Installatie en configuratie van de AMP-module via AnyConnect 4.x en AMP-controller

Inhoud

Inleiding

Dit document gaat door stappen om de Advanced Malware Protection (AMP)-connector met AnyConnect te installeren.

AnyConnect AMP Enabler wordt gebruikt als medium om AMP voor endpoints te implementeren. Op zichzelf heeft het geen mogelijkheid om bestandsdispositie te veroordelen. Het duwt de AMP voor Endpoints software op een eindpunt van ASA. Nadat de Advanced Malware Protection is geïnstalleerd, gebruikt u de wolkencapaciteit om de verwerking van bestanden te controleren. Nadere AMP-service kan bestanden naar dynamische analyse, ThreatGrid, sturen om onbekend bestandsgedrag te scoren. Deze bestanden kunnen als kwaadaardig worden veroordeeld indien aan bepaalde artefacten is voldaan. Dit is zeer nuttig voor aanvallen met een dag op nul.

Voorwaarden

Vereisten

- AnyConnect Secure Mobility Client versie 4.x
- FirePOWER/AMP voor endpoints
- Adaptieve Security Adapter Manager (ASDM) versie 7.3.2 of hoger

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Adaptieve security applicatie (ASA) 5525 met software versie 9.5.1
- AnyConnect Secure Mobility Client 4.2.0096 op Microsoft Windows 7 Professional 64-bits
- ASDM versie 7.5.1(12)

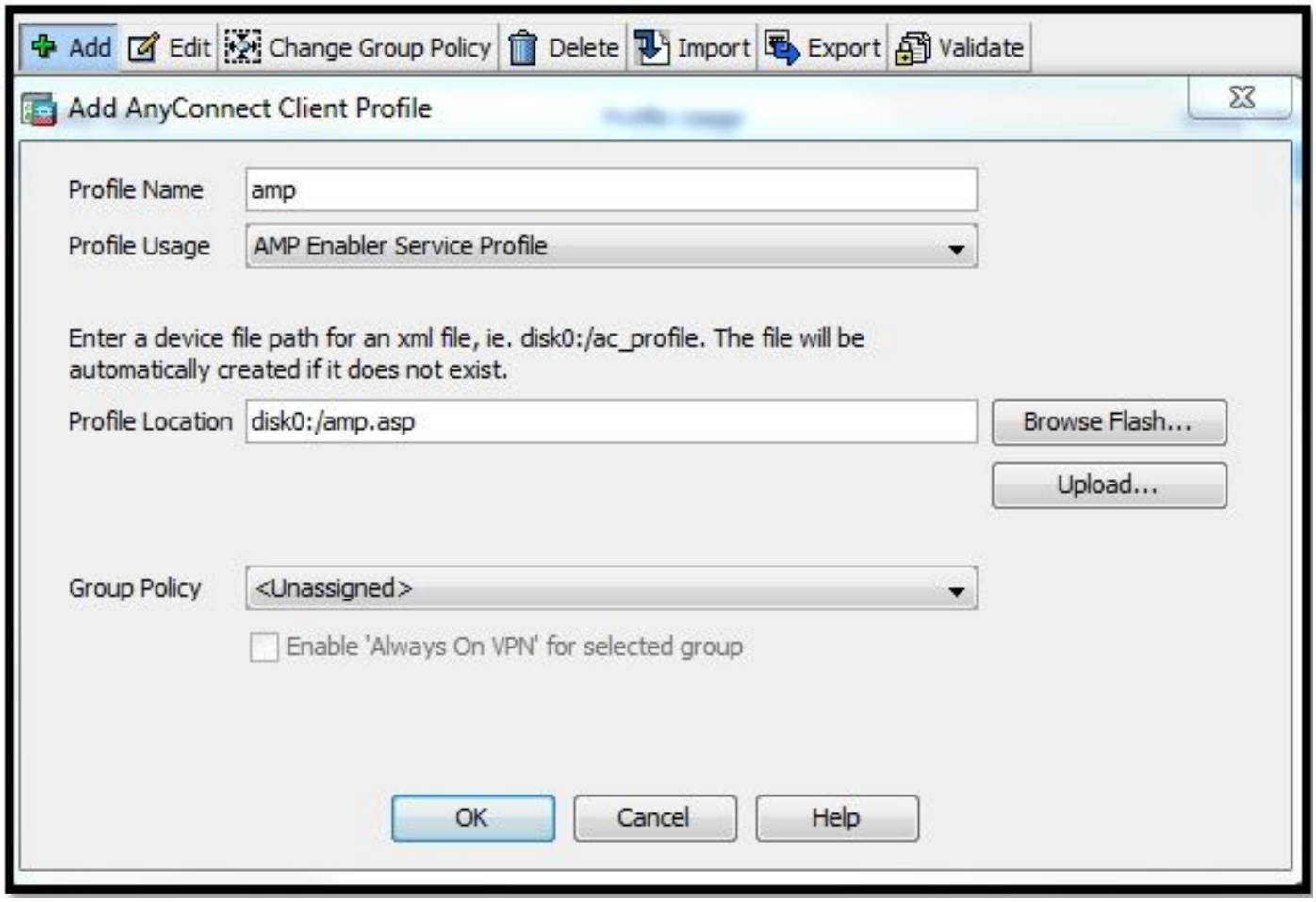
AnyConnect-implementaties voor AMP-ondersteuning via ASA

