Instalação e configuração do módulo AMP através do AnyConnect 4.x e do ativador AMP

Contents

Introduction

Este documento segue as etapas para instalar o conector Advanced Malware Protection (AMP) com AnyConnect.

O AnyConnect AMP Enabler é usado como um meio para implantar a AMP para endpoints. Ele mesmo não tem nenhuma capacidade de condenar a disposição do arquivo. Ele envia o software AMP para endpoints para um endpoint do ASA. Quando o AMP é instalado, ele usa a capacidade de nuvem para verificar a eliminação dos arquivos. Outro serviço AMP pode enviar arquivos para análise dinâmica chamada ThreatGrid, para pontuar comportamento de arquivos desconhecidos. Esses arquivos podem ser condenados como mal-intencionados se determinados artefatos forem atendidos. Isso é amplamente útil para ataques de dia zero.

Prerequisites

Requirements

- AnyConnect Secure Mobility Client versão 4.x
- FireAMP / AMP para endpoints
- Adaptive Security Device Manager (ASDM) versão 7.3.2 ou posterior

Componentes Utilizados

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

- Adaptive Security Appliance (ASA) 5525 com versão de software 9.5.1
- AnyConnect Secure Mobility Client 4.2.00096 no Microsoft Windows 7 Professional de 64 bits
- ASDM versão 7.5.1(112)

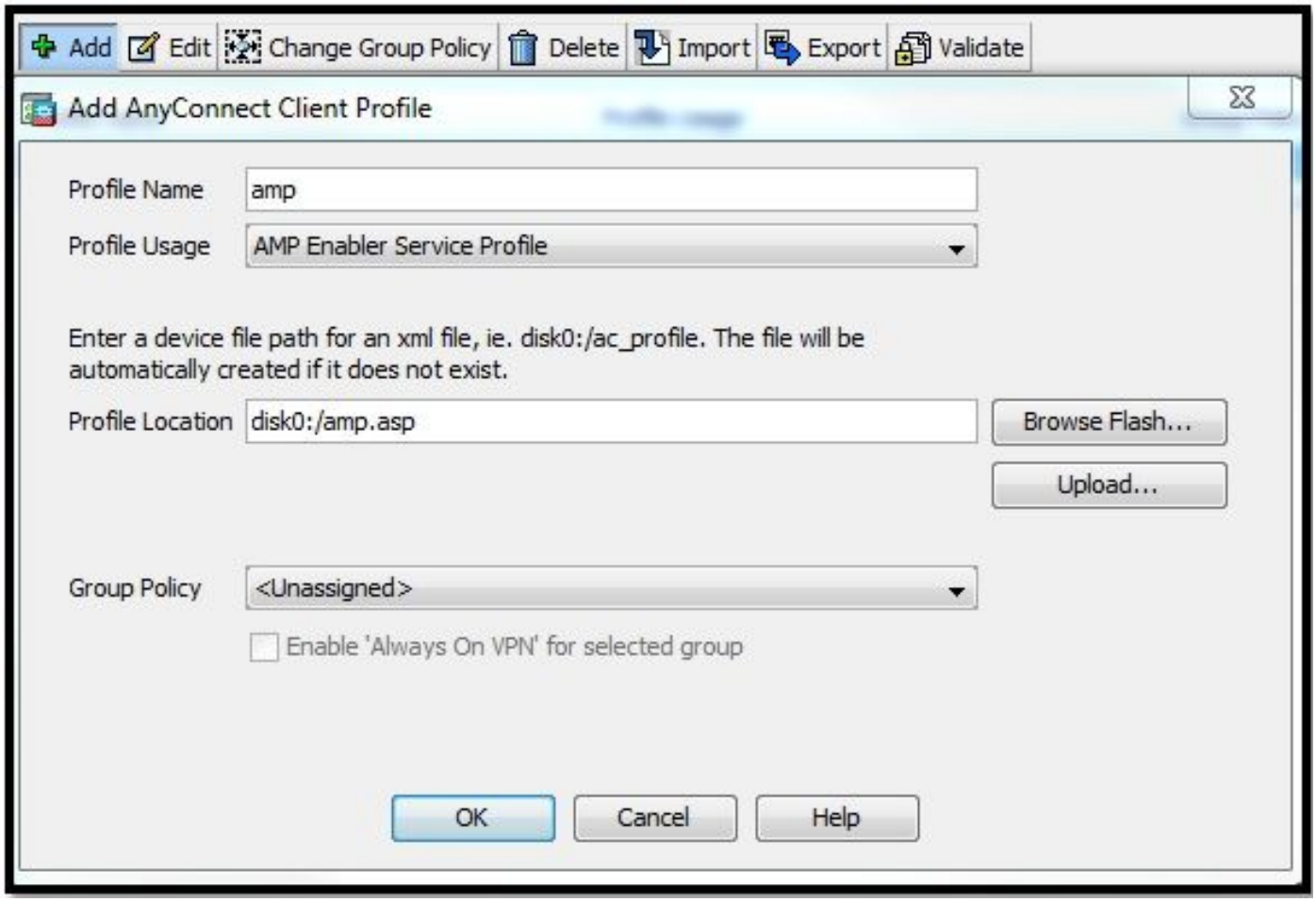
Implantação do AnyConnect para o AMP Enabler através do ASA

