通過AnyConnect 4.x和AMP Enabler安裝和配置AMP模組

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[通過ASA的AMP啟用程式的AnyConnect部署](#)
[第1步：配置AnyConnect AMP啟用程式客戶端配置檔案](#)
[第2步：編輯組策略下載AnyConnect AMP啟用程式](#)
[步驟3:下載FireAMP策略](#)
[第4步：下載網路安全客戶端配置檔案](#)
[第5步：使用AnyConnect連線並驗證模組的安裝](#)
[第6步：啟動VPN連線安裝AMP啟用程式和AMP聯結器](#)
[第7步：檢查AnyConnect並驗證是否已安裝所有裝置](#)
[第8步：使用殭屍PDF檔案中包含的Eicar字串進行測試](#)
[第9步：部署摘要](#)
[步驟10:執行緒檢測驗證](#)
[其他資訊](#)
[相關資訊](#)

簡介

本文逐步完成使用AnyConnect安裝高級惡意軟體防護(AMP)聯結器的步驟。

AnyConnect AMP啟用程式用作部署面向終端的AMP的媒介。它本身沒有任何能力判定檔案的處置情況。它將面向終端的AMP軟體從ASA推送到終端。安裝AMP後，它會使用雲容量檢查檔案性質。進一步的AMP服務可以將檔案提交到名為ThreatGrid的動態分析中，以便對未知檔案行為進行評分。如果符合某些專案，這些檔案可能被認定為惡意檔案。這在零日攻擊中非常有用。

必要條件

需求

- AnyConnect安全行動化使用者端版本4.x
- FireAMP/AMP端點版
- 自適應安全裝置管理器(ASDM)版本7.3.2或更高版本

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用軟體版本9.5.1的調適型安全裝置(ASA)5525
- Microsoft Windows 7 Professional 64位版AnyConnect安全00096動客戶端4.2.1
- ASDM版本7.5.1(12)