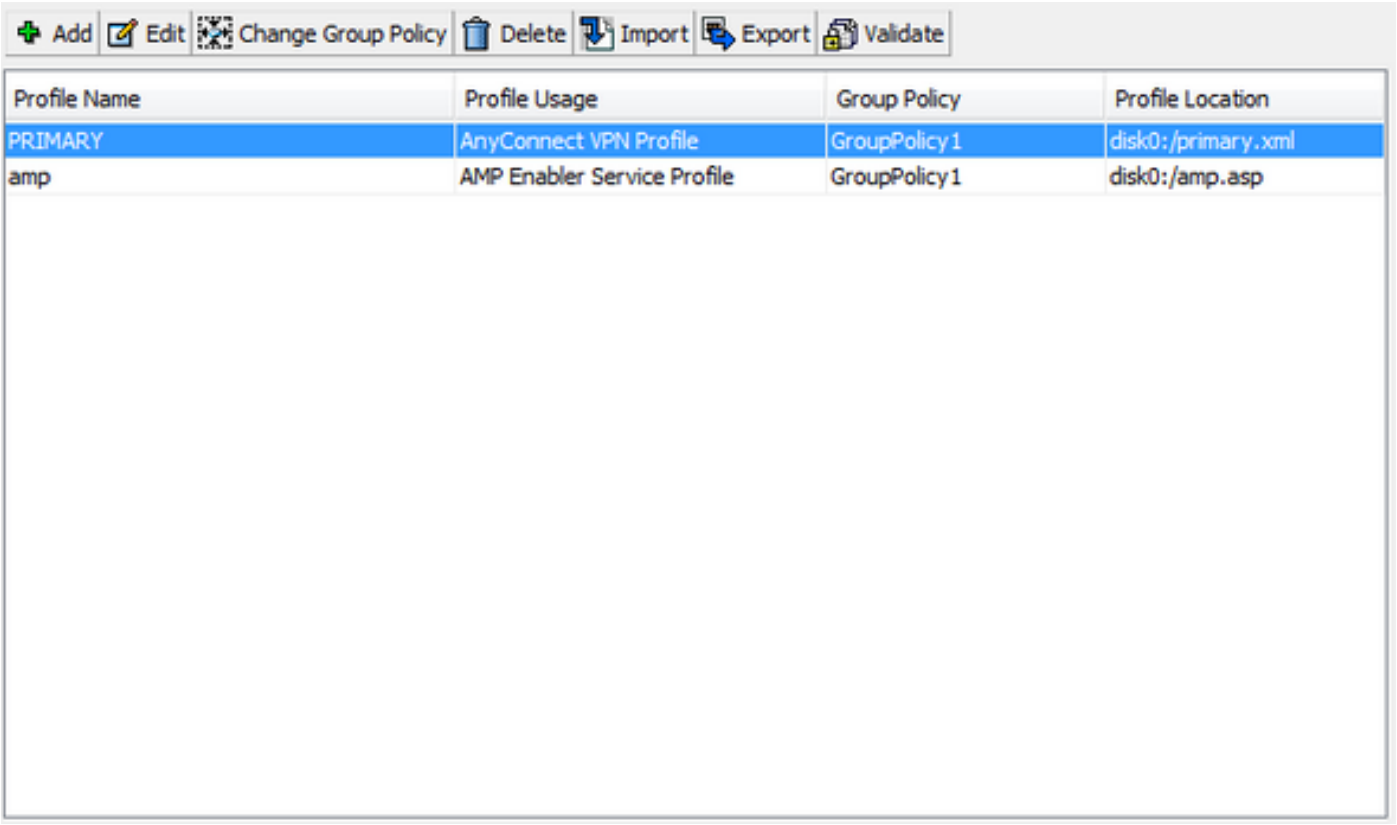
De bij de configuratie betrokken stappen zijn als volgt:

- Configureer het clientprofiel van AnyConnect AMP Enabler.
- Bewerk het AnyConnect VPN-groepsbeleid en download het AMP Enabler-serviceprofiel.
- Meld u aan bij het AMP-dashboard om de URL-downloadlink van de connector te krijgen.
- Controleer de installatie op de gebruikersmachine.

Stap 1: Clientprofiel met AnyConnect AMP Enabler configureren

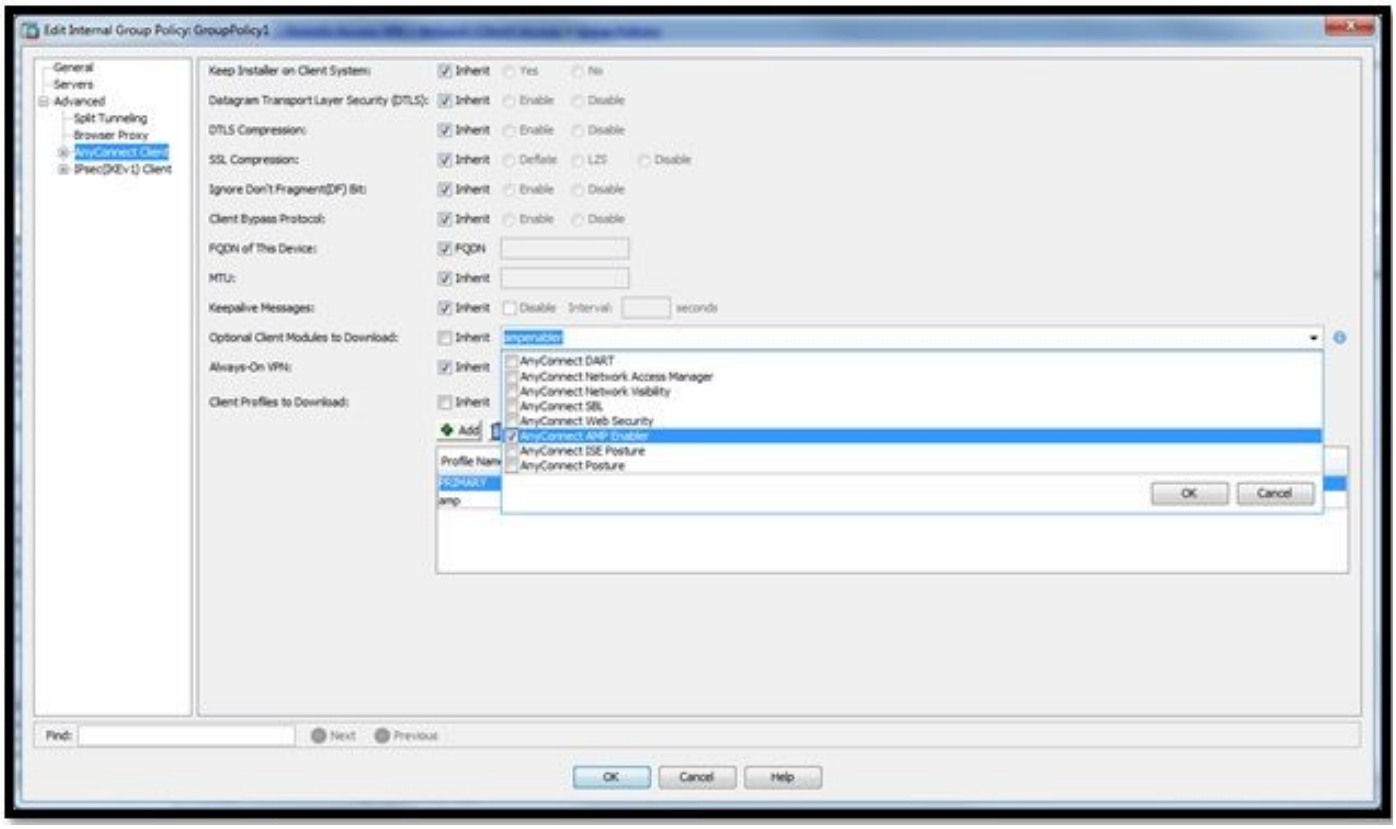
- navigeren naar **Configuratie > Remote Access VPN > Netwerktoegang (client) > AnyConnect-clientprofiel**.
- Voeg het **AMP-serviceprofiel toe**.