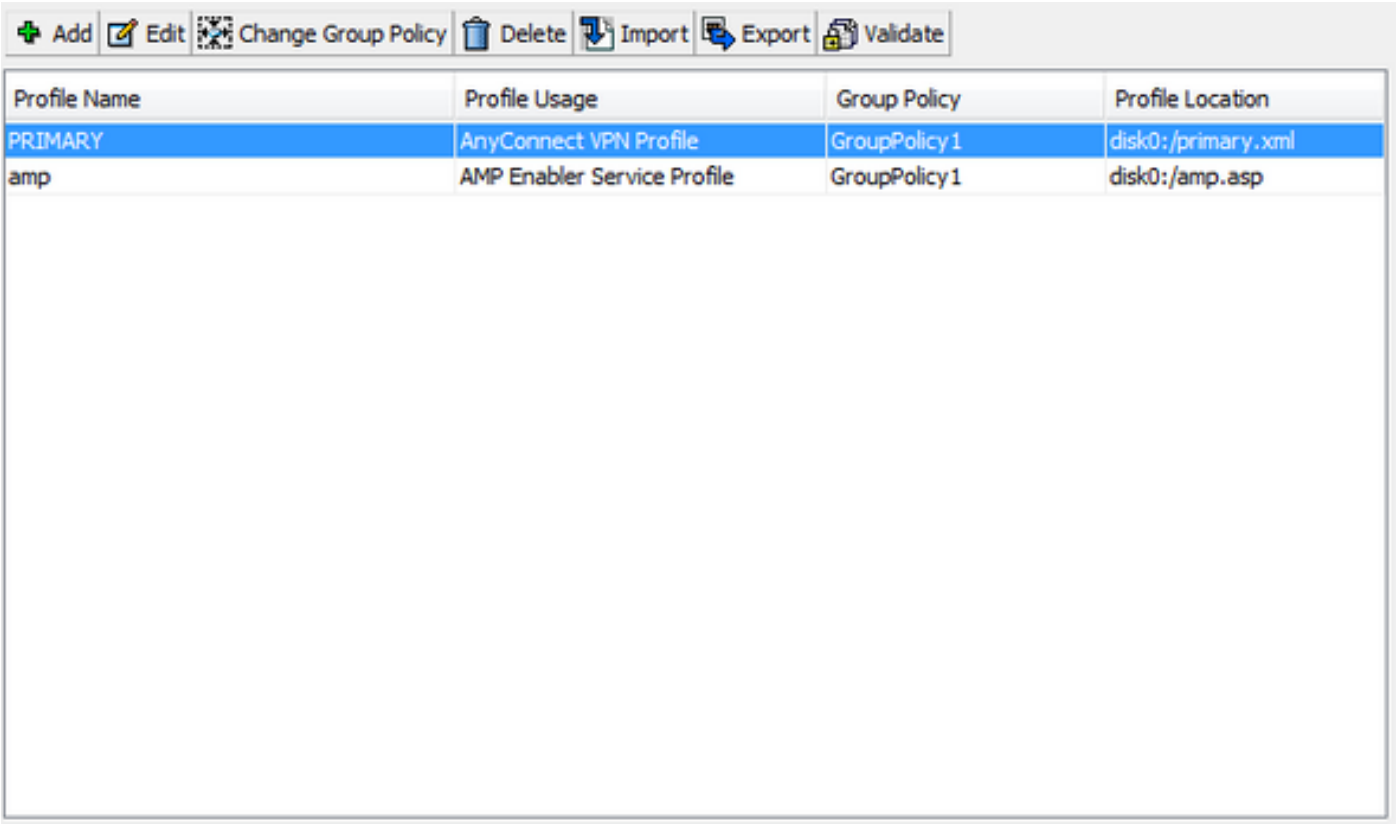
As etapas envolvidas na configuração são as seguintes:

- Configure o perfil do cliente do AnyConnect AMP Enabler.
- Edite a política de grupo do AnyConnect VPN e faça o download do Perfil de serviço do ativador AMP.
- Faça login no painel AMP para obter o link de download da URL do conector.
- Verifique a instalação na máquina do usuário.

Passo 1: Configurar o perfil do cliente do AnyConnect AMP Enabler

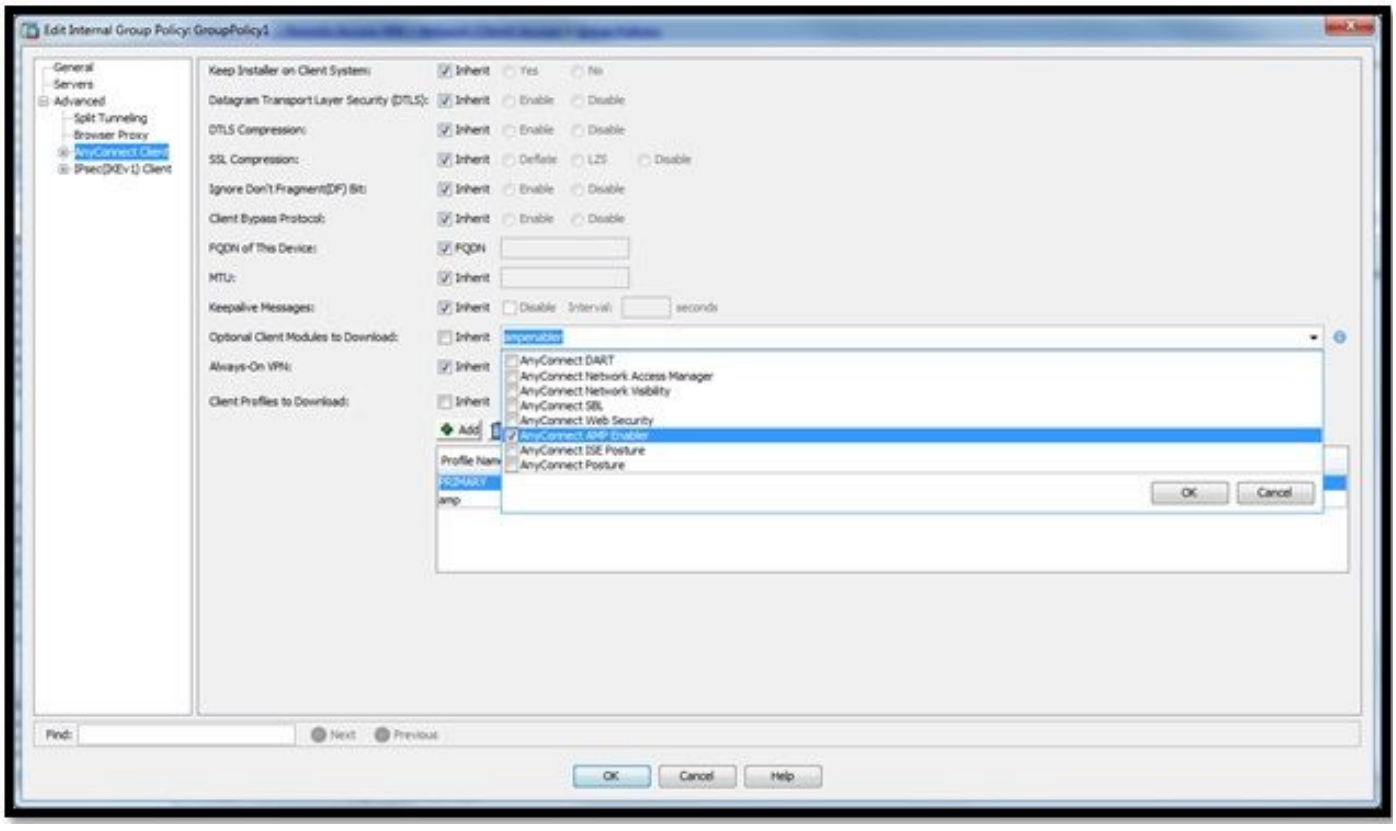
- Navegue até **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Adicione o **perfil de serviço do ativador AMP**.