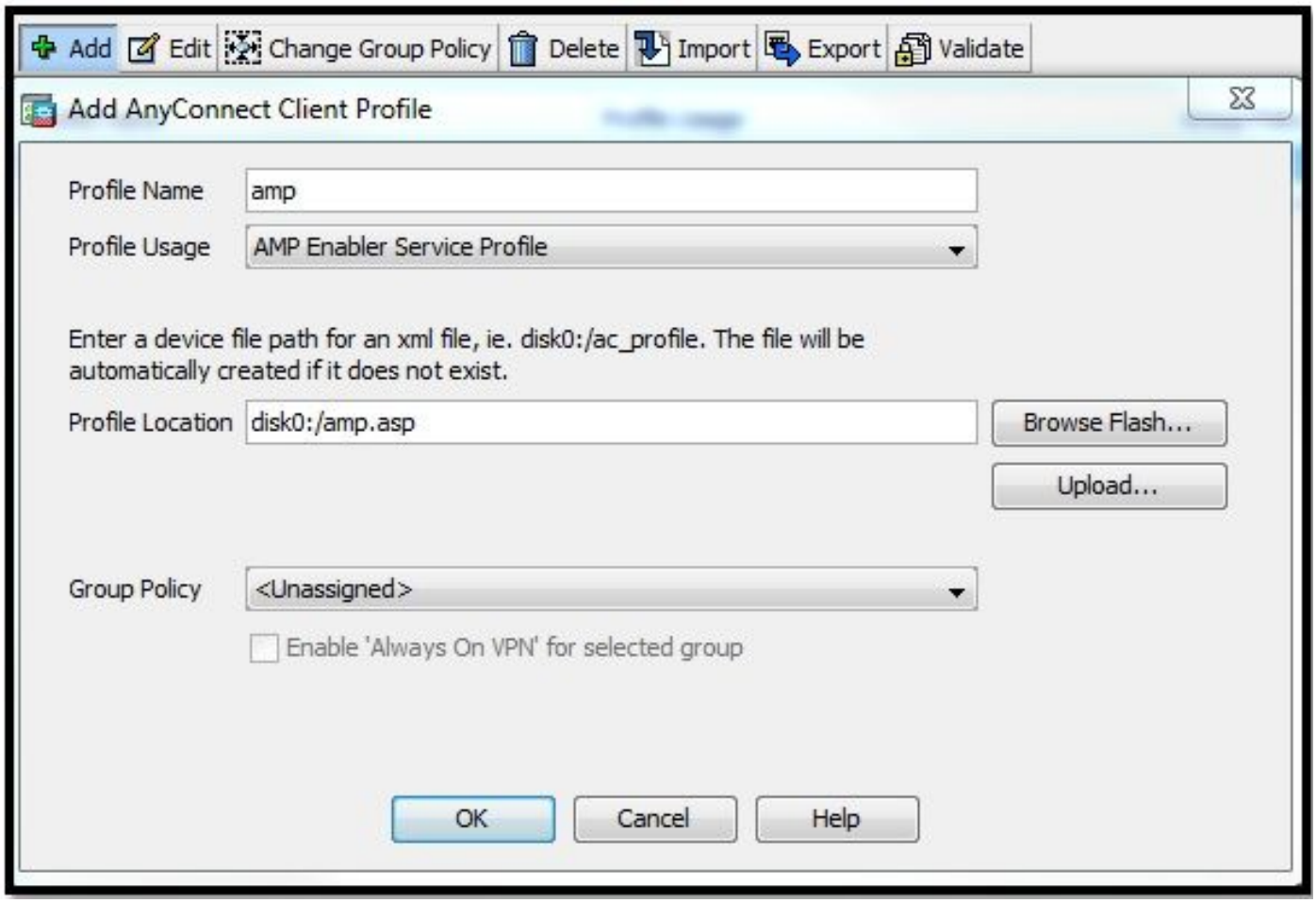
通過ASA的AMP啟用程式的AnyConnect部署

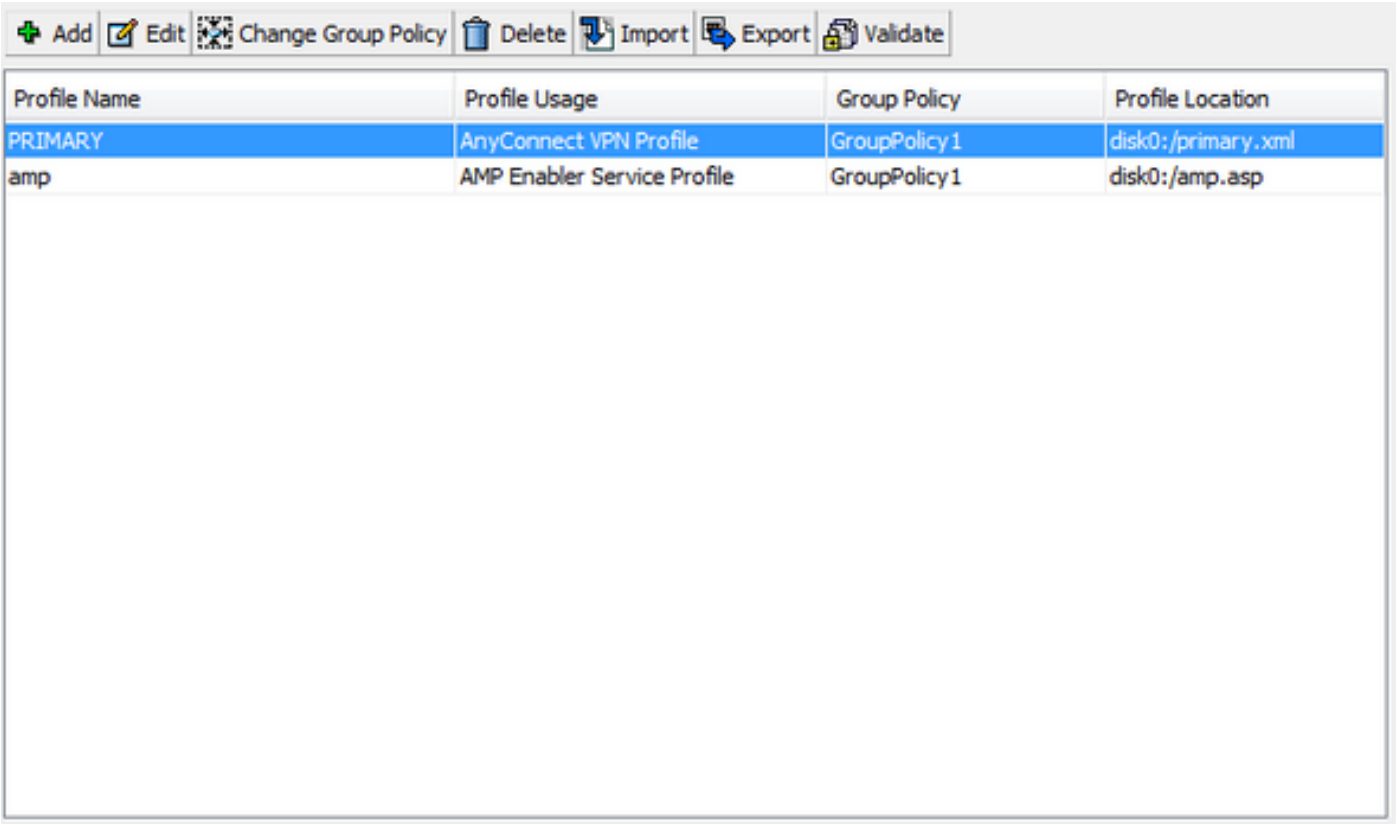
設定中涉及的步驟如下：

- 配置AnyConnect AMP Enabler客戶端配置檔案。
- 編輯AnyConnect VPN組策略並下載AMP啟用程式服務配置檔案。
- 登入到AMP儀表板以獲取聯結器URL下載連結。
