A instalação e configuração do módulo AMP com AnyConnect 4.x e AMP Habilitador

Índice

Introdução

Este original atravessa etapas instalar o conector avançado da proteção do malware (AMP) com AnyConnect.

O AnyConnect AMP Habilitador é usado como um media para distribuir o AMP para valores-limite. Próprio não tem nenhuma capacidade de condenar a disposição do arquivo. Empurra o AMP para o software dos valores-limite para um valor-limite do ASA. Uma vez que o AMP é instalado usa a capacidade da nuvem verificar para ver se há a disposição de arquivos. Um serviço mais adicional AMP pode submeter arquivos a ThreatGrid chamado análise dinâmica, para marcar o comportamento dos arquivos do desconhecido. Estes arquivos podem ser condenados como maliciosos se determinados produtos manufaturados são encontrados. Isto é extensamente útil para ataques de zero-dia.

Pré-requisitos

Requisitos

- Versão de cliente segura 4.x da mobilidade de AnyConnect
- FireAMP/AMP para valores-limite
- Versão 7.3.2 ou mais recente adaptável do Security Device Manager (ASDM)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Ferramenta de segurança adaptável (ASA) 5525 com versão de software 9.5.1
- Cliente seguro 4.2.00096 da mobilidade de AnyConnect em 64-bit profissional de Microsoft Windows 7
- Versão 7.5.1(112) ASDM

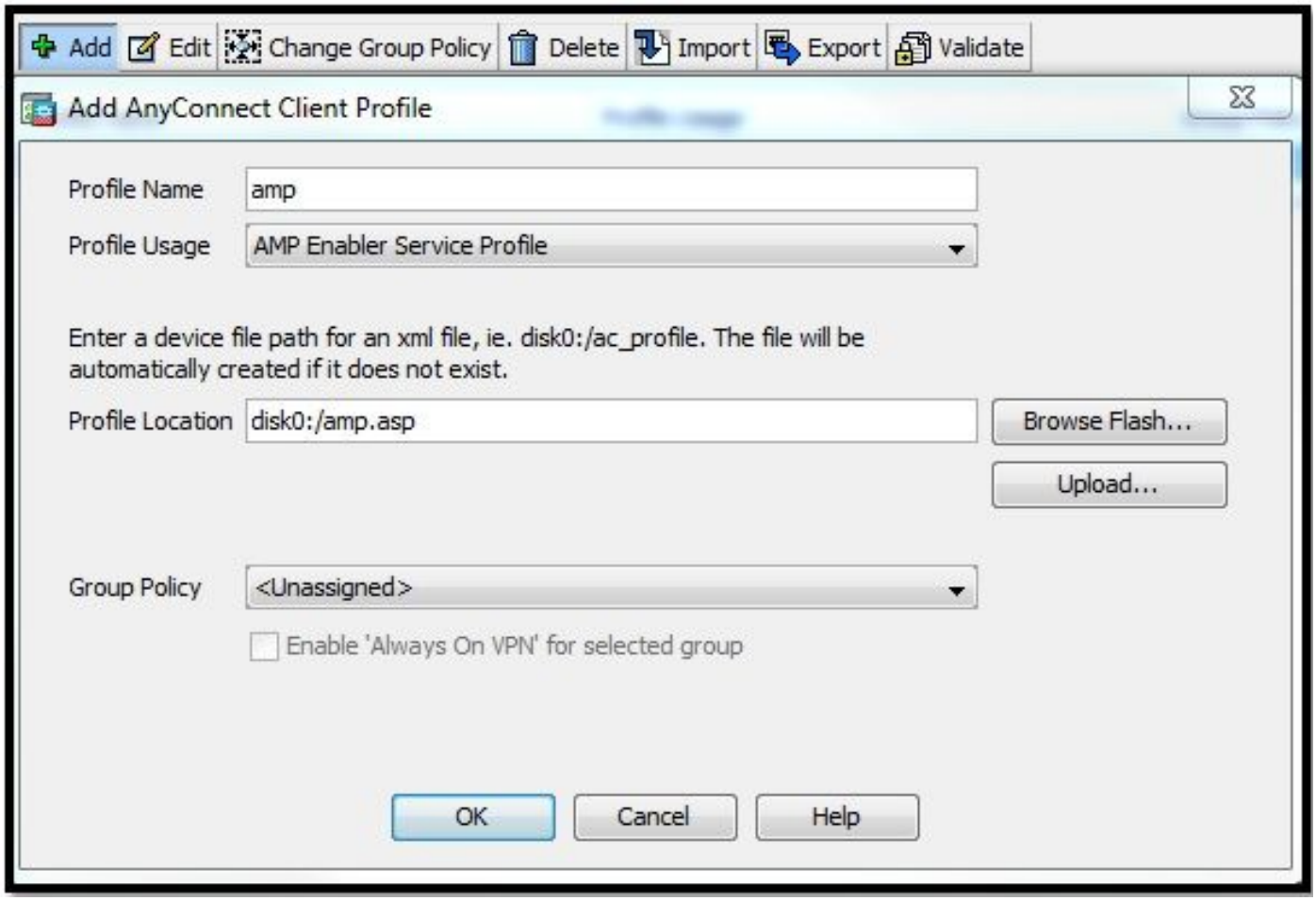
Desenvolvimento de AnyConnect para AMP Habilitador com o ASA