Passo 2: Edite a política de grupo para baixar o AnyConnect AMP Enabler

- Navegue até **Configuration > Remove Access VPN > Group Policies > Edit** (Configuração > Remover VPN de Acesso > Políticas de Grupo > Editar).
- Vá para **Avançado > Cliente AnyConnect > Módulos de cliente opcionais para baixar.**
- Escolha **AnyConnect AMP Enabler.**



Passo 3: Baixe a política do FireAMP

Note: Antes de continuar, verifique se o sistema atende aos requisitos da AMP do conector do Windows do endpoint.

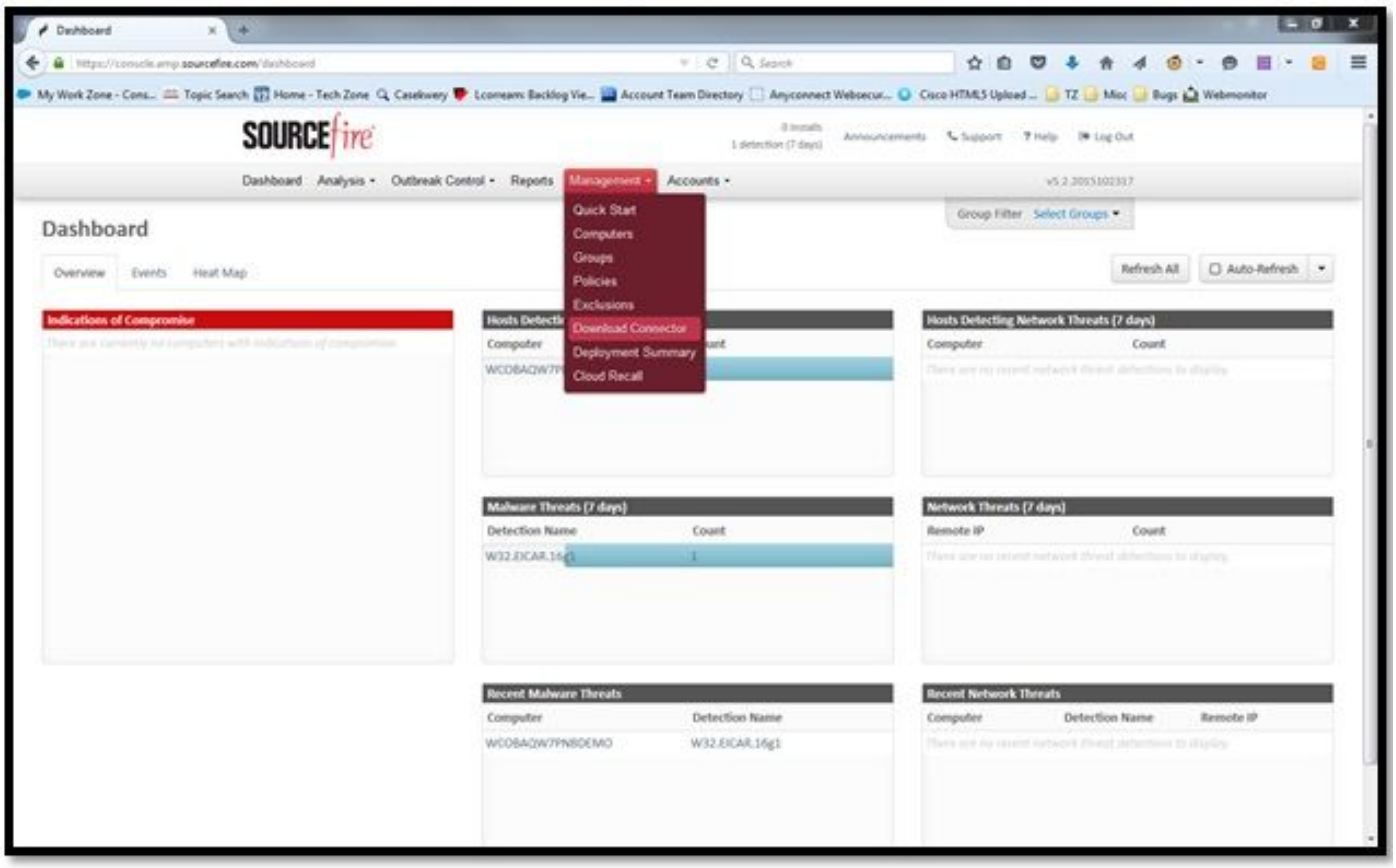
Requisitos do sistema para o AMP para endpoints Conector do Windows

Esses são os requisitos mínimos do sistema para o conector FireAMP baseado no sistema operacional Windows. O conector FireAMP suporta as versões de 32 e 64 bits desses sistemas operacionais. A documentação mais recente da AMP pode ser encontrada na implantação da AMP