- 驗證使用者電腦上的安裝。

第1步：配置AnyConnect AMP啟用程式客戶端配置檔案

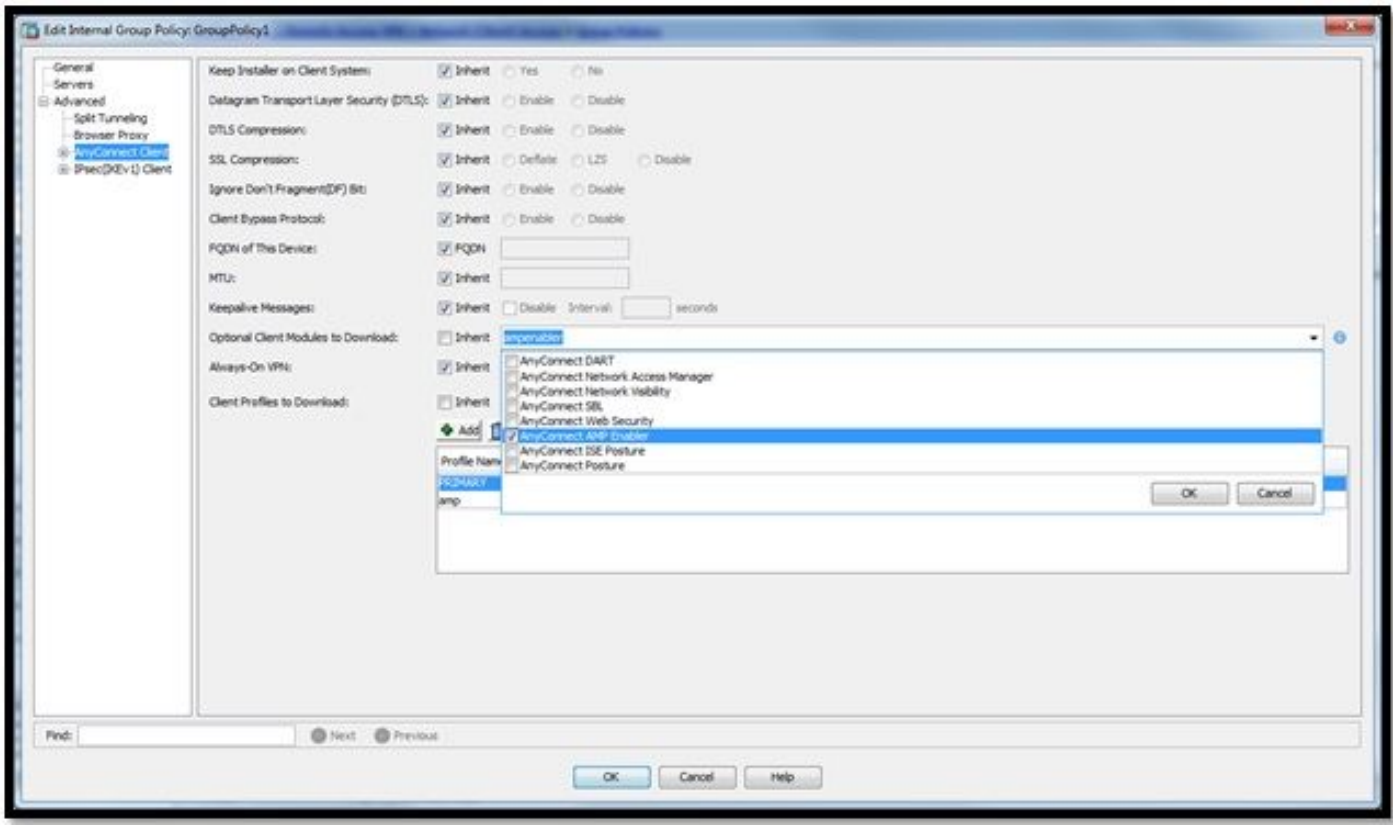
- 導航到**Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Client Profile**。
- 新增**AMP Enabler Service Profile**。





