de AnyConnect en Microsoft Windows 7 64-bit profesionales
- Versión 7.5.1(112) ASDM

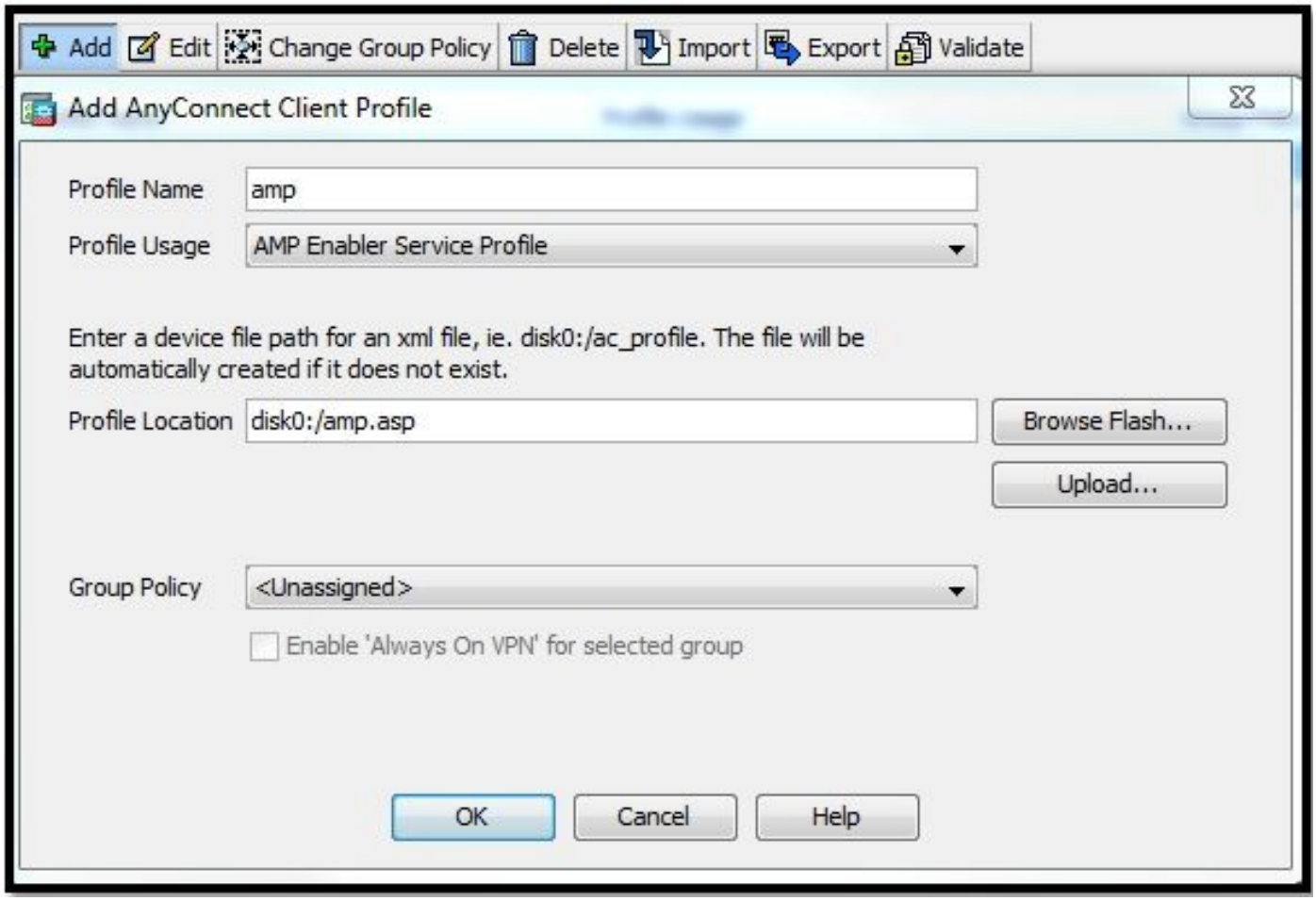
Despliegue de AnyConnect para el Enabler AMP a través del ASA