Stap 2: Bewerk het groepsbeleid om de AnyConnect-AMP-controller te downloaden

- Navigeren in **configuratie > Toegang VPN verwijderen > Groepsbeleid > Bewerken**.
- Ga naar **Geavanceerd > AnyConnect-client > optionele clientmodules voor downloads.**
- Kies **AnyConnect AMP Enabler.**



Stap 3: FirePOWER-beleid downloaden

Opmerking: Controleer voordat u verdergaat of uw systeem voldoet aan de vereisten voor de Advanced Malware Protection of Endpoints Windows Connector.

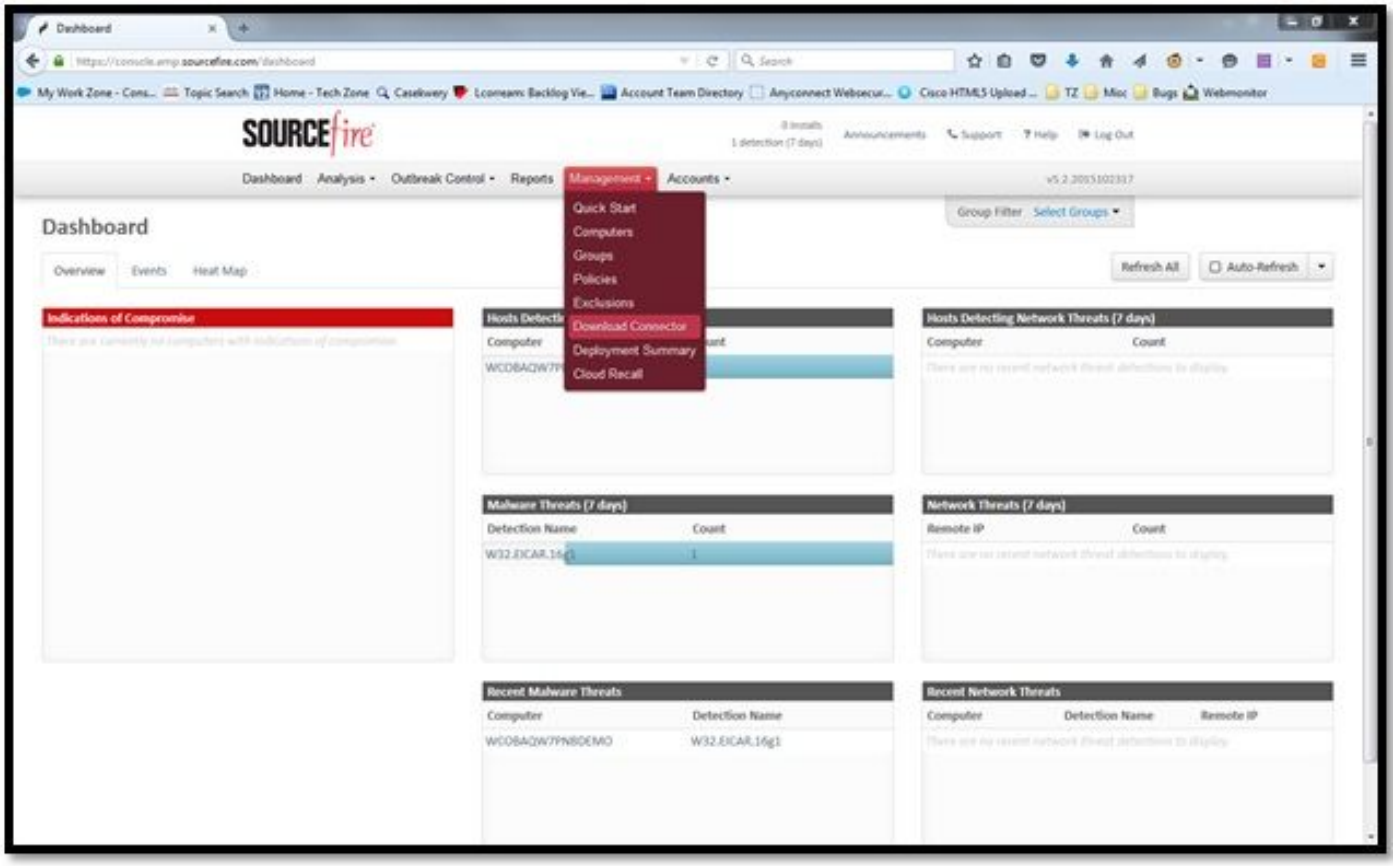
Systeemvereisten voor Advanced Malware Protection voor endpoints en Windows-connector

Dit zijn de minimum systeemvereisten voor de FireAMP-connector die op het Windows-besturingssysteem is gebaseerd. De FireAMP-connector ondersteunt zowel 32-bits als 64-bits versies van deze besturingssystemen. De nieuwste AMP-documentatie is te vinden in de AMP-implementatie