第2步：編輯組策略下載AnyConnect AMP啟用程式

- 導航到Configuration > Remove Access VPN > Group Policies > Edit。
- 轉到Advanced > AnyConnect Client > Optional Client Modules to Download。
- 選擇AnyConnect AMP Enabler。



步驟3:下載FireAMP策略

附註：繼續之前，請檢查系統是否滿足終端AMP Windows聯結器的要求。

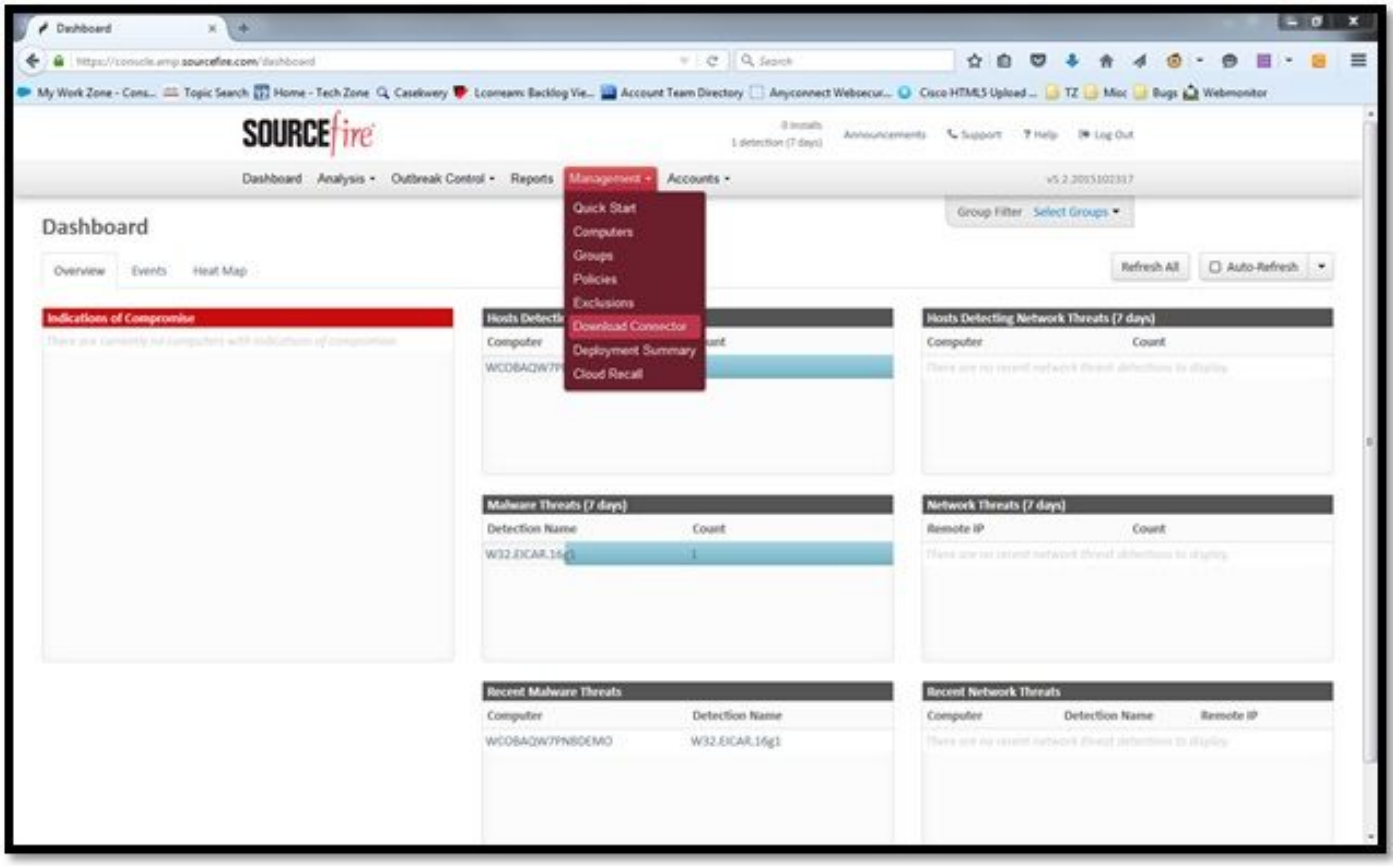
面向終端的AMP Windows聯結器的系統要求

這些是基於Windows作業系統的FireAMP聯結器的最低系統要求。FireAMP聯結器支援這些作業系統的32位和64位版本。最新的AMP文檔可在AMP部署中找到

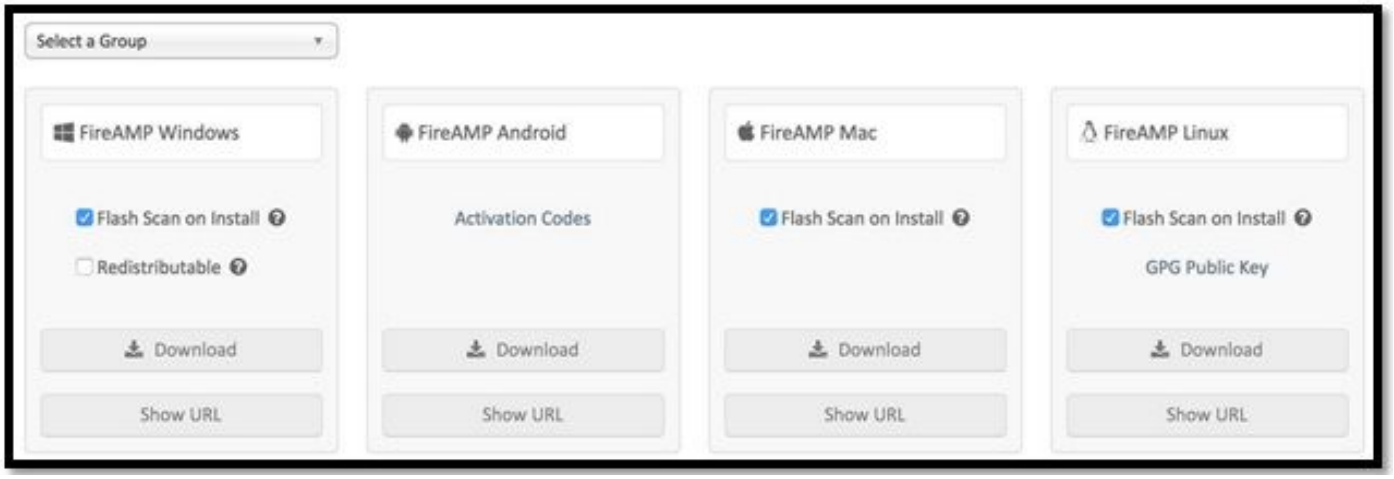
作業系統	處理器	記憶體	磁碟空間、僅雲模式	磁碟空間
Microsoft Windows 7	1 GHz或更快的處理器	1 GB RAM	150 MB可用硬碟空間 — 僅雲模式	1GB可用硬碟空間 — TETRA
Microsoft Windows 8和8.1（需要FireAMP聯結器5.1.3或更高版本）	1 GHz或更快的處理器	512 MB記憶體	150 MB可用硬碟空間 — 僅雲模式	1GB可用硬碟空間 — TETRA
Microsoft Windows Server 2003	1 GHz或更快的處理器	512 MB記憶體	150 MB可用硬碟空間 — 僅雲模式	1GB可用硬碟空間 — TETRA
Microsoft Windows Server 2008	2 GHz或更快的處理器	2 GB RAM	150 MB可用硬碟空間 — 僅雲模式	1GB可用硬碟空間 — TETRA
Microsoft Windows Server 2012（需要FireAMP聯結器5.1.3或更高版本）	2 GHz或更快的處理器	2 GB RAM	150 MB可用硬碟空間 — 僅雲模式	1 GB可用硬碟空間 — TETRA