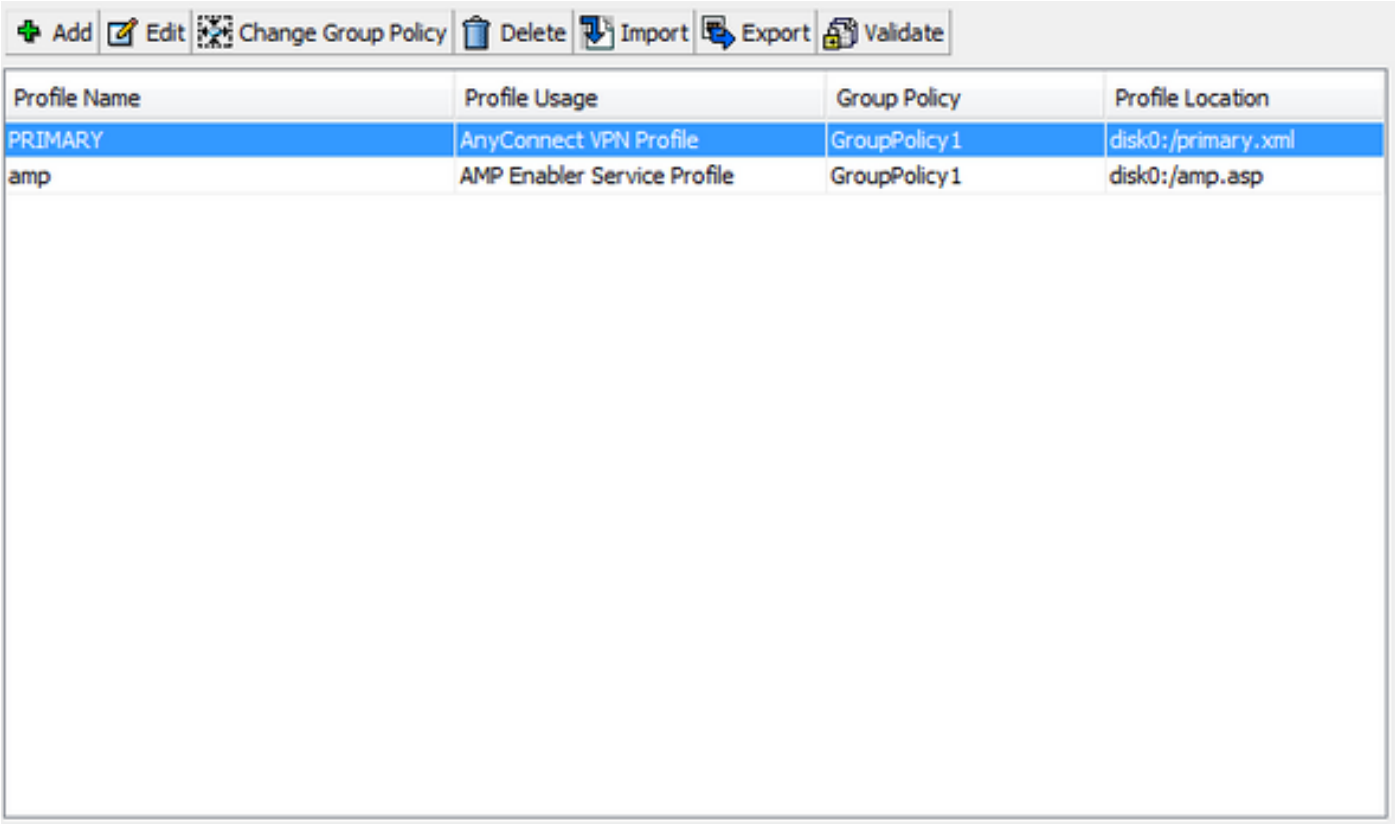
Los pasos implicados en la configuración son como sigue:

- Configure el perfil del cliente del Enabler de AnyConnect AMP.
- Corrija la directiva del grupo de AnyConnect VPN y descargue el perfil del servicio del Enabler AMP.
- Ábrase una sesión al panel AMP para conseguir el link de la transferencia directa del conector URL.
- Verifique la instalación en la máquina del usuario.

Paso 1: Configure el perfil del cliente del Enabler de AnyConnect AMP

- Navegue a la **configuración > al acceso del VPN de acceso remoto > de la red (cliente) > al perfil del cliente de AnyConnect**.
- Agregue el **perfil del servicio del Enabler AMP**.

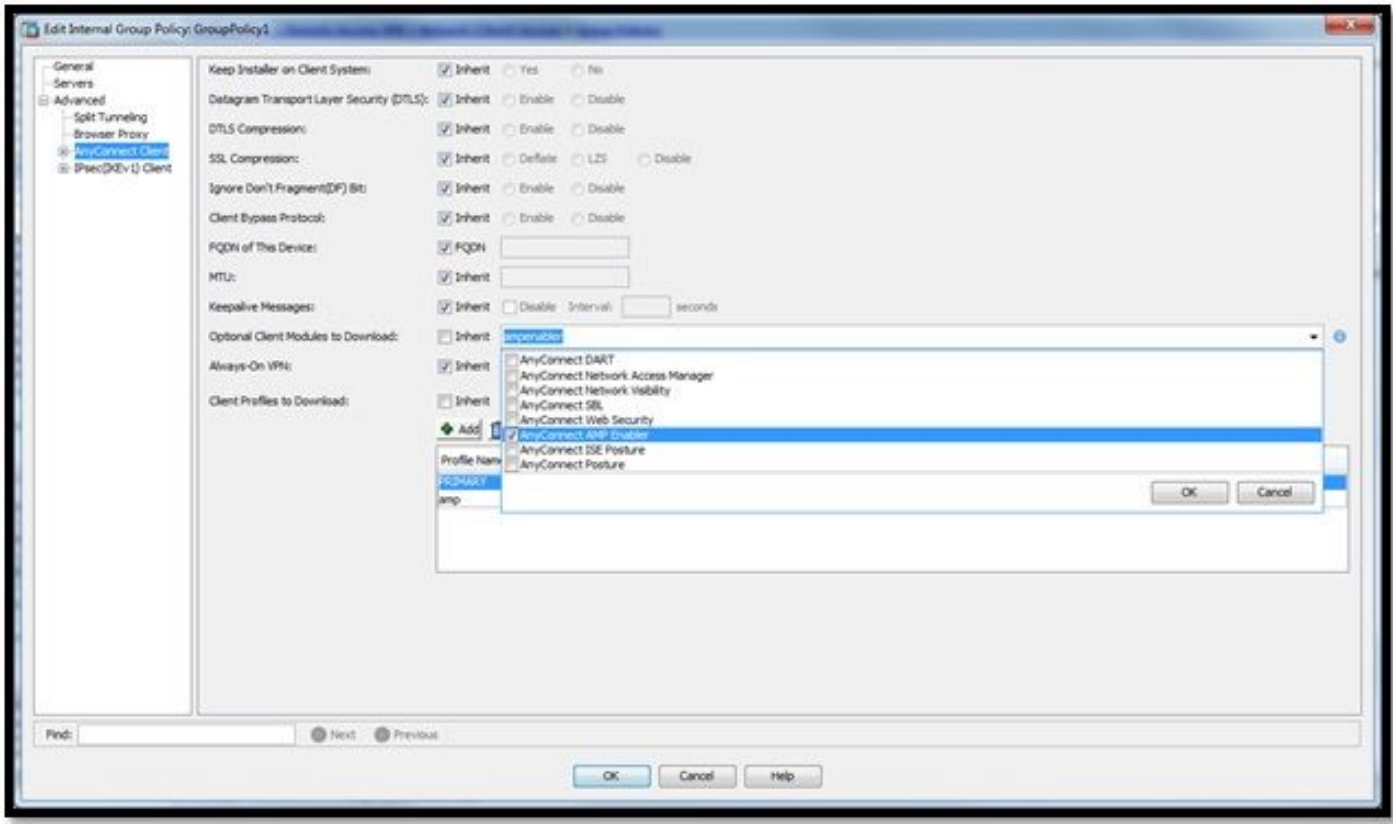




Paso 2: Corrija la Grupo-directiva para descargar el Enabler de AnyConnect AMP

- Navegue a la **configuración > quitan el acceso VPN > las directivas del grupo > corrigen**.
- Va a **avanzado > el cliente de AnyConnect > los módulos cliente opcionales a descargar.**