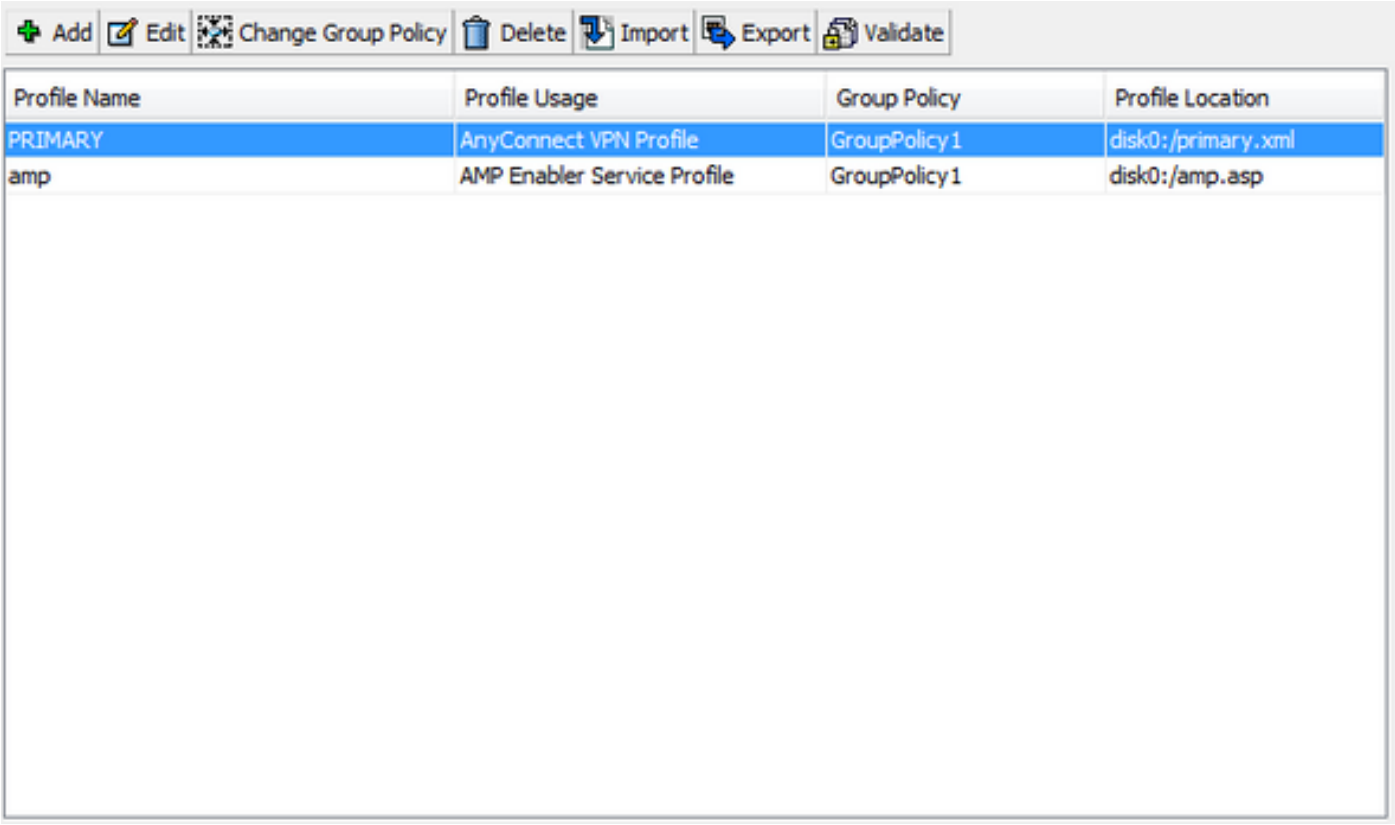
As etapas envolvidas na configuração são como segue:

- Configurar o perfil do cliente de AnyConnect AMP Habilitador.
- Edite a política do grupo de VPN de AnyConnect e transfira o perfil do serviço AMP Habilitador.
- Entre ao painel AMP a fim obter a relação da transferência do conector URL.
- Verifique a instalação na máquina do usuário.

Passo 1: Configurar o perfil do cliente de AnyConnect AMP Habilitador

- Navegue à **configuração > ao acesso do acesso remoto VPN > da rede (cliente) > ao perfil do cliente de AnyConnect**.
- Adicionar o **perfil do serviço AMP Habilitador**.