最常見的是將AMP安裝程式放在企業Web伺服器上。

若要下載聯結器，請導覽至**管理>下載聯結器**。然後依次選擇type和**Download** FireAMP(Windows、Android、Mac、Linux)。



Download Connector頁面允許您下載每種型別的FireAMP聯結器的安裝程式包。此包可以放置在網路共用上或通過管理軟體分發。



選擇組

- **僅稽核**：根據通過每個檔案計算的SHA-256監視系統。此「僅稽核」模式不會隔離惡意軟體，但會傳送事件作為警報。
- **保護**：使用隔離惡意檔案保護模式。監視檔案複製和移動。
- **分類**：這用於已受感染/感染的電腦上。
- **伺服器:**用於Windows伺服器的安裝套件，其中聯結器的安裝不帶Tetra引擎和DFC驅動程式。此組根據其名稱為非域控制器伺服器設計。
- **域控制器**：此組的預設策略設定為稽核模式，與伺服器組中一樣。關聯此組中的所有Active Directory伺服器，這意味著聯結器將在Windows域控制器上運行。

AMP具有名為TETRA的功能，該功能是完整的防病毒引擎。此選項是每個策略的可選選項。

功能

- **安裝時進行快閃記憶體掃描**：掃描進程在安裝期間運行。執行速度相對較快，建議只運行一次。
- **可再分發**：您應下載一個軟體包，其中包含32位和64位安裝程式。而不是載入程式，該載入程式可以在執行後保持此選項未勾選狀態並下載安裝程式檔案。

  附註：您可以建立自己的組並配置與其關聯的策略。其目的是將所有伺服器（例如Active Directory伺服器）置於一個組中，其中策略處於稽核模式。
  載入程式和可再發行安裝程式還都包含一個policy.xml檔案，該檔案用作AMP聯結器的配置檔案。