- Elija el **Enabler de AnyConnect AMP.**



Paso 3: Descargue la directiva de FireAMP

> **Note**: Antes de que usted proceda, controle si su sistema cumple los requisitos para el AMP del conector de Windows de las puntos finales.

Requisitos de sistema para el AMP para el conector de Windows de las puntos finales

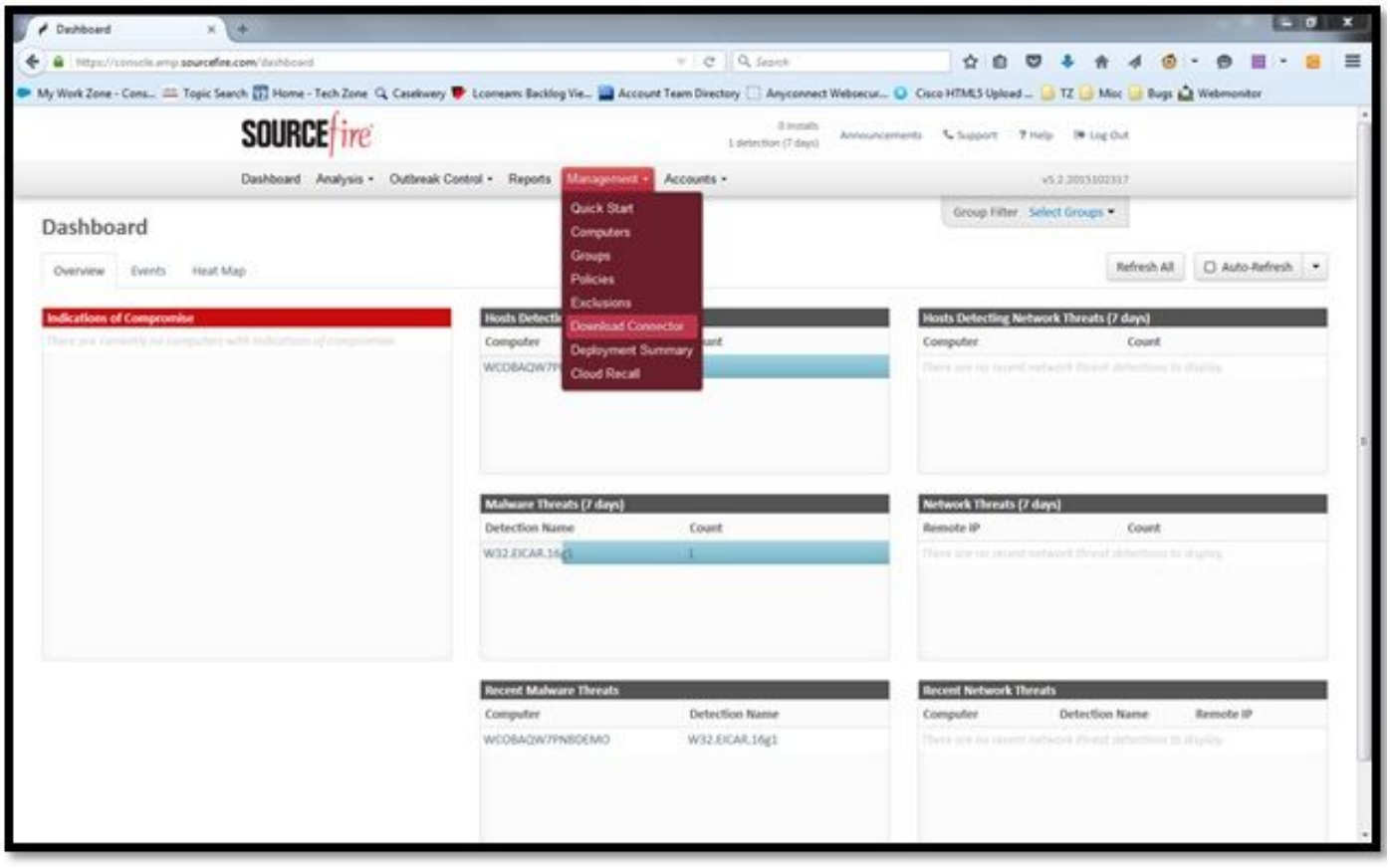
Éstos son los requisitos mínimos del sistema para el conector de FireAMP basado en el sistema operativo Windows. El conector de FireAMP utiliza las versiones de 32 bits y 64-bit de estos sistemas operativos. La última documentación AMP se puede encontrar en el despliegue AMP

Sistema operativo	Procesador	Memoria	Espacio de disco, Modo de la nube solamente	Espacio de disco
Microsoft Windows 7	1 gigahertz o un procesador más rápido	RAM 1 GB	Espacio en disco duro disponible del 150 MB - Modo de la nube- solamente	Espacio en disco duro disponible 1GB - TETRA
Microsoft Windows 8 y 8.1 (requiere el conector 5.1.3 de FireAMP o más adelante)	1 gigahertz o un procesador más rápido	RAM DEL 512 MB	Espacio en disco duro disponible del 150 MB - Modo de la nube- solamente	Espacio en disco duro disponible 1GB – TETRA
Microsoft Windows Server	1 gigahertz o un procesador más	RAM DEL 512 MB	Espacio en disco duro disponible	Espacio en disco duro disponible