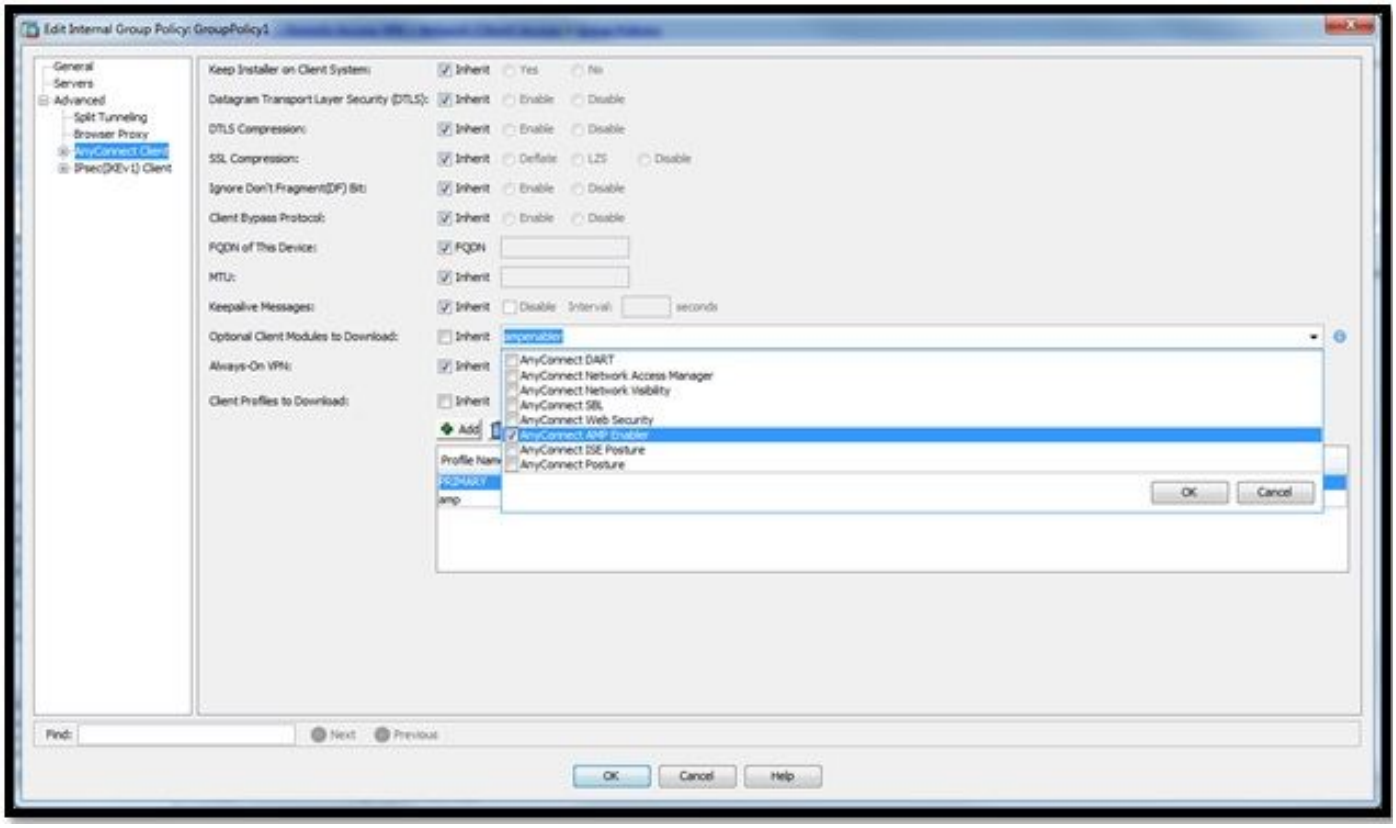




Passo 2: Edite a Grupo-política para transferir o AnyConnect AMP Habilitador

- Navegue à **configuração > removem as políticas do VPN de acesso > do grupo > editam**.
- Vai a **avançado > o cliente de AnyConnect > os módulos opcionais do cliente a transferir.**

- Escolha **AnyConnect AMP Habilitador.**



Passo 3: Transfira a política de FireAMP

> Nota: Antes que você continue, verifique se seu sistema cumpre as exigências para o AMP do conector de Windows dos valores-limite.

Requisitos do sistema para o AMP para o conector de Windows dos valores-limite

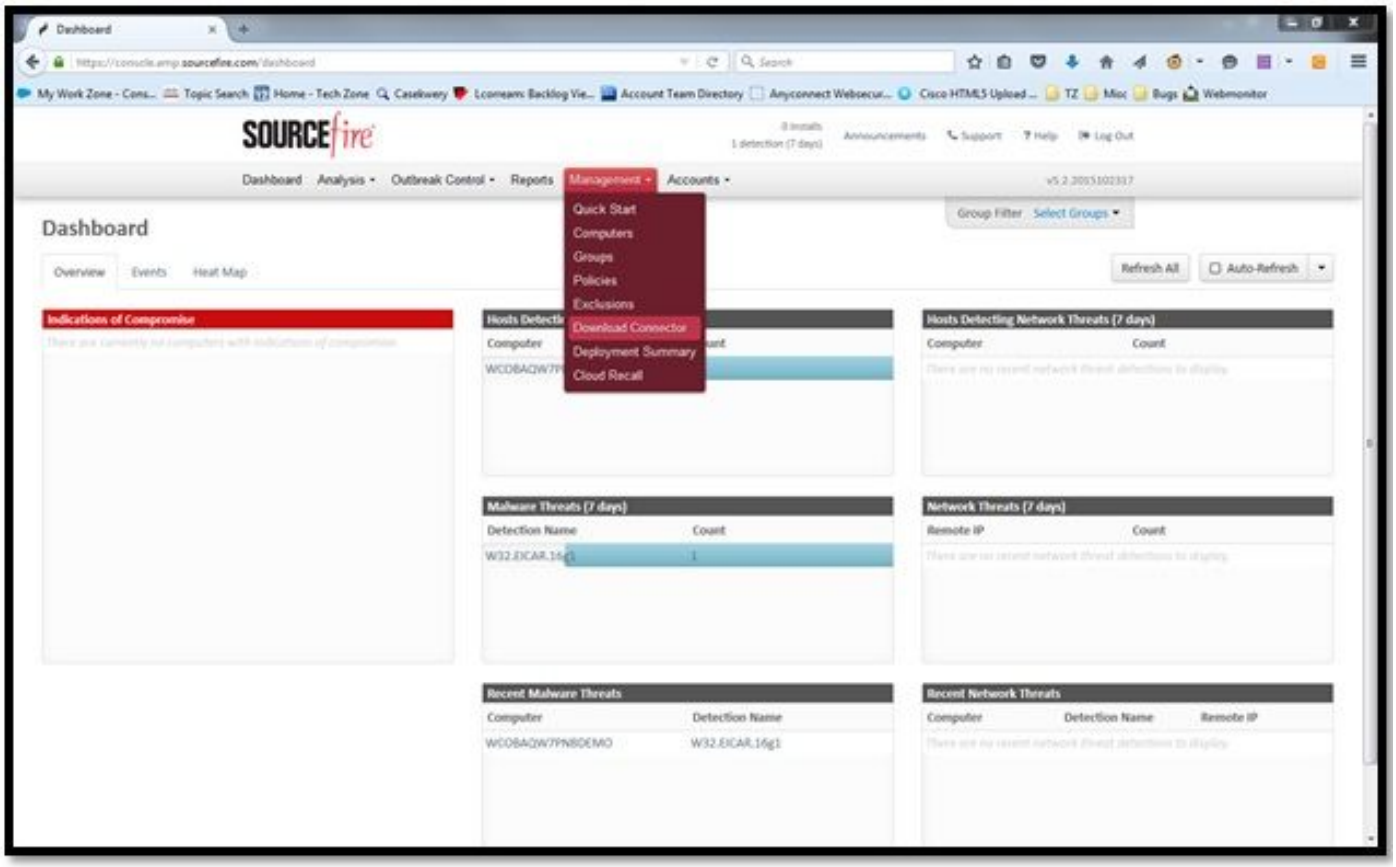
Estes são os requisitos de sistema mínimo para o conector de FireAMP baseado no sistema operacional de Windows. O conector de FireAMP apoia versões de 32 bits e 64-bit destes sistemas operacionais. A documentação a mais atrasada AMP pode ser encontrada no desenvolvimento AMP