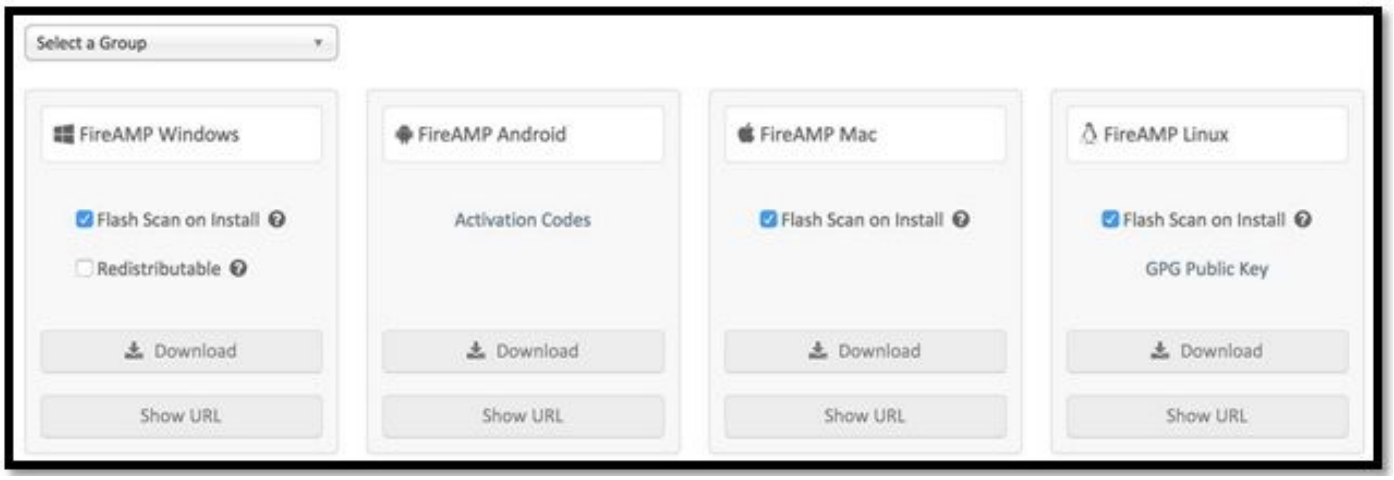
Besturingssysteem	processor	Geheugen	Disc-ruimte, Alleen cloudmodus	Schijf ruimte
Microsoft Windows 7	1 GHz of snellere processor	1 GB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA
Microsoft Windows 8 en 8.1 (hiervoor is FirePOWER-connector 5.1.3 of hoger nodig)	1 GHz of snellere processor	512 MB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA
Microsoft Windows Server 2003	1 GHz of snellere processor	512 MB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA
Microsoft Windows Server 2008	2 GHz of snellere processor	2 GB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA
Microsoft Windows Server 2012 (hiervoor is FireAMP-connector 5.1.3 of hoger nodig)	2 GHz of snellere processor	2 GB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA

Het meest gebruikelijk is om de installateur van AMP op de website van de onderneming te laten plaatsen.

Ga om de connector te downloaden naar **Management > Download connector**. Kies vervolgens type en **Download** FirePOWER (Windows, Android, Mac, Linux).



Met de pagina Download Connector kunt u de installatiepakketten voor elk type van FireAMP-connector downloaden. Dit pakket kan op een netwerkaandeel worden geplaatst of via beheersoftware worden verspreid.



Een groep selecteren

- **Alleen controle:** Controle van het systeem op basis van SHA-256 berekend over elk bestand. Deze Controlemodus stelt de malware niet in quarantaine, maar stuurt een gebeurtenis als alarm.
- **Beschermen:** Beveiliging van modus met quarantainebestanden. Monitorbestand kopiëren en verplaatsen.
- **Triage:** Dit is voor gebruik op een reeds gecompromitteerde/geïnfecteerde computer.
- **Server:** Installatiesuite voor Windows server, waar de connector installeert zonder Tetra-motor en DFC-stuurprogramma. Deze groep is ontworpen door de naam ervan voor servers die niet op het domein vallen.

- **Domain Controller:** Het standaardbeleid voor deze groep wordt ingesteld op audit mode zoals in servergroep. Associeer al uw actieve directory servers in deze groep, dit betekent dat de connector op een Windows Domain Controller zal worden uitgevoerd.

De AMP heeft de functie TETRA, de volledige antivirusmotor. Deze optie is optioneel per beleid.

Functies

- **Flash Scan op installatie:** Scan het proces tijdens de installatie. Het is relatief snel om te starten en aanbevolen slechts één keer te draaien.
- **Herverdelbaar:** U dient één pakket te downloaden, dat 32-bits en 64-bits installatieprogramma's bevat. In plaats van een bootstrapper, die beschikbaar is om deze optie los te laten en de installatiebestanden te downloaden, zodra deze uitgevoerd is.

  Opmerking: U kunt uw eigen groep maken en hieraan gekoppeld beleid configureren. Het doel is om alle actieve telefoongids servers in één groep te plaatsen, waar het beleid in de auditmodus staat.
  De rapper en de herdistribueerbaar installateur bevatten ook allebei een bestand policy.xml dat wordt gebruikt als configuratiebestand voor de AMP-connector.