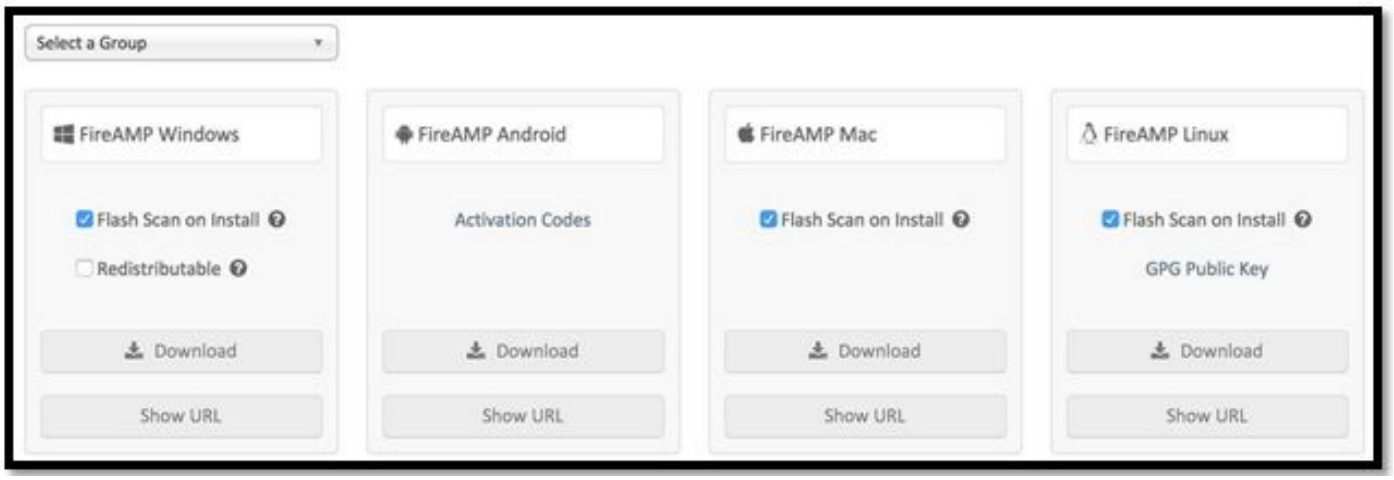
2003	rápido		del 150 MB - Modo de la nube- solamente	1GB - TETRA
Servidor 2008 de Microsoft Windows	2 gigahertz o un procesador más rápido	RAM 2 GB	Espacio en disco duro disponible del 150 MB – Modo de la nube solamente	Espacio en disco duro disponible 1GB – TETRA
Servidor 2012 de Microsoft Windows (requiere el conector 5.1.3 de FireAMP o más adelante)	2 gigahertz o un procesador más rápido	RAM 2 GB	Espacio en disco duro disponible del 150 MB - Modo de la nube solamente	1 GB de espacio en disco duro disponible – TETRA

El más común es tener el instalador AMP colocado en el servidor Web de la empresa.

Para descargar el conector, navegue al **conector de la Administración > de la transferencia directa**. Entonces elija el tipo, y la **transferencia directa** FireAMP (Windows, Android, mac, Linux).



La página del conector de la transferencia directa permite que usted descargue los paquetes del instalar para cada tipo de conector de FireAMP. Este paquete se puede poner en un recurso compartido de red o distribuir vía el software de administración.



Seleccione a un grupo

- **Auditoría solamente:** Vigilar el sistema basado en el SHA-256 calculaba sobre cada fichero. Este modo de la auditoría solamente no quarantine el malware, sino envía un evento como alerta.
- **Proteja:** Modo de protección con los ficheros malévolos de la cuarentena. Vigile la copia de archivo y muévase.
- **Clasificación:** Esto está para el uso en el ordenador ya comprometido/infectado.
- **Servidor:** Habitación de la instalación para el Servidor Windows, en donde el conector instala sin el tetra motor y el driver DFC. Su nombre para los servidores del regulador del no-dominio diseña a este grupo.
- **Regulador del dominio:** La directiva predeterminada para este grupo se fija al modo de auditoría como en el grupo de servidores. Asocie a todos sus servidores Active Directory en este grupo, ese significa que el conector se ejecutará en un regulador del Dominio de Windows.

El AMP tiene la característica llamada TETRA, que es motor lleno del antivirus. Esta opción es opcional por la directiva.

Características

- **La exploración de destello encendido instala:** Funcionamientos del proceso de la exploración durante la instalación. Es relativamente rápido realizarse y recomendado ejecutarse solamente una vez.
- **Redistributable:** Usted debe descargar un solo paquete, que contiene los instaladores de 32 bits y 64-bit. Bastante que un bootstrapper, que está disponible dejando esta opción unticked y descarga los ficheros del instalador, una vez que estuvo ejecutado.

> **Note**: Usted puede crear a su propio grupo y configurar la directiva asociada a ella. El propósito es colocar toda e.g. los servidores Active Directory en un grupo, donde está la directiva en el modo de auditoría.
> El bootstrapper y el instalador redistributable también ambos contienen un `fichero policy.xml` que se utilice como archivo de configuración para el conector AMP.