Sistema operacional	Processador	Memória	O espaço de disco, Modo da nuvem somente	O espaço de disco
Microsoft Windows 7	1 gigahertz ou processador mais rápido	1 GB RAM	O espaço no disco rígido disponível do 150 MB - Modo da nuvem-somente	O espaço no disco rígido 1GB disponível - TETRA
Microsoft Windows 8 e 8.1 (exige o conector 5.1.3 de FireAMP ou mais atrasado)	1 gigahertz ou processador mais rápido	512 MB RAM	O espaço no disco rígido disponível do 150 MB - Modo da nuvem-somente	O espaço no disco rígido 1GB disponível – TETRA

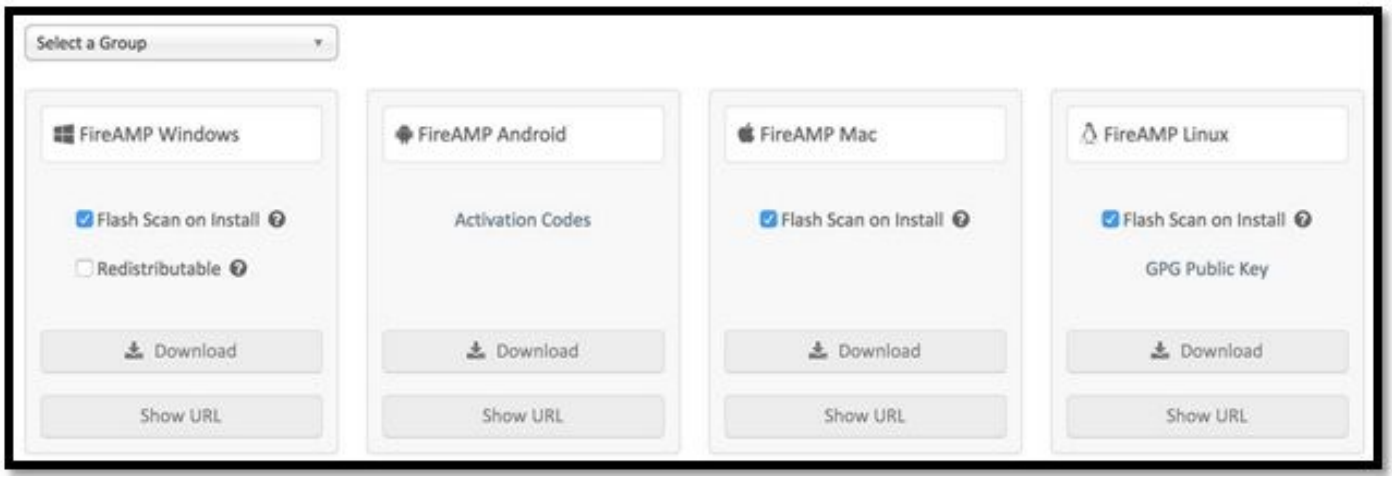
Microsoft Windows Server 2003	1 gigahertz ou processador mais rápido	512 MB RAM	O espaço no disco rígido disponível do 150 MB - Modo da nuvem-somente	O espaço no disco rígido 1GB disponível - TETRA
Microsoft Windows server 2008	2 gigahertz ou processador mais rápido	2 GB RAM	O espaço no disco rígido disponível do 150 MB – Modo da nuvem somente	O espaço no disco rígido 1GB disponível – TETRA
Microsoft Windows server 2012 (exige o conector 5.1.3 de FireAMP ou mais atrasado)	2 gigahertz ou processador mais rápido	2 GB RAM	O espaço no disco rígido disponível do 150 MB - Modo da nuvem somente	1 GB de espaço no disco rígido disponível – TETRA

O mais comum é ter o instalador AMP colocado no servidor de Web da empresa.

A fim transferir o conector, navegue ao **conector do Gerenciamento > da transferência**. Escolha então o tipo, e a **transferência** FireAMP (Windows, Android, Mac, Linux).



A página do conector da transferência permite que você transfira os pacotes da instalação para cada tipo de conector de FireAMP. Este pacote pode ser colocado em uma parte da rede ou ser distribuído através do software de gestão.



Selecione um grupo

- **Auditoria somente:** Monitorar o sistema baseado no SHA-256 calculou sobre cada arquivo. Este modo da auditoria somente não quarantine o malware, mas envia um evento como um alerta.
- **Proteja:** Proteja o modo com arquivos maliciosos da quarentena. Monitore a cópia de arquivo e mova-se.
- **Triagem:** Isto é para o uso computador já comprometido/contaminado.
- **Servidor:** Série da instalação para o server de Windows, aonde o conector instala sem motor Tetra e direcionador DFC. Este grupo é projetado por seu nome para server do controlador do NON-domínio.
- **Controlador de domínio:** A política padrão para este grupo é ajustada ao modo de auditoria como no grupo de servidor. Associe todos seus servidores ative directory neste grupo, esse significa que o conector estará sendo executado em um controlador de domínio de Windows.

O AMP tem a característica chamada TETRA, que é motor completo do antivirus. Esta opção é opcional pela política.

Características

- **A varredura instantânea instala sobre:** Corridas do processo da varredura durante a instalação. É relativamente rápido executar e recomendado ser executado somente uma vez.
- **Redistributable:** Você deve transferir um único pacote, que contém instaladores de 32 bits e 64-bit. Um pouco do que um bootstrapper, que estivesse disponível deixando esta opção unticked e transfere os arquivos do instalador, uma vez que executado.

> Nota: Você pode criar seu próprio grupo e configurar-lhe política associada. A finalidade é colocar toda por exemplo servidores ative directory em um grupo, onde a política reage do modo da auditoria.
> O bootstrapper e o instalador redistributable igualmente ambos contêm um `arquivo policy.xml` que seja usado como um arquivo de configuração para o conector AMP.