Stap 4: Clientprofiel voor webbeveiliging downloaden

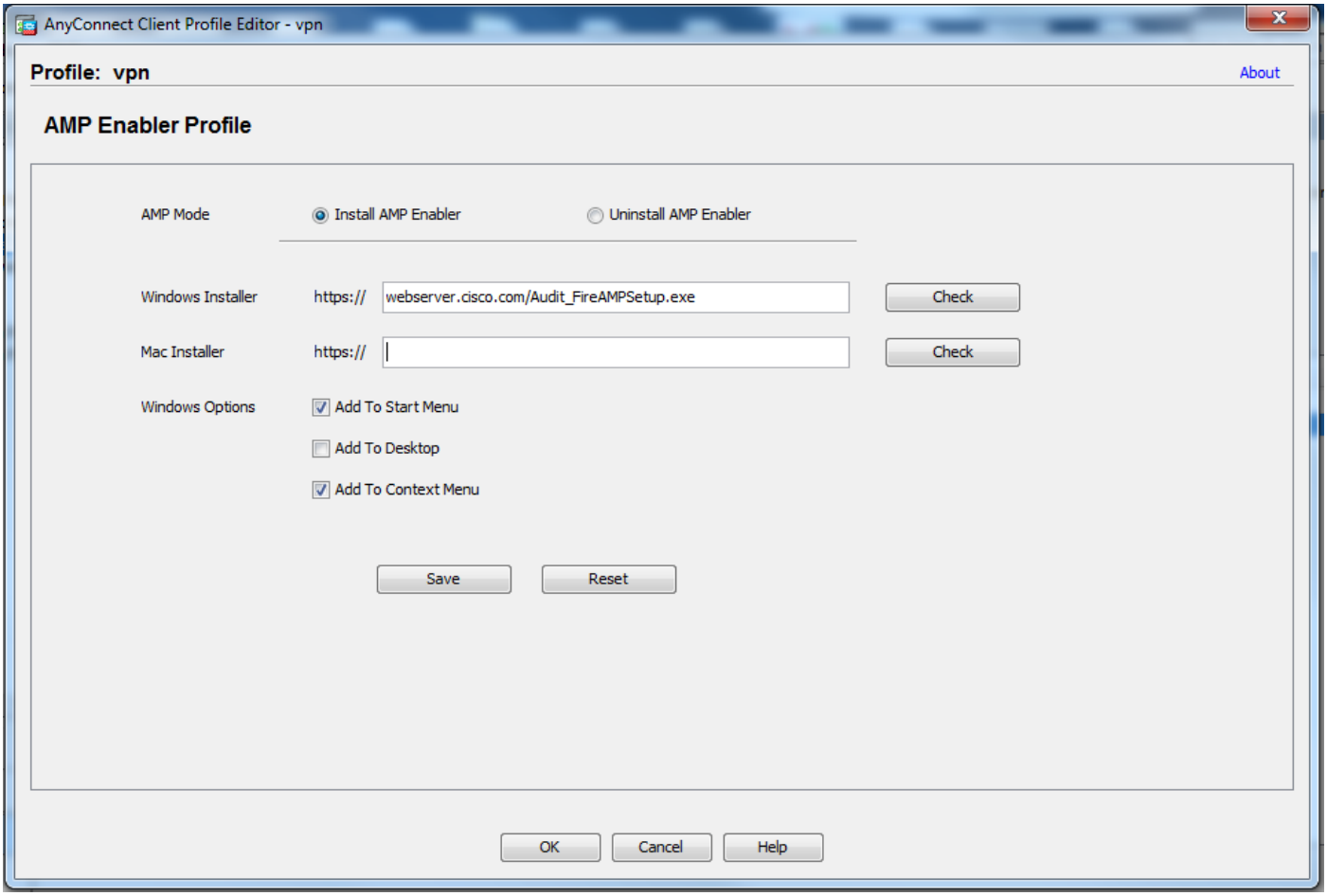
Geef een webserver van het bedrijf of een netwerkaandeel op met de AMP-installateur. Dit wordt het meest gebruikt door bedrijven om bandbreedte op te slaan en vertrouwde installateurs op een gecentraliseerde locatie te plaatsen.

Zorg ervoor dat de HTTPS-link op de eindpunten kan worden bereikt zonder certificaatfout en dat het basiscertificaat in de machinewinkel is geïnstalleerd.

Ga terug naar het AMP-profiel dat voor de ASA is gemaakt (stap 1) en bewerk **AMP Enabler-profiel**:

1. Klik voor de AMP-modus op de radioknop **Installeer AMP Enabler**.
2. Voeg in het veld **Windows Installatieprogramma** de IP voor de webserver en het bestand voor FireAMP toe.
3. Windows-opties zijn optioneel.

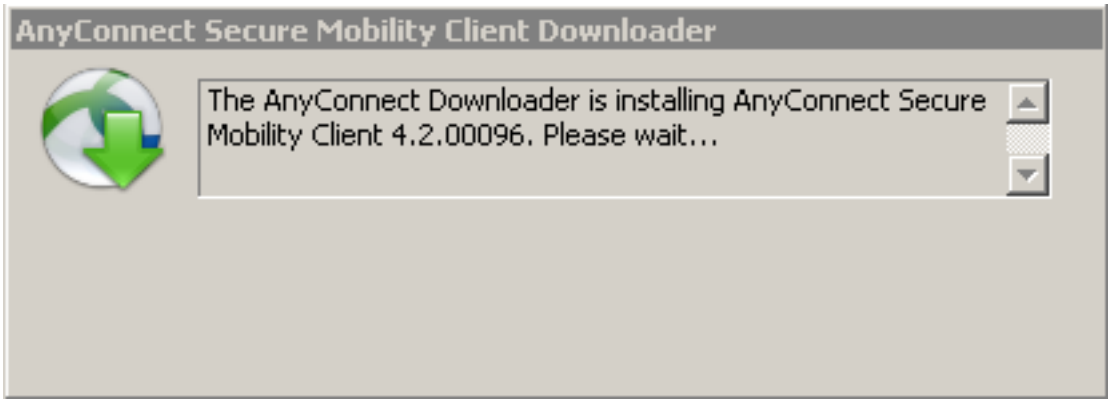
   Klik op **OK** en pas de wijzigingen toe.