Paso 4: Descargue el perfil del cliente de la Seguridad de la red

Especifique el servidor Web de la compañía o un recurso compartido de red con el instalador AMP. Esto es la más de uso general a través de las compañías salvar el ancho de banda y

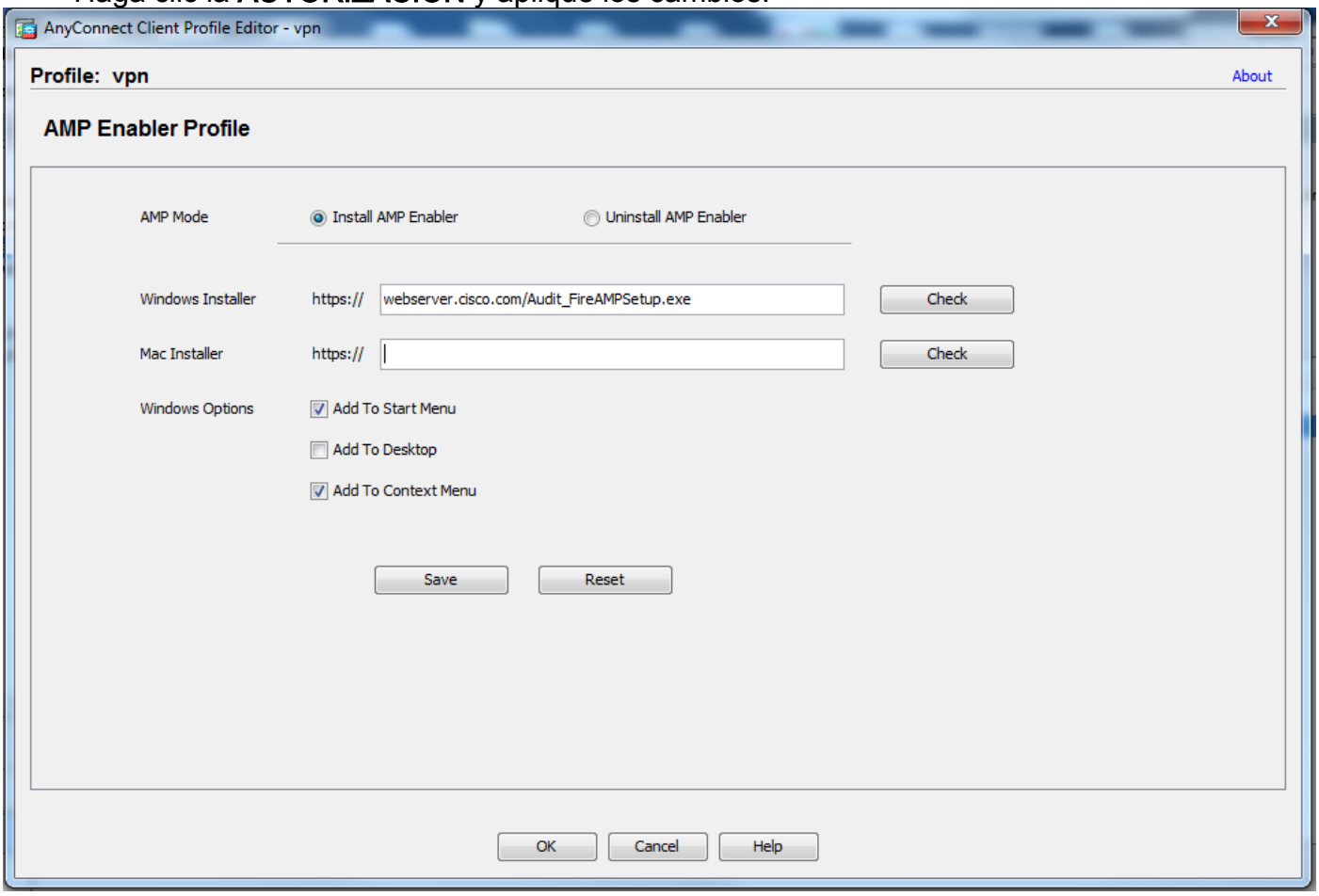
colocar los instaladores de confianza en la ubicación centralizada.

Esté por favor seguro que el link HTTPS se puede alcanzar en las puntos finales sin ningún error del certificado y que el certificado raíz está instalado en el almacén de la máquina.

Vuelva al perfil AMP creado antes en el ASA (el paso 1) y corrige el **perfil del Enabler AMP**:

1. Para el modo AMP, haga clic el botón de radio del **Enabler del instalar AMP**.
2. En el campo del **instalador de Windows**, agregue el IP para el servidor Web y el fichero para el FireAMP.
3. Las opciones de Windows son opcionales.

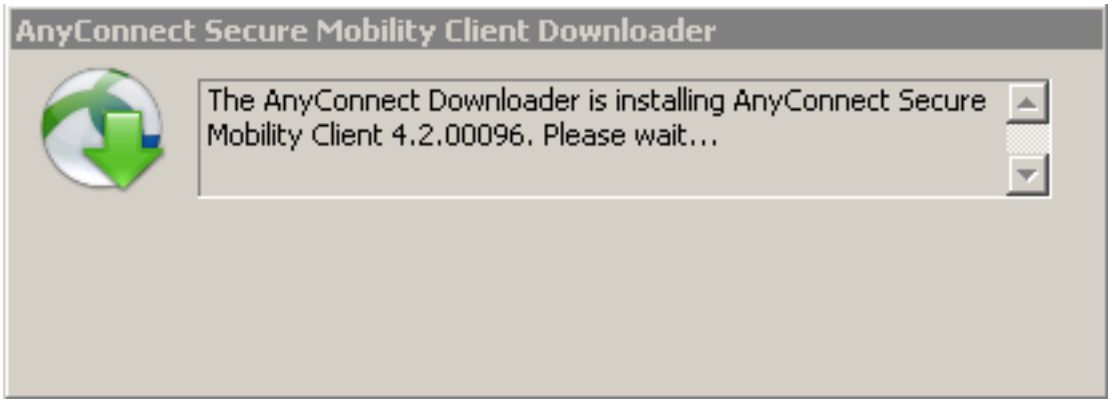
   Haga clic la **AUTORIZACIÓN** y aplique los cambios.