Passo 4: Transfira o perfil do cliente da Segurança da Web

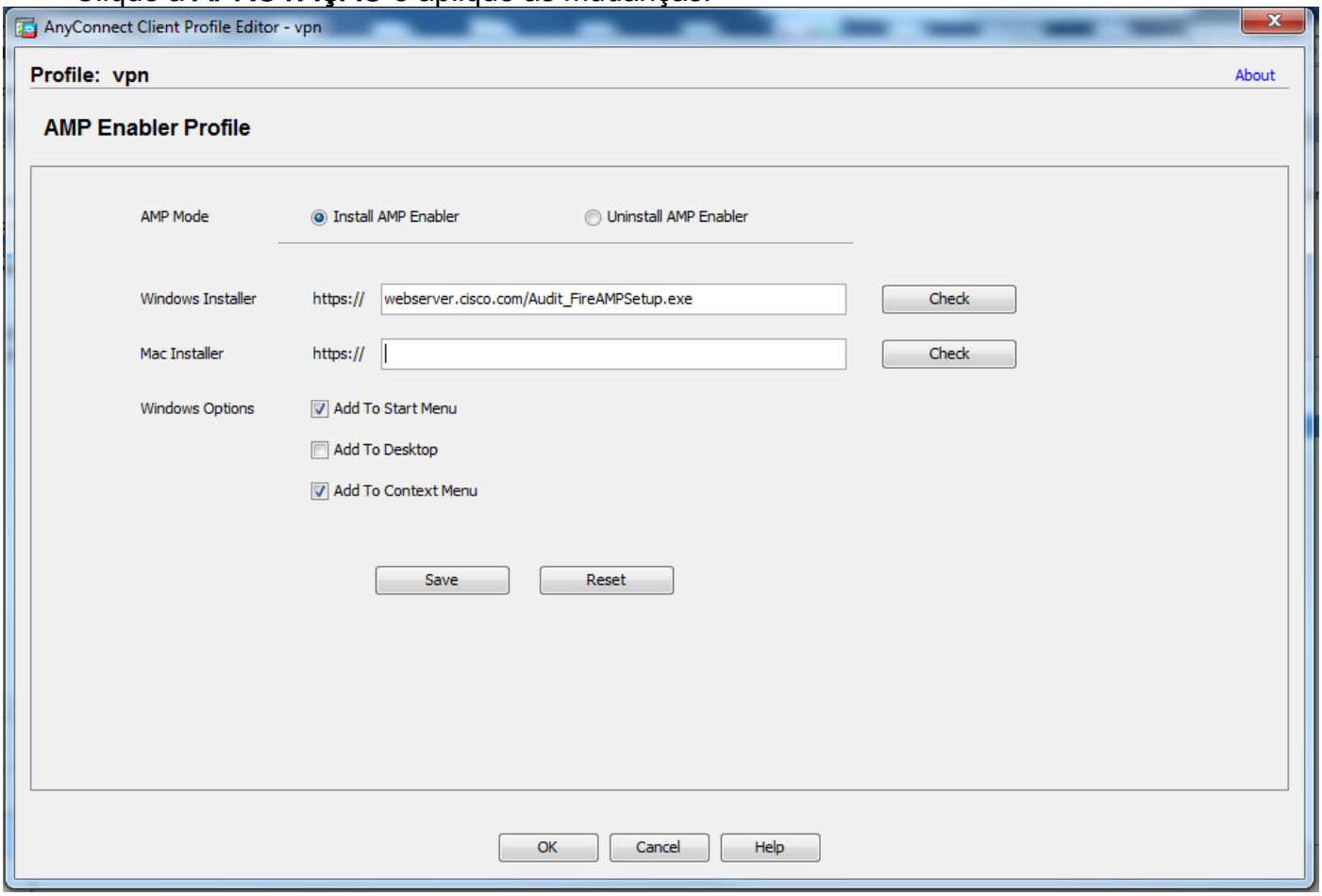
Especifique o servidor de Web da empresa ou uma parte da rede com instalador AMP. Isto é o mais de uso geral através das empresas salvar a largura de banda e colocar instaladores confiados na localização centralizada.

Seja por favor certo que a relação HTTPS pode ser alcançada nos valores-limite sem nenhum erro do certificado e que o certificado de raiz está instalado na loja da máquina.

Vá para trás ao perfil AMP criado antes no ASA (etapa 1) e edite o **perfil AMP Habilitador**:

1. Para o modo AMP, clique o botão de rádio da **instalação AMP Habilitador**.
2. No campo do **instalador de Windows**, adicionar o IP para o servidor de Web e o arquivo para o FireAMP.
3. As opções de Windows são opcionais.

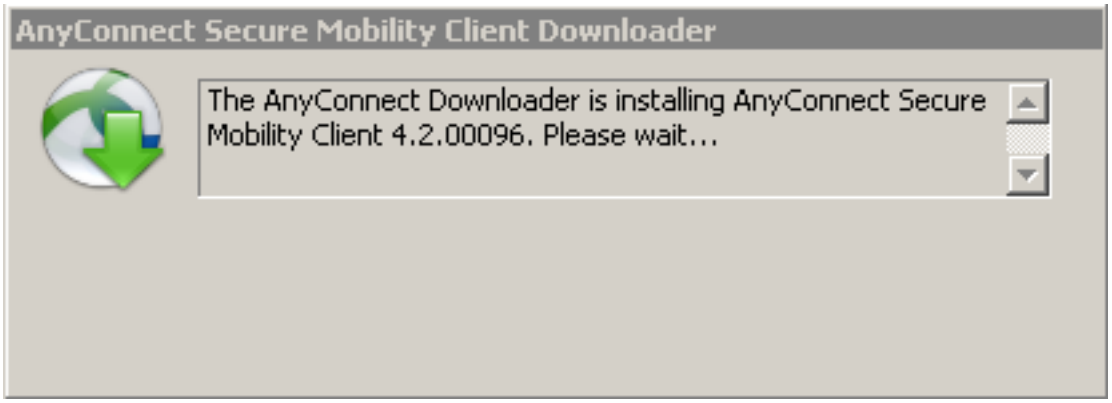
   Clique a **APROVAÇÃO** e aplique as mudanças.