Stap 5: Connect met AnyConnect en controleer de installatie van de module

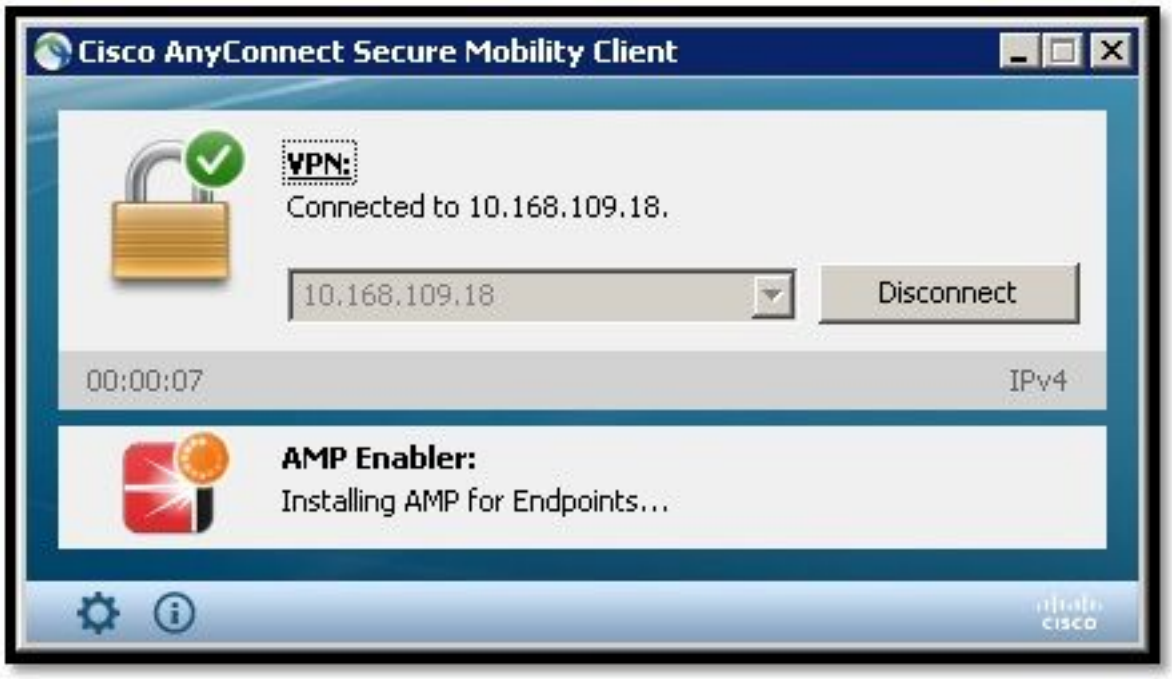
Wanneer een VPN-gebruiker AnyConnect aansluit, drukt ASA de AnyConnect AMP Enabler-module door VPN. Voor reeds ingelogde gebruikers, wordt het aanbevolen om uit te loggen en dan terug in te loggen zodat de functionaliteit wordt ingeschakeld.

```
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%
```



Stap 6: Start VPN Connection installatieautomaat van AMP en AMP-aansluiting

Zodra u op de knop drukt om de VPN te starten, wordt de nieuwe downloader-module gedownload. Dit zal AMP in staat stellen en het AMP pakket van het URL pad hebben gedownload dat u een paar stappen eerder hebt opgegeven.




```
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]
```

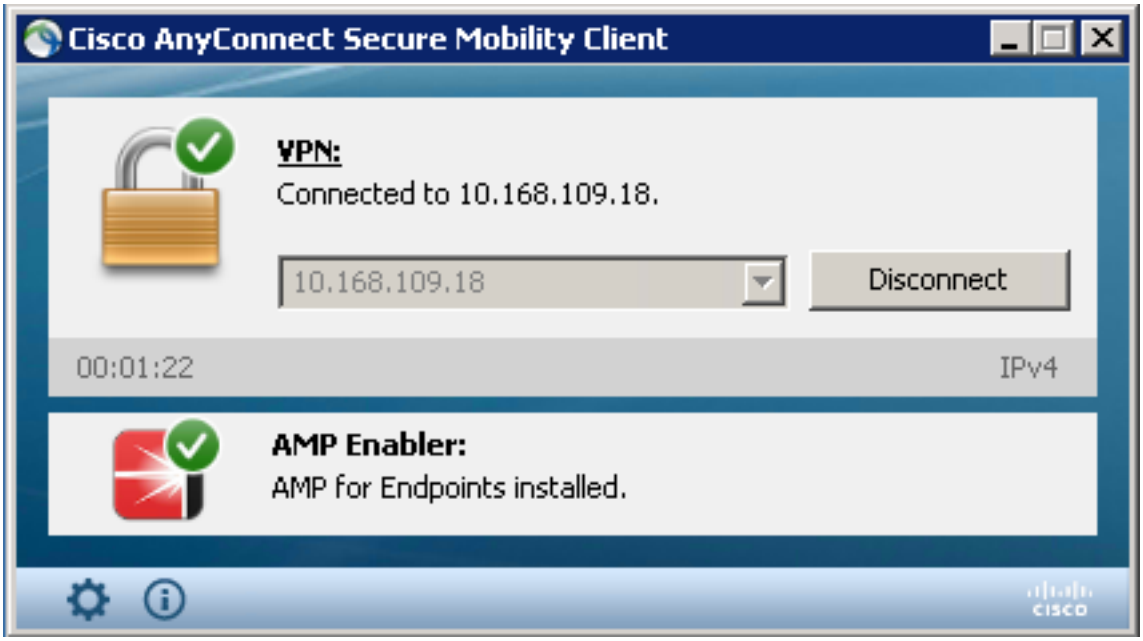
Stap 7: Controleer AnyConnect en controleer of alles is geïnstalleerd

Controleer AnyConnect en controleer of alles correct geïnstalleerd is nadat de VPN is aangesloten en de configuratie van de webserver is geïnstalleerd.

In services.msc kunt u een nieuwe dienst vinden die CiscoAMP_5.1.3 wordt genoemd. In de opdracht PowerShell zien we:

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

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



Met het installatieprogramma van AMP worden nieuwe stuurprogramma's aan het Windows-besturingssysteem toegevoegd. U kunt de driverquery-opdracht gebruiken om een lijst van de stuurprogramma's op te geven.