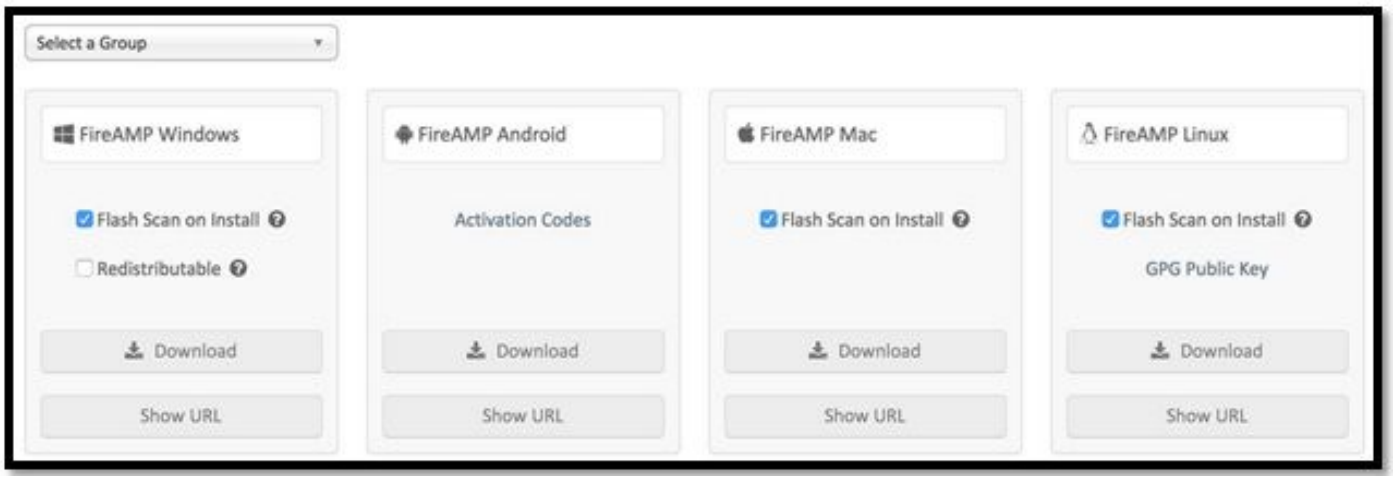
Sistema operacional	Processador	Memória	Espaço em disco, Modo somente nuvem	Espaço em disco
Microsoft Windows 7	Processador de 1 GHz ou mais rápido	1 GB de RAM	150 MB de espaço disponível no disco rígido - modo somente na nuvem	1 GB de espaço disponível no disco rígido - TETRA
Microsoft Windows 8 e 8.1 (requer FireAMP Connector 5.1.3 ou posterior)	Processador de 1 GHz ou mais rápido	512 MB de RAM	150 MB de espaço disponível no disco rígido - modo somente na nuvem	1 GB de espaço disponível no disco rígido - TETRA
Microsoft Windows Server 2003	Processador de 1 GHz ou mais rápido	512 MB de RAM	150 MB de espaço disponível no disco rígido - modo somente na nuvem	1 GB de espaço disponível no disco rígido - TETRA
Microsoft Windows Server 2008	Processador de 2 GHz ou mais rápido	2 GB de RAM	150 MB de espaço disponível no disco rígido - modo somente na nuvem	1 GB de espaço disponível no disco rígido - TETRA
Microsoft Windows Server 2012 (requer o FireAMP Connector 5.1.3 ou posterior)	Processador de 2 GHz ou mais rápido	2 GB de RAM	150 MB de espaço disponível no disco rígido - modo somente na nuvem	1 GB de espaço disponível no disco rígido - TETRA

O mais comum é colocar o instalador da AMP no servidor web da empresa.

Para baixar o conector, navegue até **Management > Download Connector**. Em seguida, escolha o tipo e **Baixe o** FireAMP (Windows, Android, Mac, Linux).



A página Baixar conector permite que você faça o download dos pacotes de instalação para cada tipo de conector FireAMP. Este pacote pode ser colocado em um compartilhamento de rede ou distribuído por meio de software de gerenciamento.



Selecionar um grupo

- **Somente auditoria:** Monitorando o sistema com base no SHA-256 calculado sobre cada arquivo. Este modo de Auditoria apenas não coloca o malware em quarentena, mas envia um evento como um alerta.
- **Proteger:** Modo de proteção com arquivos mal-intencionados em quarentena. Monitorar cópia e movimentação de arquivos.
- **Triagem:** Destina-se ao uso em computadores já comprometidos/infectados.
- **Servidor:** Conjunto de instalação para servidor Windows, onde o conector é instalado sem o mecanismo Tetra e o driver DFC. Esse grupo é projetado por seu nome para servidores de controladores que não são de domínio.

- **Controlador de domínio:** A política padrão para esse grupo é definida para o modo de auditoria como no grupo Servidor. Associe todos os servidores do Ative Diretory neste grupo, o que significa que o conector estará em execução em um Controlador de Domínio do Windows.

O AMP tem o recurso chamado TETRA, que é um mecanismo antivírus completo. Essa opção é opcional por política.

Recursos

- **Flash Scan na instalação:** O processo de verificação é executado durante a instalação. É relativamente rápido e recomendado executar apenas uma vez.
- **Redistribuível:** Você deve fazer o download de um único pacote, que contém instaladores de 32 e 64 bits. Em vez de um bootstrapper, que está disponível, deixando essa opção sem marca e fazendo o download dos arquivos do instalador, uma vez executados.

> **Note**: Você pode criar seu próprio grupo e configurar a política associada para ele. O objetivo é colocar todos, por exemplo, os servidores Ative Diretory em um grupo, onde a política está no modo de auditoria.
> O instalador bootstrapper e redistribuível também contém um arquivo policy.xml usado como um arquivo de configuração para o conector AMP.