Paso 5: Conecte con AnyConnect y verifique la instalación del módulo

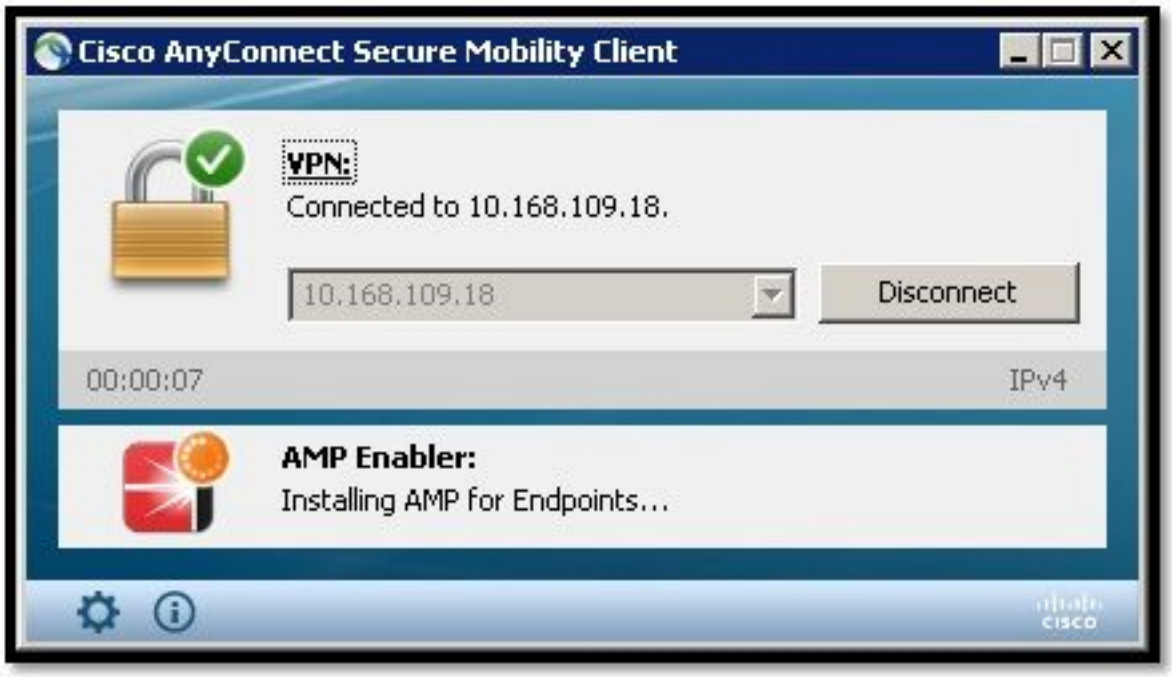
Cuando los usuarios de VPN de Anyconnect conectan, el ASA empuja el módulo del Enabler de AnyConnect AMP con el VPN. Para ya los usuarios autenticados, se recomienda para terminar una sesión y después para abrirse una sesión detrás para que las funciones sean activadas.

```
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%
```



Paso 6: Encienda la conexión VPN para instalar el Enabler AMP y el conector AMP

Una vez que usted golpea el botón conecte para comenzar el VPN, él descarga el nuevo módulo del descargador. Esto tendrá enabler AMP y descarga el paquete AMP del trayecto del URL que usted especificó los pares de los pasos antes.




```
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]
```

Paso 7: Controle AnyConnect y verifique si todo está instalada

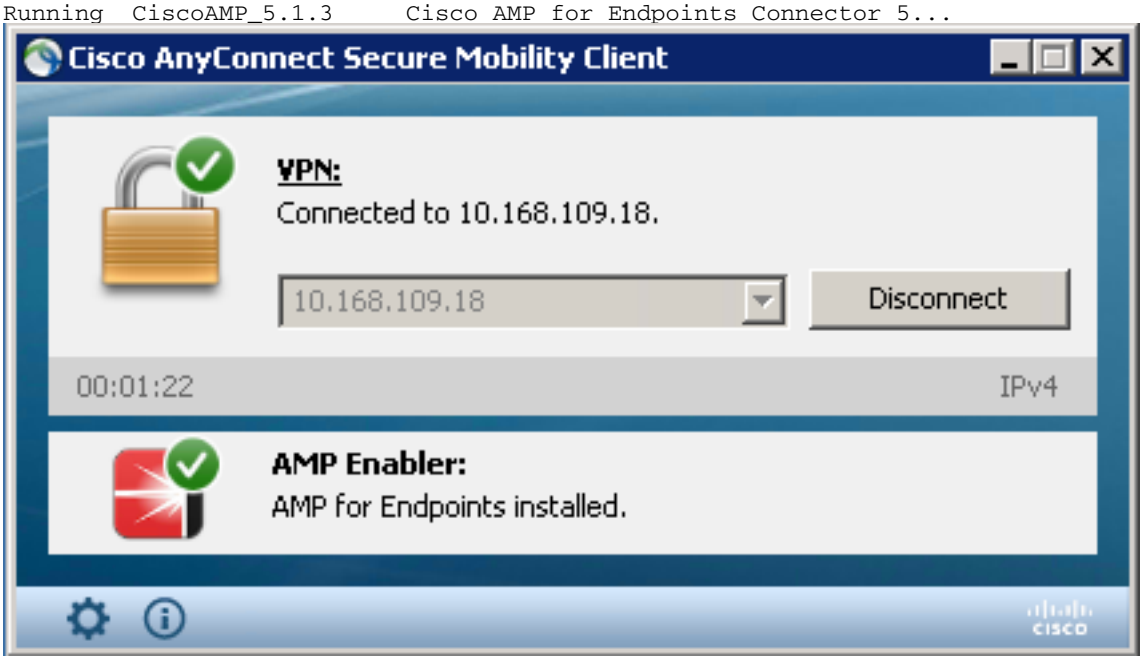
Una vez que el VPN está conectado y la configuración del servidor Web está instalada, controle AnyConnect y verifiqúelo que todo está instalada correctamente.

En el services.msc usted puede encontrar un nuevo servicio llamado CiscoAMP_5.1.3. En el

comando de Powershell vemos:

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

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



El instalador AMP agrega los nuevos drivers al OS (Sistema operativo) Windows. Usted puede ser que utilice el comando del driverquery de enumerar los dirvers.