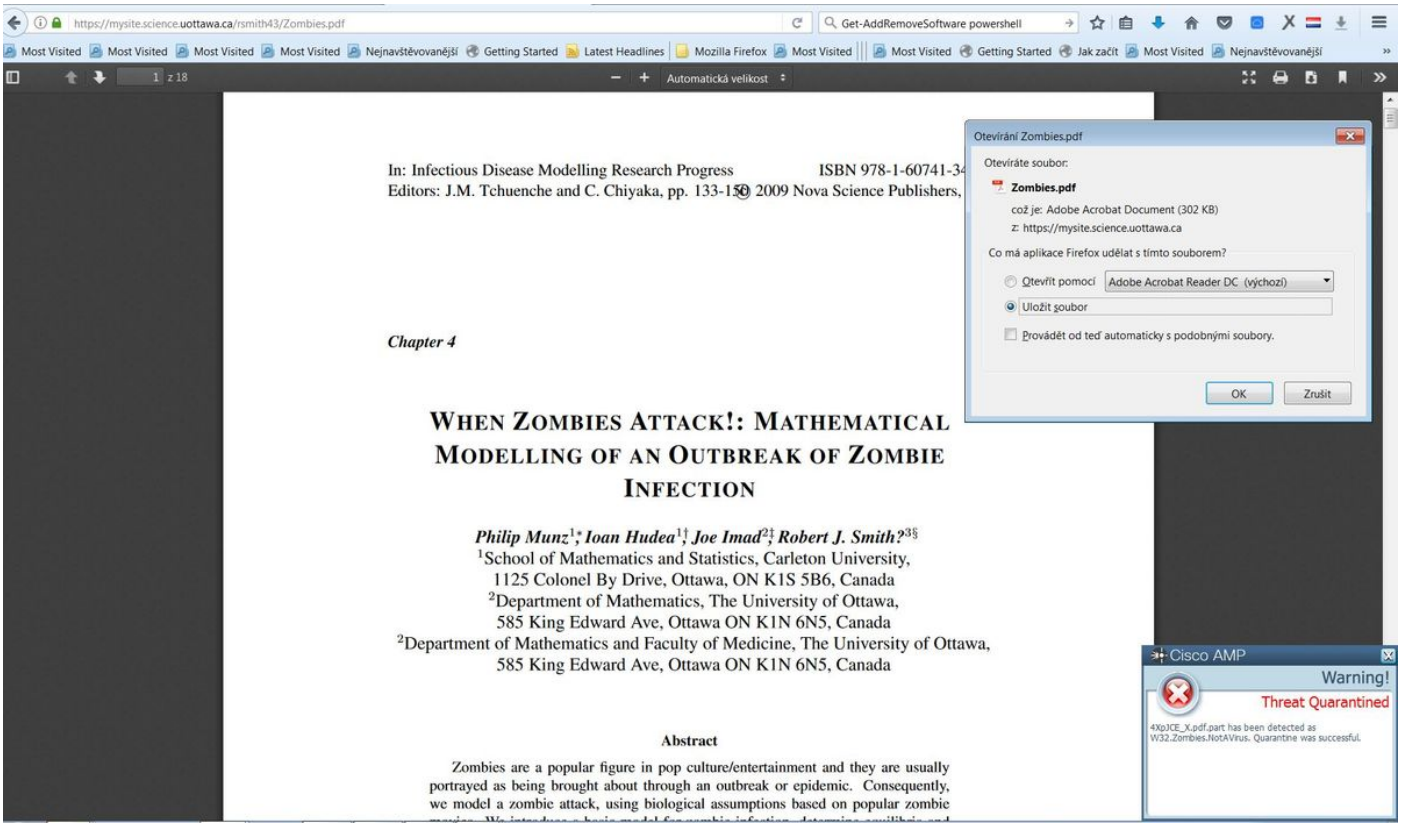
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

Stap 8: Testen met een Eicar String in een PDF-bestand van Zombies

Test met een Eicar string in een PDF-bestand van Zombies in een testcomputer om te controleren of het kwaadaardige bestand in quarantaine staat.



In: Infectious Disease Modelling Research Progress ISBN 978-1-60741-3
Editors: J.M. Tchuenche and C. Chiyaka, pp. 133-158 © 2009 Nova Science Publishers,

Chapter 4

WHEN ZOMBIES ATTACK!: MATHEMATICAL MODELLING OF AN OUTBREAK OF ZOMBIE INFECTION

Philip Munz[1]*, Ioan Hudea*[1]*, Joe Imad*[2]*, Robert J. Smith?*[3§]
[1]School of Mathematics and Statistics, Carleton University,
1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada
[2]Department of Mathematics, The University of Ottawa,
585 King Edward Ave, Ottawa ON K1N 6N5, Canada
[2]Department of Mathematics and Faculty of Medicine, The University of Ottawa,
585 King Edward Ave, Ottawa ON K1N 6N5, Canada