Passo 4: Baixe o perfil do cliente do Web Security

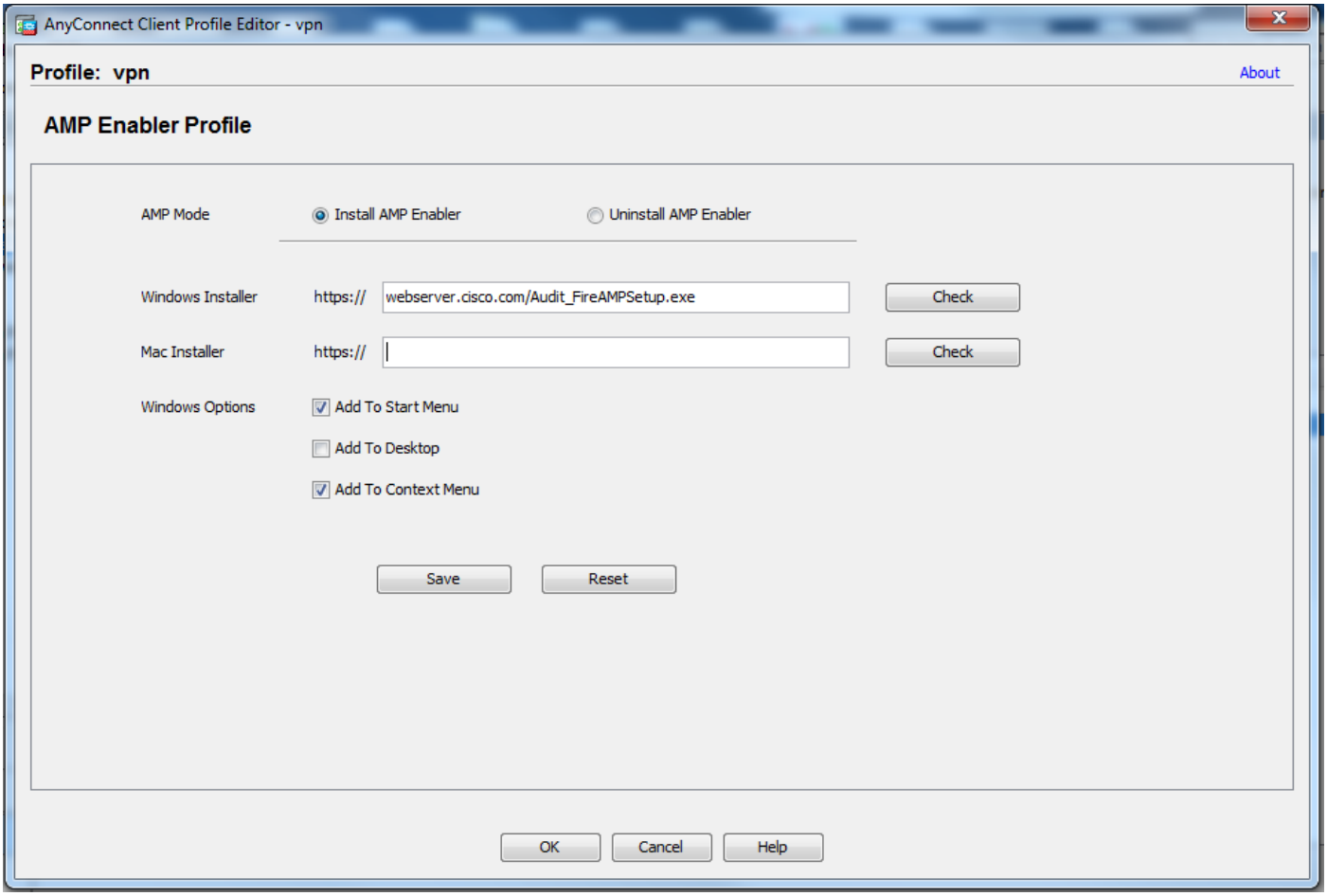
Especifique o servidor Web da empresa ou um compartilhamento de rede com o instalador da AMP. Isso é mais comumente usado em empresas para economizar largura de banda e colocar instaladores confiáveis em locais centralizados.

Certifique-se de que o link HTTPS pode ser alcançado nos endpoints sem nenhum erro de certificado e de que o certificado raiz está instalado no armazenamento da máquina.

Volte para o perfil da AMP criado antes no ASA (etapa 1) e edite o **perfil do ativador da AMP**:

1. No AMP Mode (Modo AMP), clique no botão de opção **Install AMP Enabler (Instalar o AMP Enabler)**.
2. No campo **Windows Installer**, adicione o IP para o servidor Web e o arquivo para o FireAMP.
3. As Opções do Windows são opcionais.

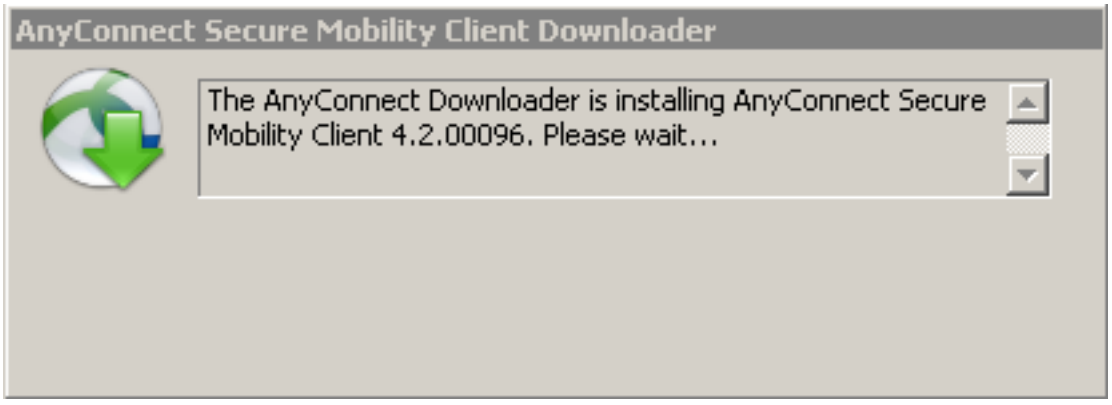
Clique em **OK** e aplique as alterações.