Passo 5: Conecte com o AnyConnect e verifique a instalação do módulo

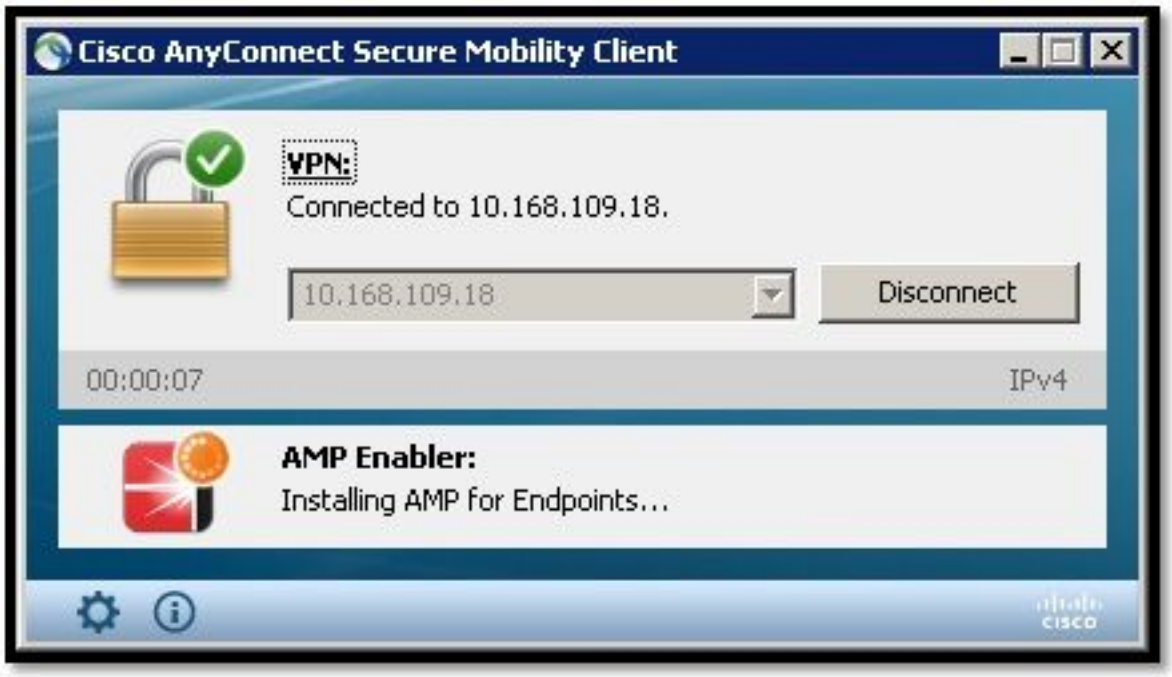
Quando os usuários de Anyconnect VPN conectam, o ASA empurra o módulo de AnyConnect AMP Habilitador com o VPN. Para já usuários conectados, recomenda-se terminar para trás e entrar então para que a funcionalidade seja permitida.

```
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%
```