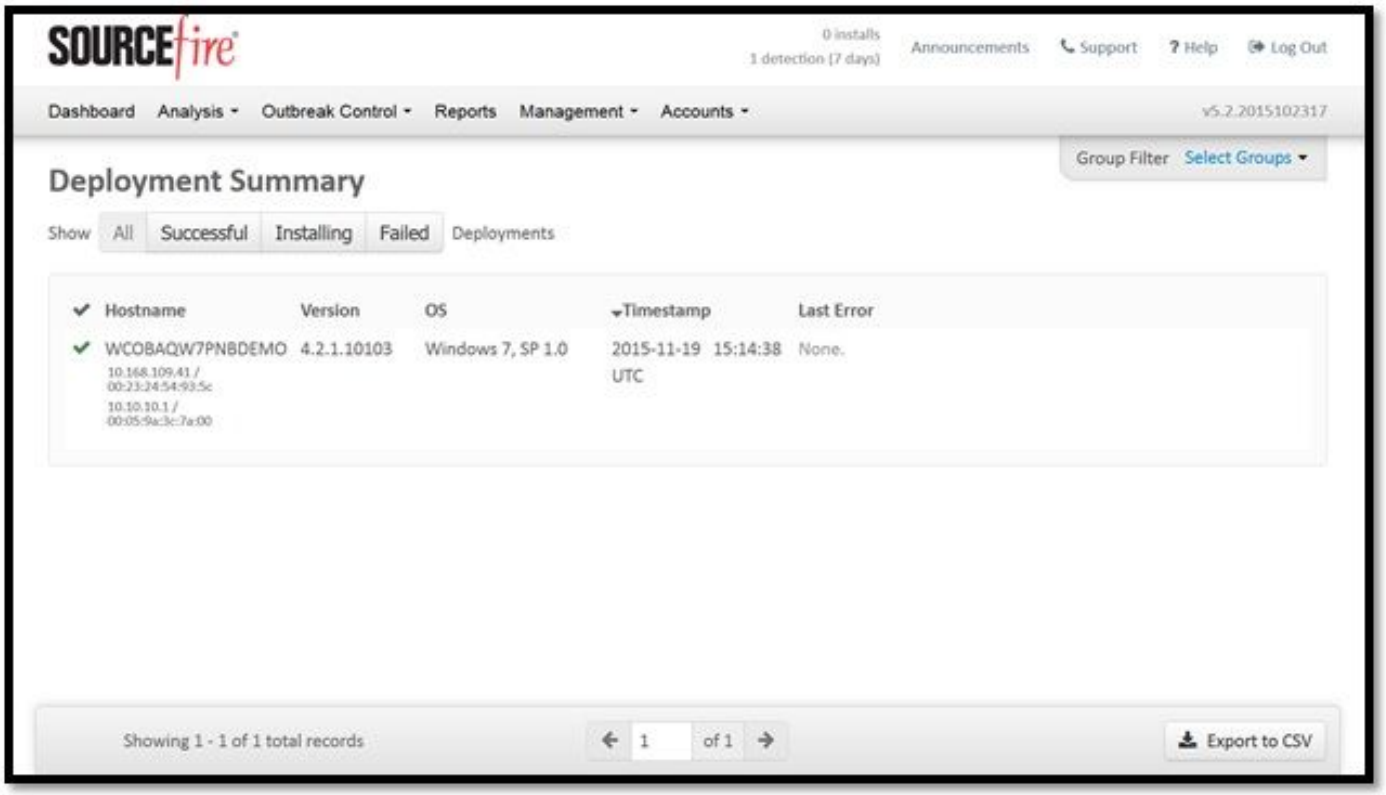
Abstract

Zombies are a popular figure in pop culture/entertainment and they are usually portrayed as being brought about through an outbreak or epidemic. Consequently, we model a zombie attack, using biological assumptions based on popular zombie

Zombies.pdf bevat oorlogen als touwtje

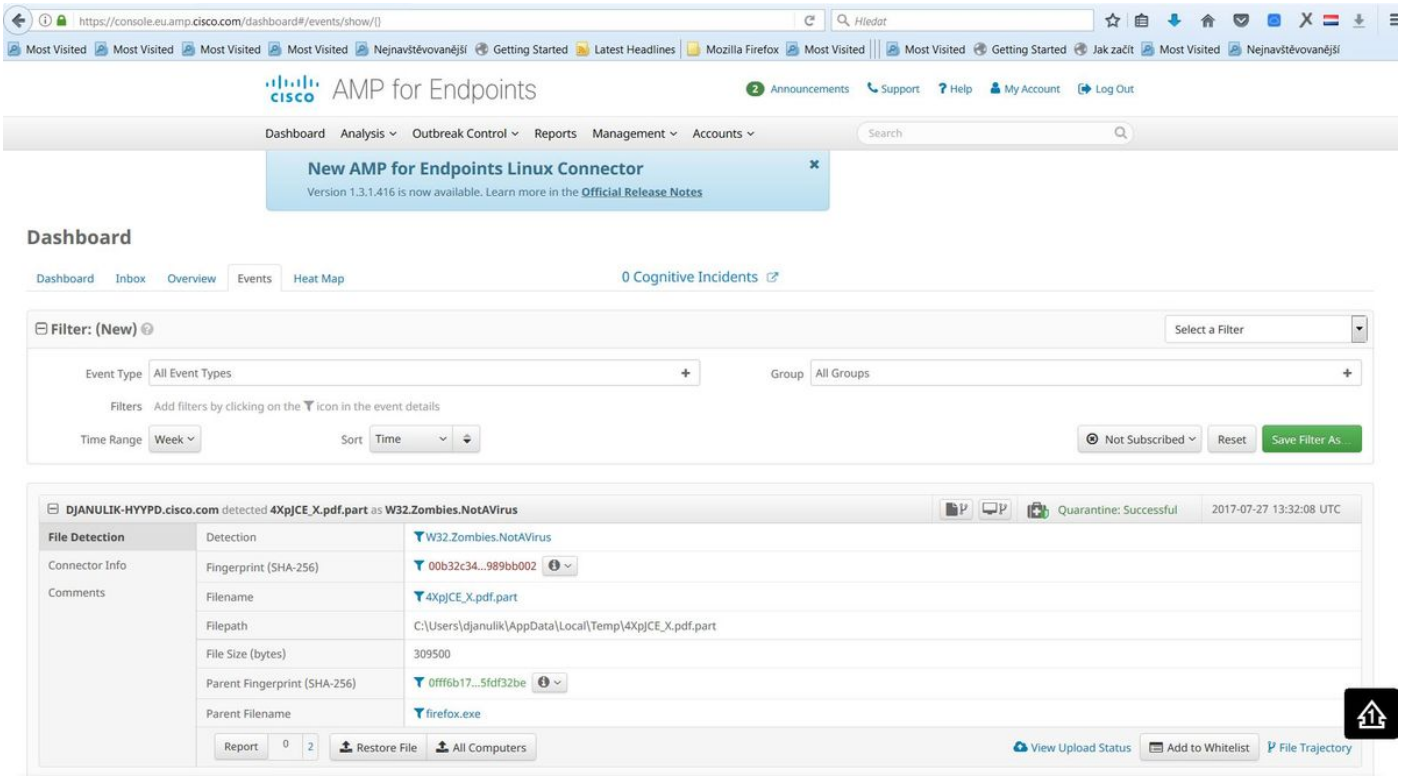
Stap 9: Samenvatting van implementatie

Deze pagina toont u een lijst van succesvolle en mislukte installaties van de connector van FireAMP evenals de installaties die momenteel in bedrijf zijn. U kunt naar **Management > Deployment Summary** gaan.



Stap 10: Detectie van bedreigingen

Zombies.pdf zorgde voor een quarantaine-event en stuurde naar het AMP-dashboard.



Quarantine Event

Aanvullende informatie

Om je AMP account te krijgen, kun je je inschrijven bij de ATS-universiteit. Dit geeft een overzicht van AMP-functionaliteit in LAB.

Gerelateerde informatie

- AMP-functie configureren
- Technische ondersteuning en documentatie – Cisco Systems