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

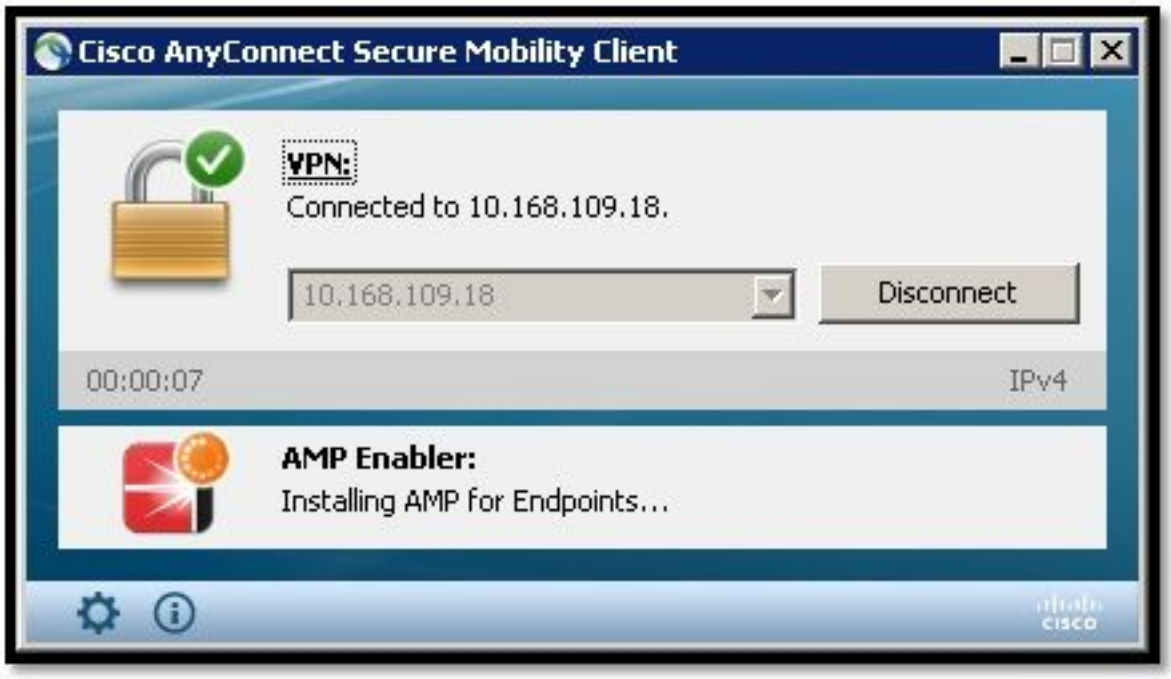
Quando os usuários do AnyConnect VPN se conectam, o ASA envia o módulo do AnyConnect AMP Enabler pela VPN. Para usuários já conectados, é recomendável fazer logoff e, em seguida, fazer logon novamente para que a funcionalidade seja habilitada.

```
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: Iniciar conexão VPN instalar o ativador AMP e o conector AMP

Quando você pressiona o botão conectar para iniciar a VPN, ela faz o download do novo módulo do downloader. Isso terá o ativador do AMP e fará o download do pacote do AMP do caminho do URL que você especificou algumas 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]
```

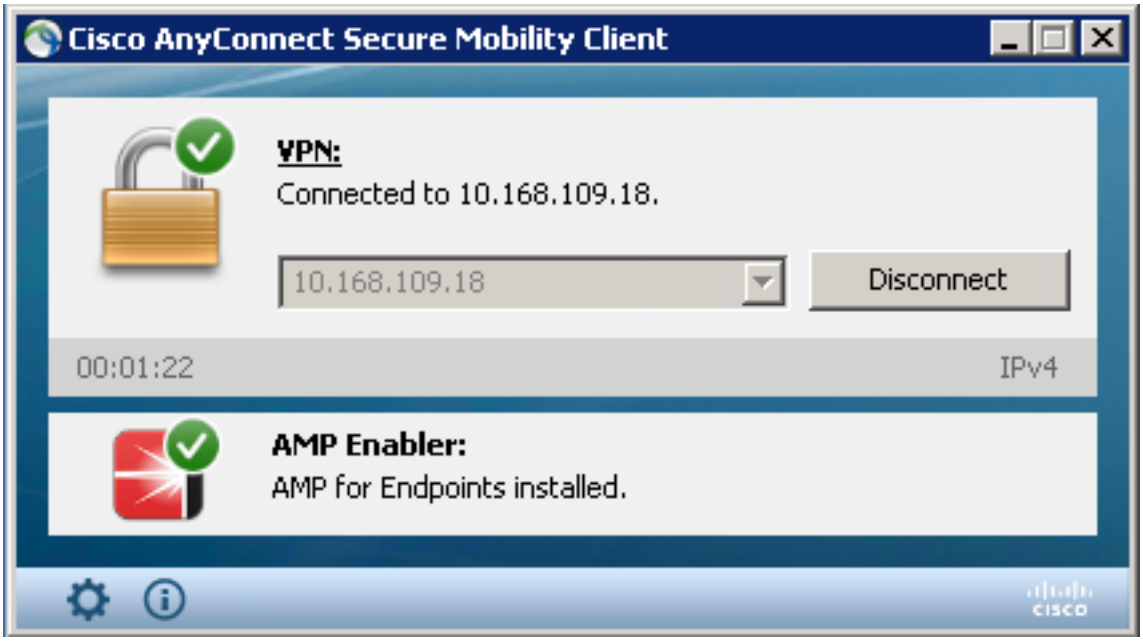
Passo 7: Verifique o AnyConnect e se tudo está instalado

Depois que a VPN estiver conectada e a configuração do servidor Web estiver instalada, verifique o AnyConnect e verifique se tudo está instalado corretamente.

No services.msc, você pode encontrar um novo serviço chamado CiscoAMP_5.1.3. No comando Powershell 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 do AMP adiciona novos drivers ao sistema operacional Windows. Você pode usar o comando driverquery para listar os drivers.