Passo 6: Ligue a conexão de VPN instalar o conector AMP Habilitador e AMP

Uma vez que você bate o botão conecte para começar o VPN, ele transfere o módulo novo do descargador. Isto terá o enabler AMP e transfere o pacote AMP do trajeto que URL você especificou pares de etapas 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]
```

Etapa 7: Verifique AnyConnect e verifique se tudo é instalado

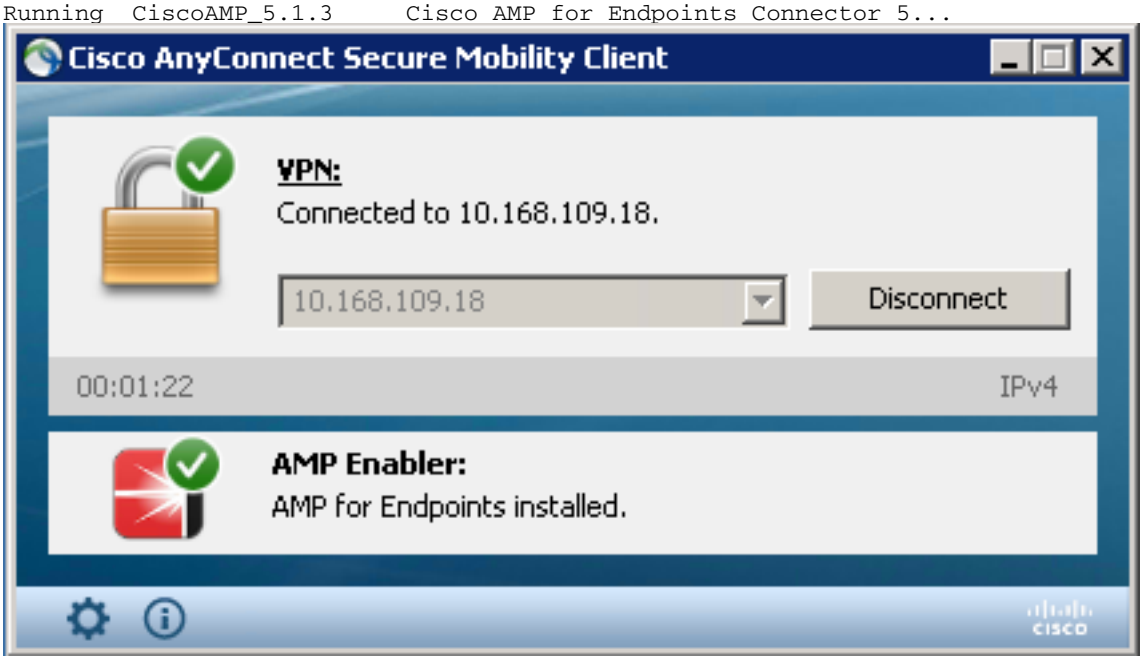
Uma vez que o VPN é conectado e a configuração do servidor de Web está instalada, verifique AnyConnect e verifique-o que tudo está instalado corretamente.

No services.msc você pode encontrar um serviço novo chamado CiscoAMP_5.1.3. No comando

de Powershell nós vemos:

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

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



O instalador AMP adiciona direcionadores novos ao SO Windows. Você pôde usar o comando do driverquery alistar os dirvers.

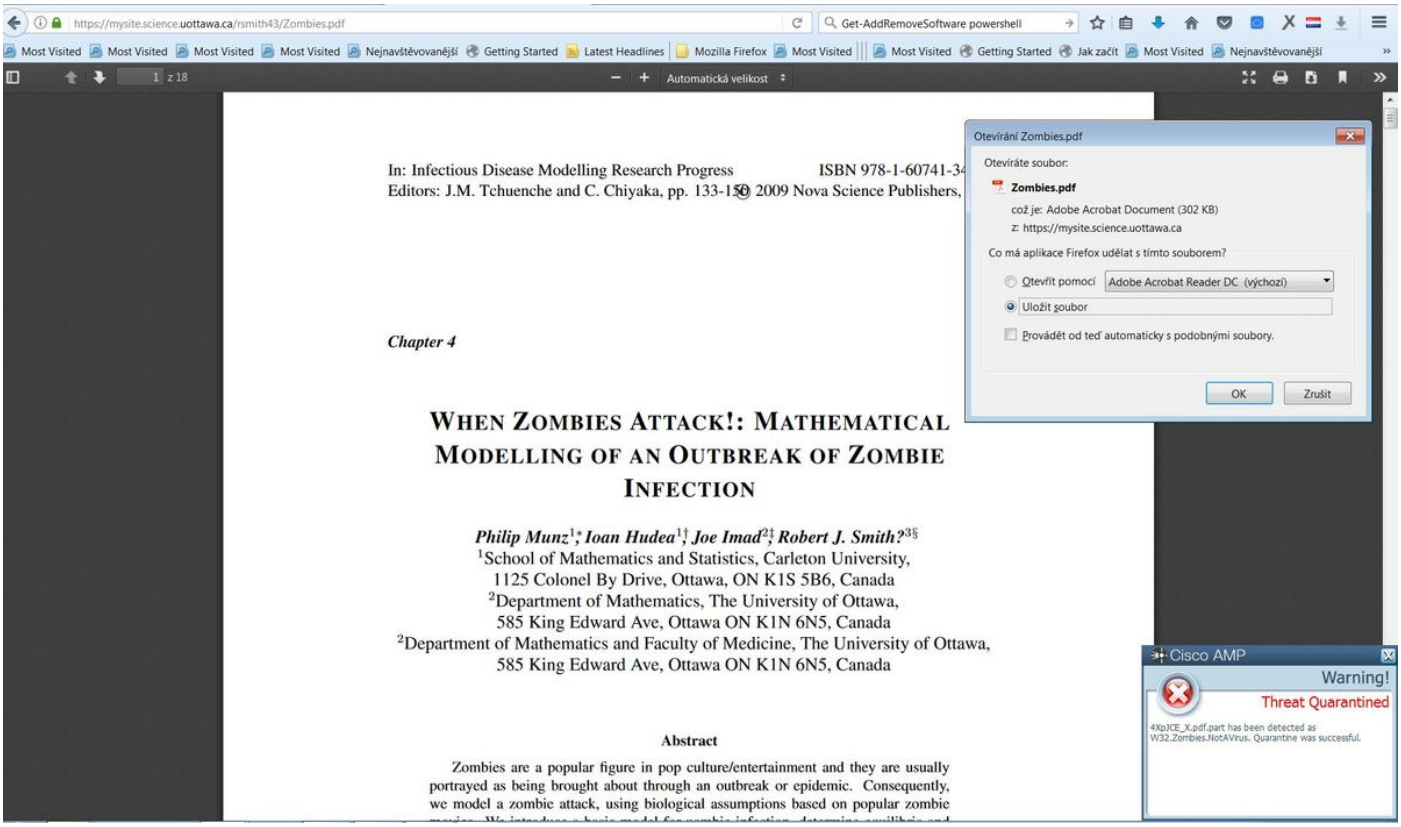