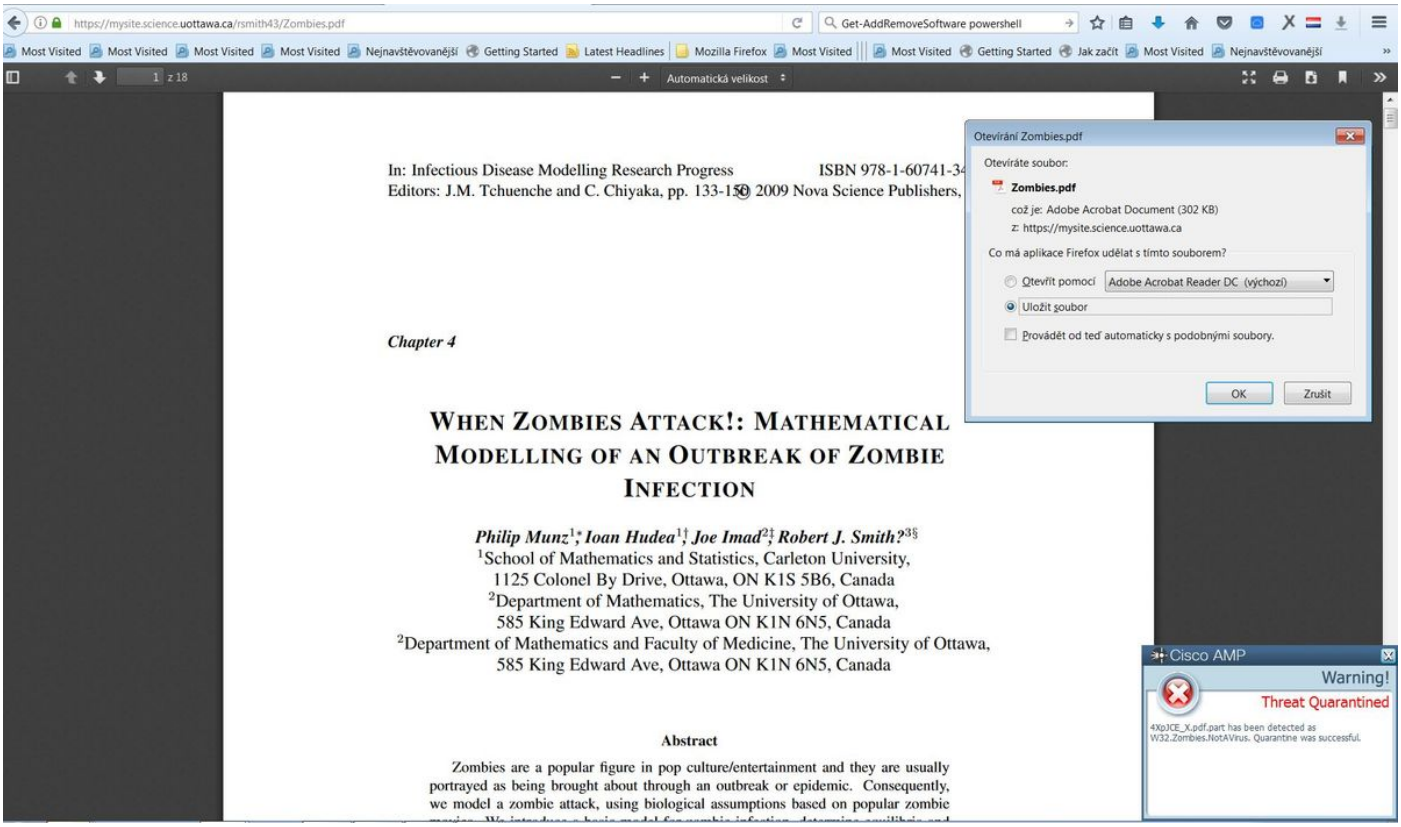
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

Paso 8: Pruebe con una cadena de Eicar contenida en un archivo PDF de los zombis

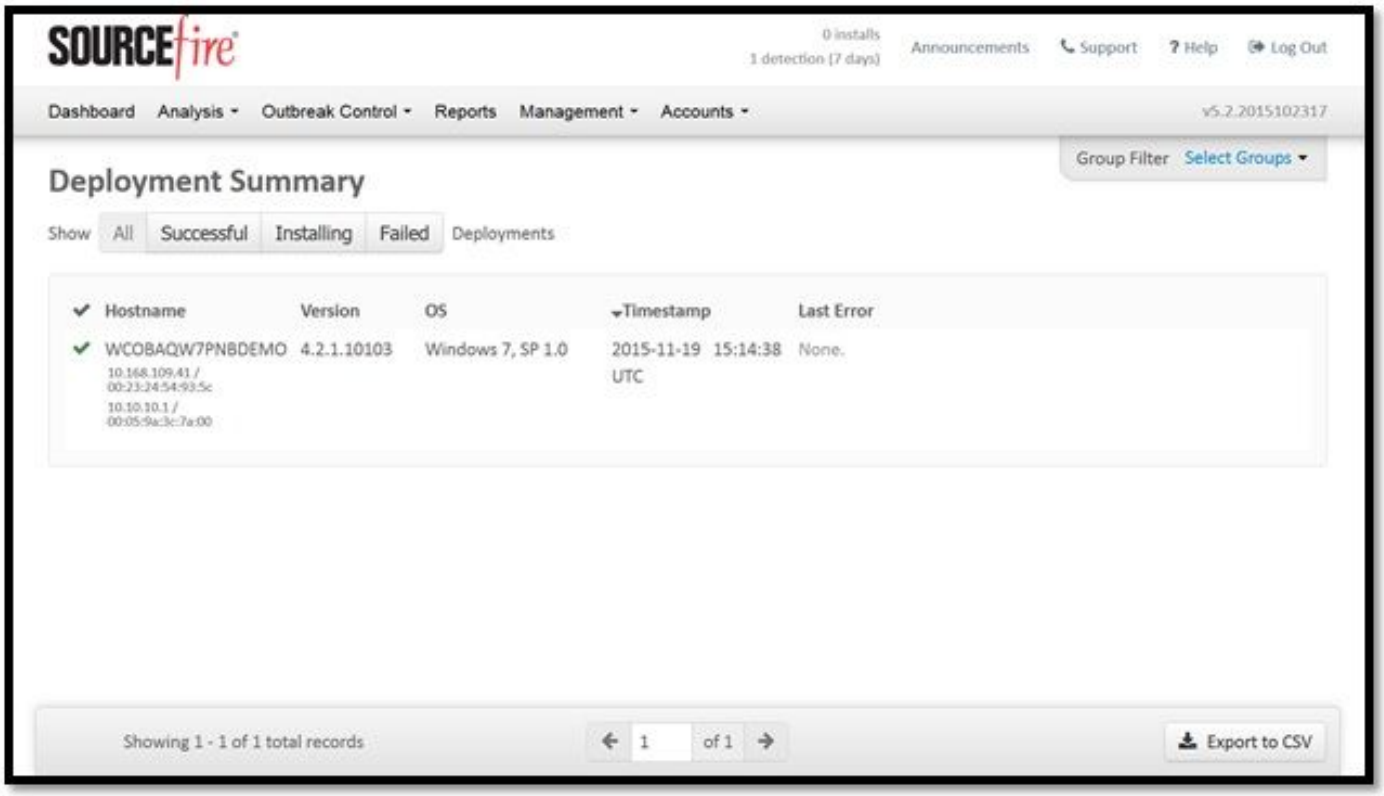
Pruebe con una cadena de Eicar contenida en un archivo PDF de los zombis en un ordenador de la prueba para verificar que el fichero malévolo quarantined.