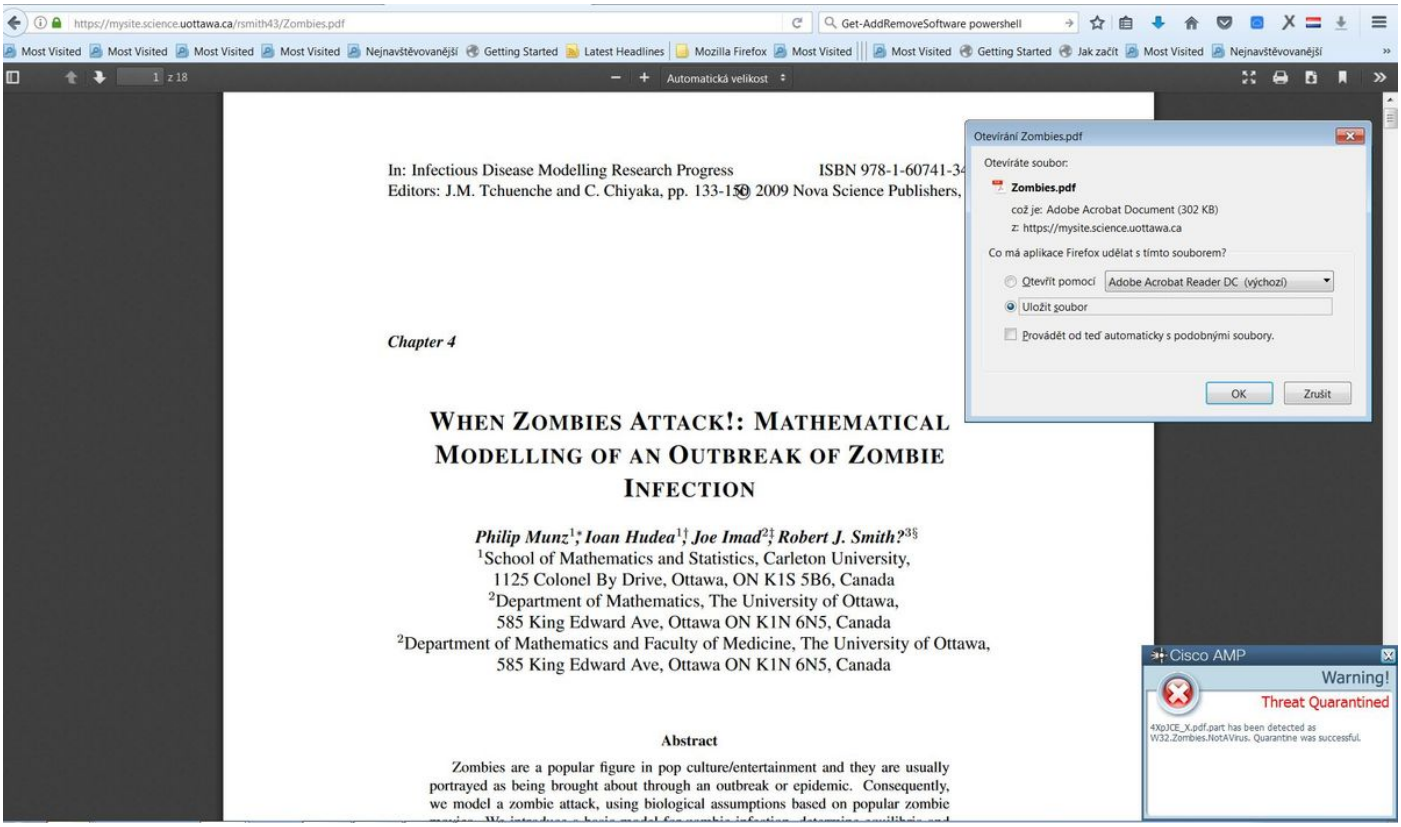
```
C:\Windows\System32>driverquery /v | findstr immunet

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 string de Eicar contida em um arquivo PDF do Zombies

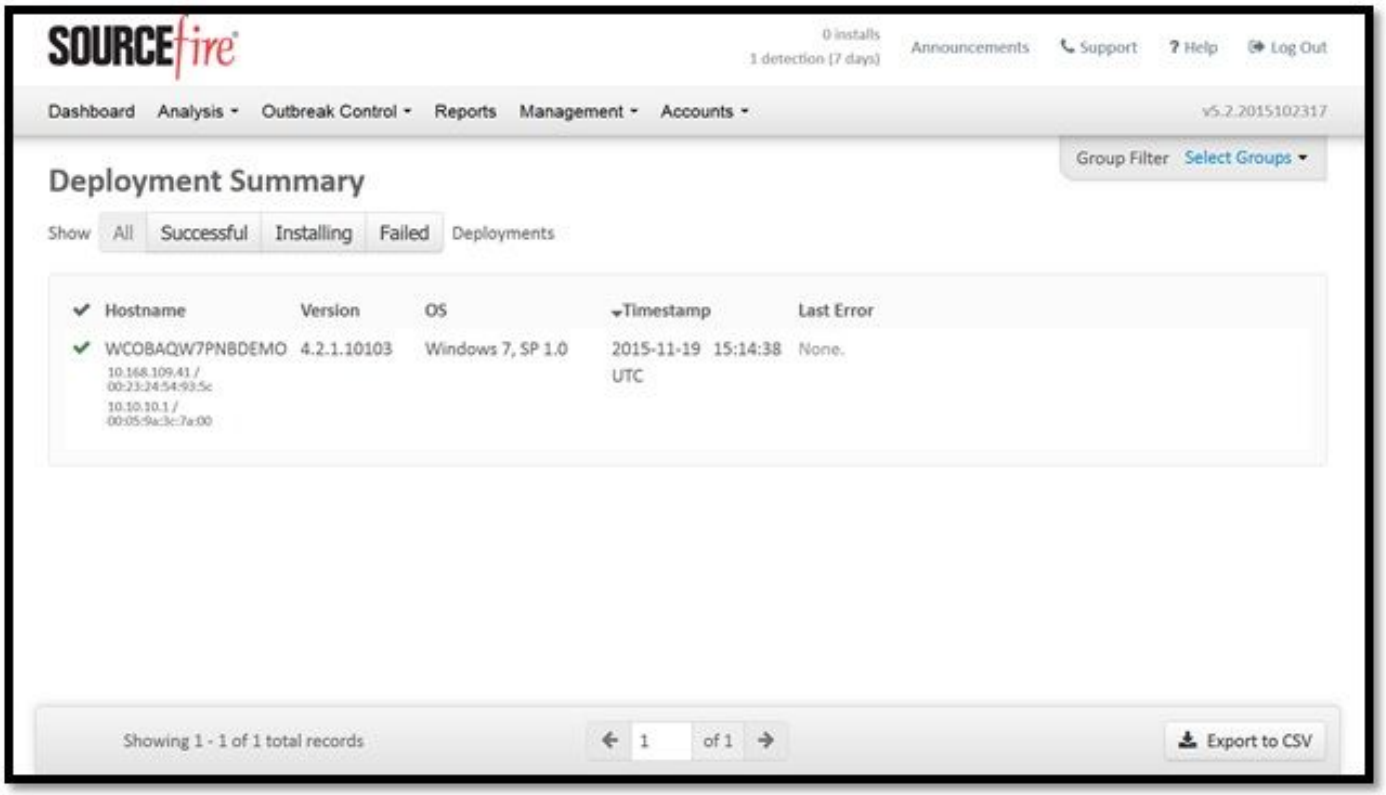
Teste com uma string Eicar contida em um arquivo PDF do Zombies em um computador de teste para verificar se o arquivo mal-intencionado está em quarentena.



Zombies.pdf contém uma string Eicar

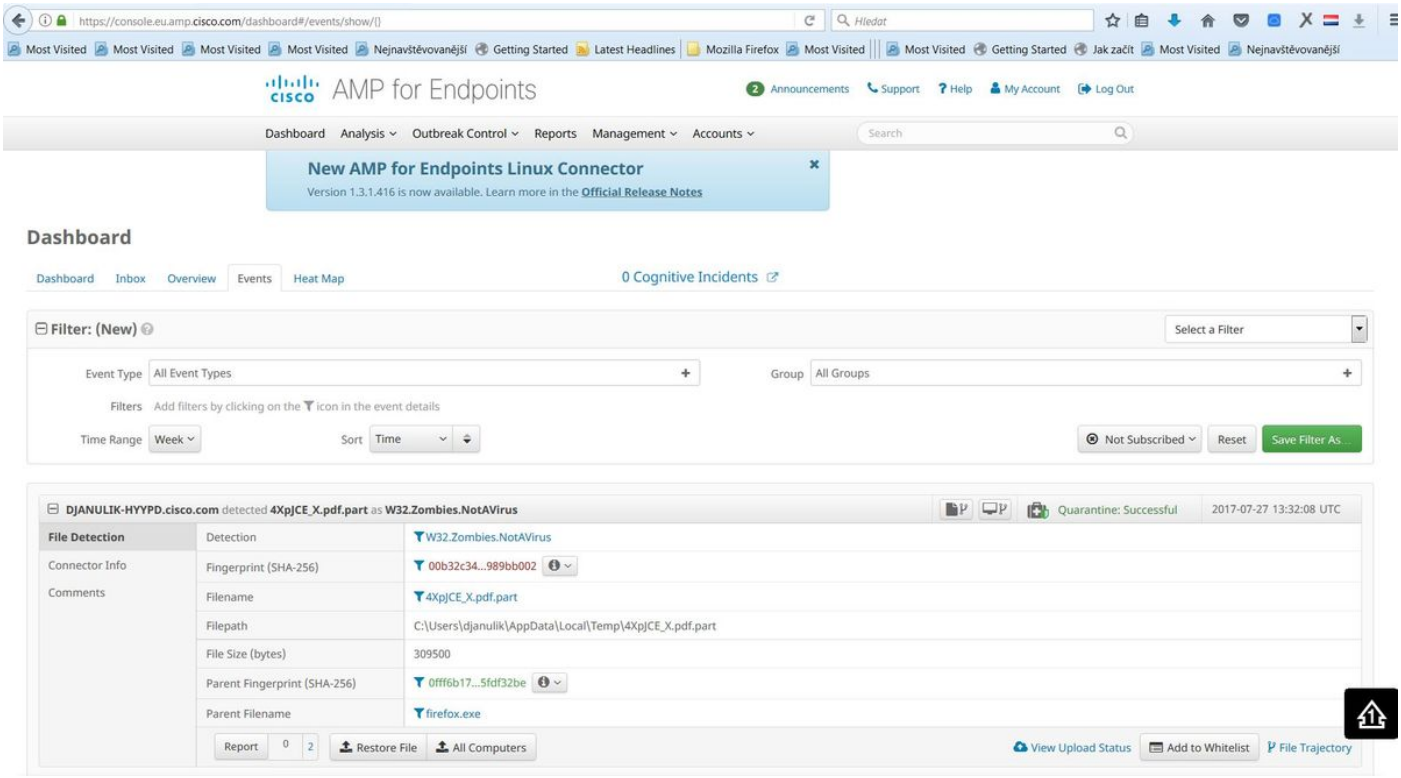
Etapa 9: Resumo da implantação

Esta página mostra uma lista das instalações bem-sucedidas e com falha do conector FireAMP, bem como das que estão em andamento no momento. Você pode ir para **Gerenciamento > Resumo da implantação**.



Etapa 10: Verificação de Detecção de Threads

O Zombies.pdf acionou um evento de quarentena, envie para o painel do AMP.



evento de quarentena

Additional Information

Para obter sua conta AMP, você pode se inscrever na ATS University. Isso oferece uma visão geral da funcionalidade do AMP no LAB.

Informações Relacionadas

- Configurar o ativador da AMP
- Suporte Técnico e Documentação - Cisco Systems