第4步：下載網路安全客戶端配置檔案

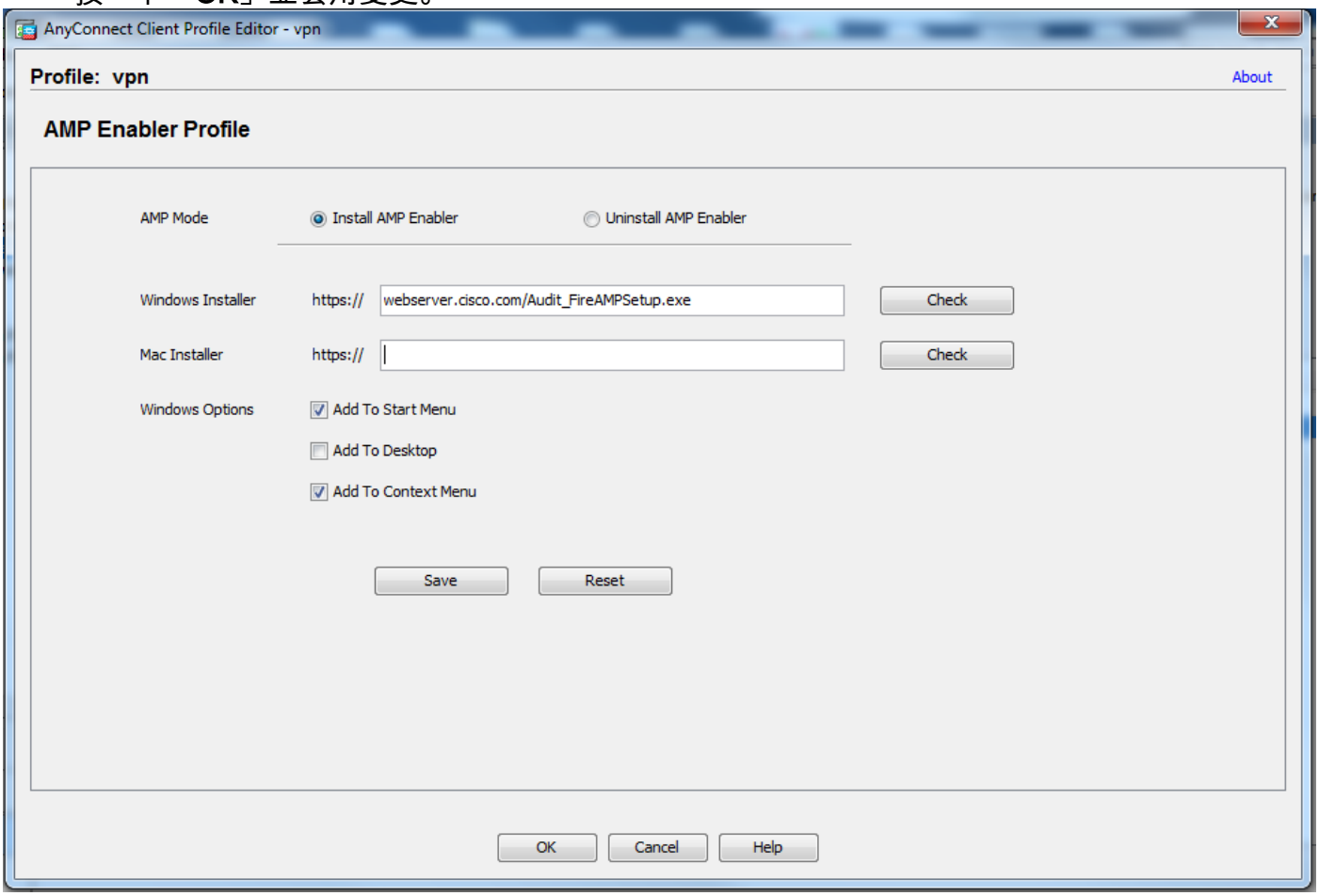
使用AMP安裝程式指定公司Web伺服器或網路共用。這在各公司中最為常用，用於節省頻寬並將受信任的安裝程式集中到位置。

請確保在端點上可以訪問HTTPS連結並且沒有任何證書錯誤，並且根證書已安裝在電腦儲存中。

返回之前在ASA上建立的AMP配置檔案（步驟1），然後編輯**AMP啟用程式配置檔案**:

1. 對於AMP模式，按一下**安裝AMP啟用程式**單選按鈕。
2. 在**Windows Installer**欄位中，為Web伺服器新增IP，為FireAMP新增檔案。
3. Windows選項是可選的。