Zombies.pdf contiene la cadena de Eicar

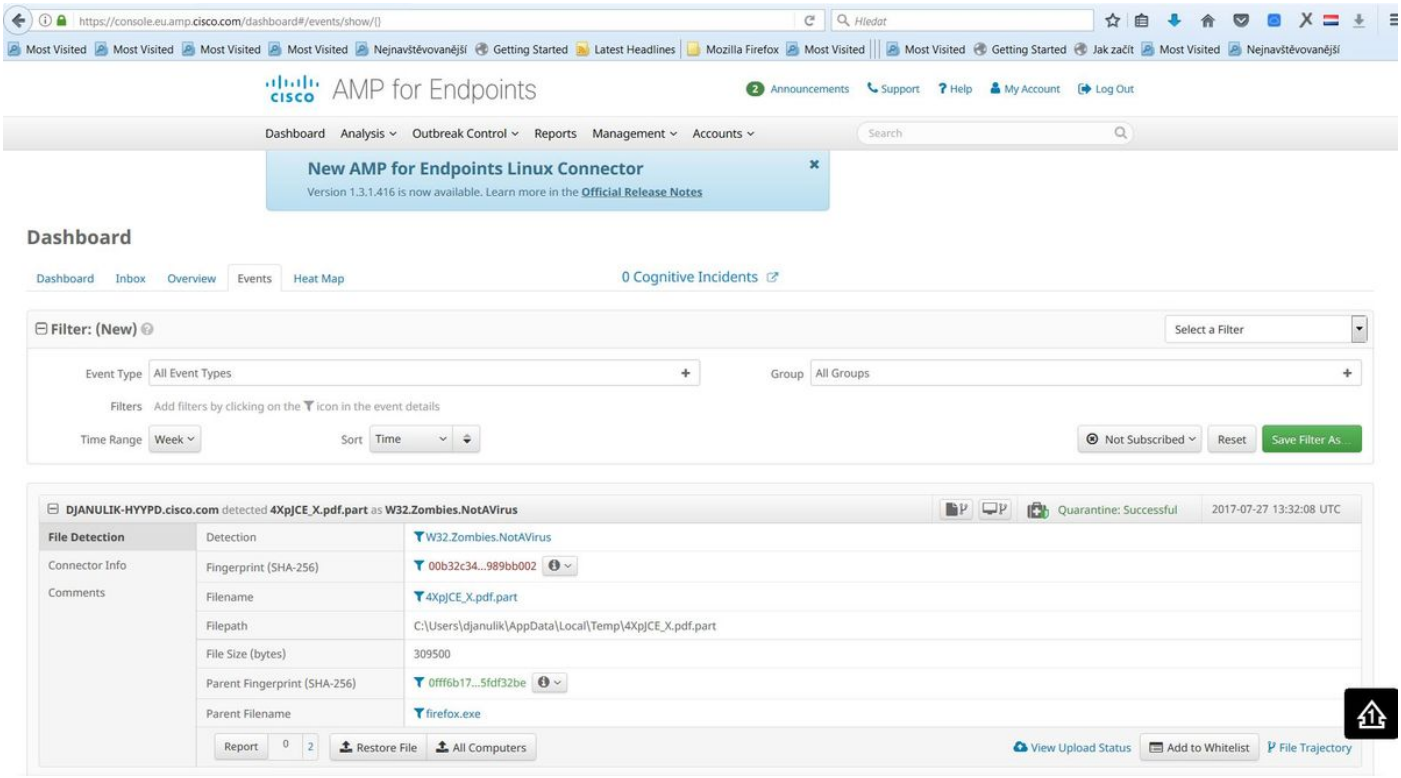
Paso 9: Resumen del despliegue

Esta página le muestra que una lista de acertado y conector fallado de FireAMP instala así como ésos actualmente en curso. Usted puede ir al **resumen de la Administración > del despliegue**.



Paso 10: Verificación de la detección del hilo

Zombies.pdf accionó un evento de la cuarentena, envía al panel AMP.



Evento de la cuarentena

Información adicional

Para conseguir su cuenta AMP, usted puede firmar para arriba para la universidad ATS. Esto le da una descripción de las funciones AMP en el LABORATORIO.

Información Relacionada

- Configure el Enabler AMP
- Soporte Técnico y Documentación - Cisco Systems