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

Passo 8: Teste com uma corda de Eicar contida em um arquivo PDF dos zombis

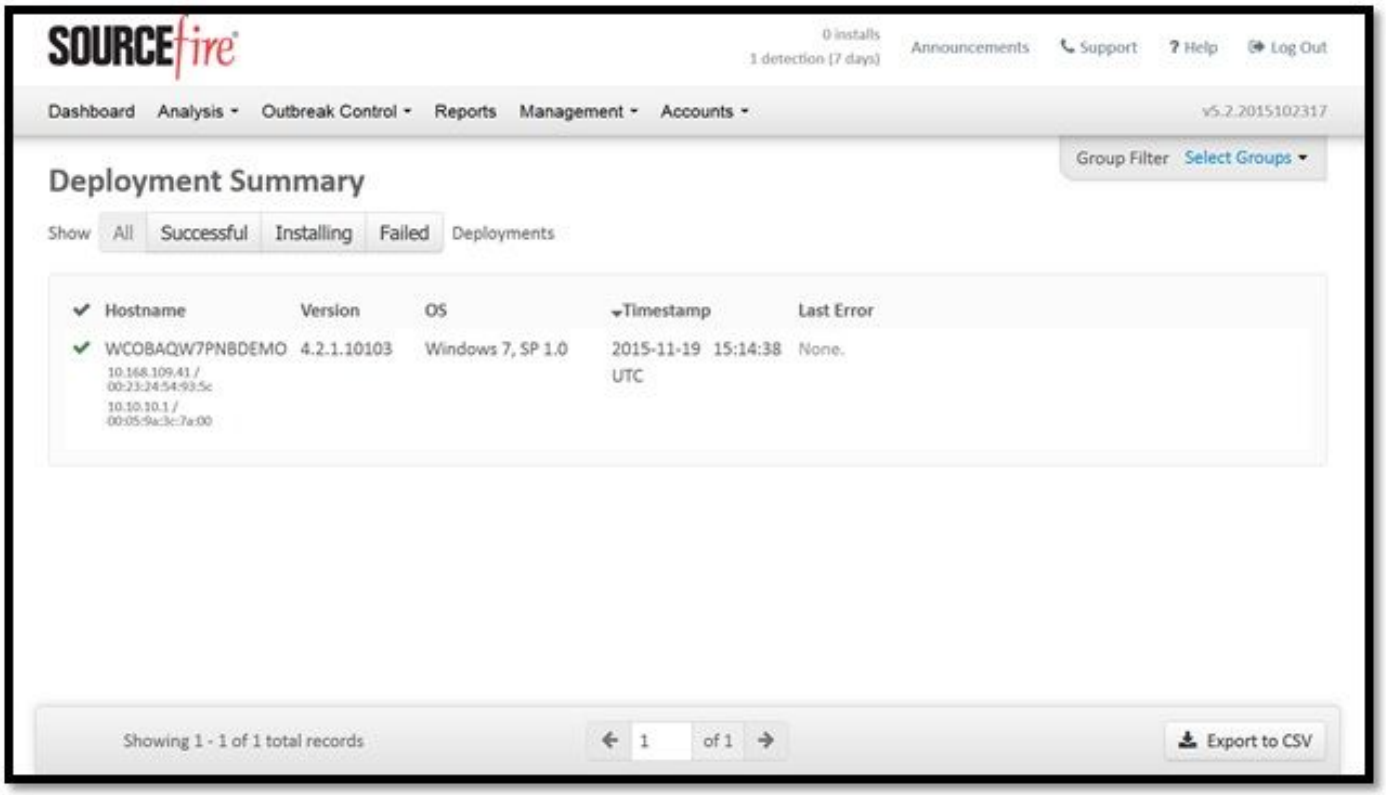
Teste com uma corda de Eicar contida em um arquivo PDF dos zombis em um computador do teste a fim verificar que o arquivo malicioso quarantined.



Zombies.pdf contém a corda de Eicar

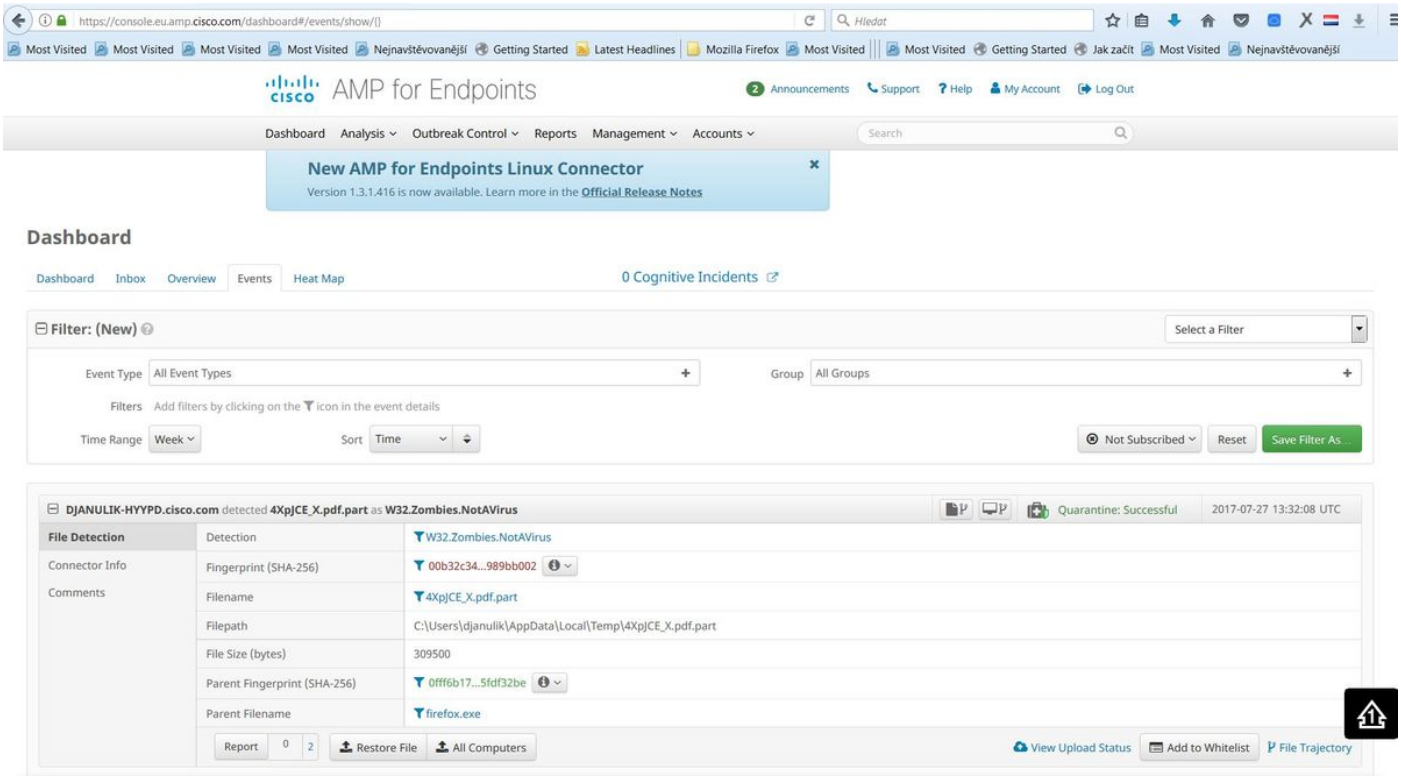
Etapa 9: Sumário do desenvolvimento

Esta página mostra-o que uma lista de bem sucedido e conector falhado de FireAMP instala assim como aqueles atualmente em andamento. Você pode ir ao **sumário do Gerenciamento > do desenvolvimento**.



Etapa 10: Verificação da detecção da linha

Zombies.pdf provocou um evento da quarentena, envia ao painel AMP.



Evento da quarentena

Additional Information

Para obter sua conta AMP, você pode assinar acima para a universidade ATS. Isto dá-lhe uma vista geral da funcionalidade AMP no LABORATÓRIO.

Informações Relacionadas

- Configurar AMP Habilitador
- Suporte Técnico e Documentação - Cisco Systems