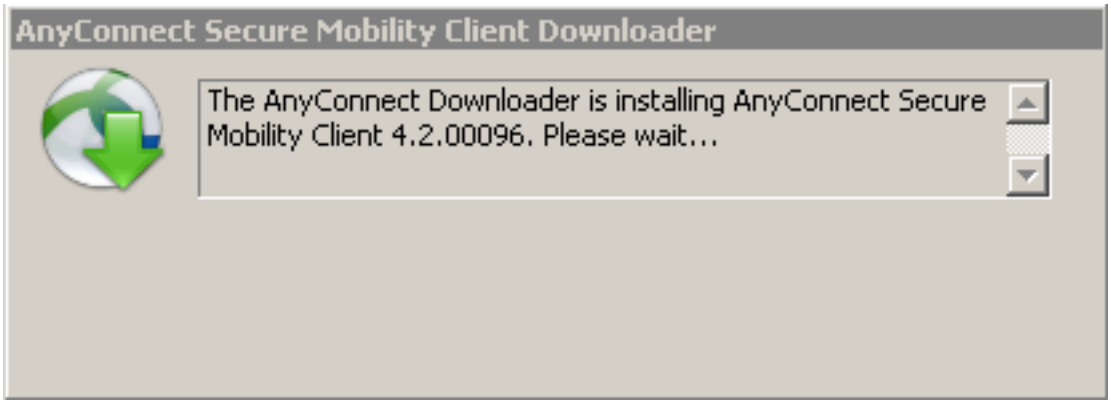
   按一下「**OK**」並套用變更。



第5步：使用AnyConnect連線並驗證模組的安裝

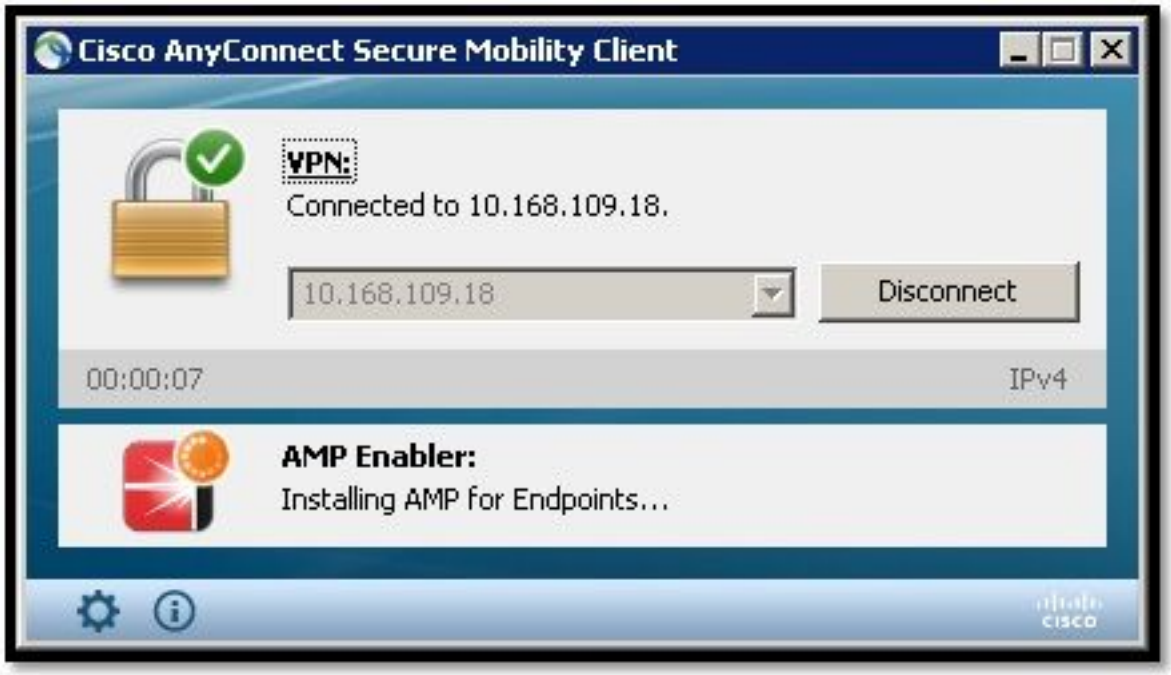
當Anyconnect VPN使用者連線時，ASA會通過VPN推送AnyConnect AMP啟用程式模組。對於已登入的使用者，建議先註銷，然後重新登入以啟用該功能。

```
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%
```



第6步：啟動VPN連線安裝AMP啟用程式和AMP聯結器

按下connect按鈕啟動VPN後，下載新的下載模組。這將具有AMP啟用程式，並從之前指定的幾步中的URL路徑下載AMP包。




```
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]
```

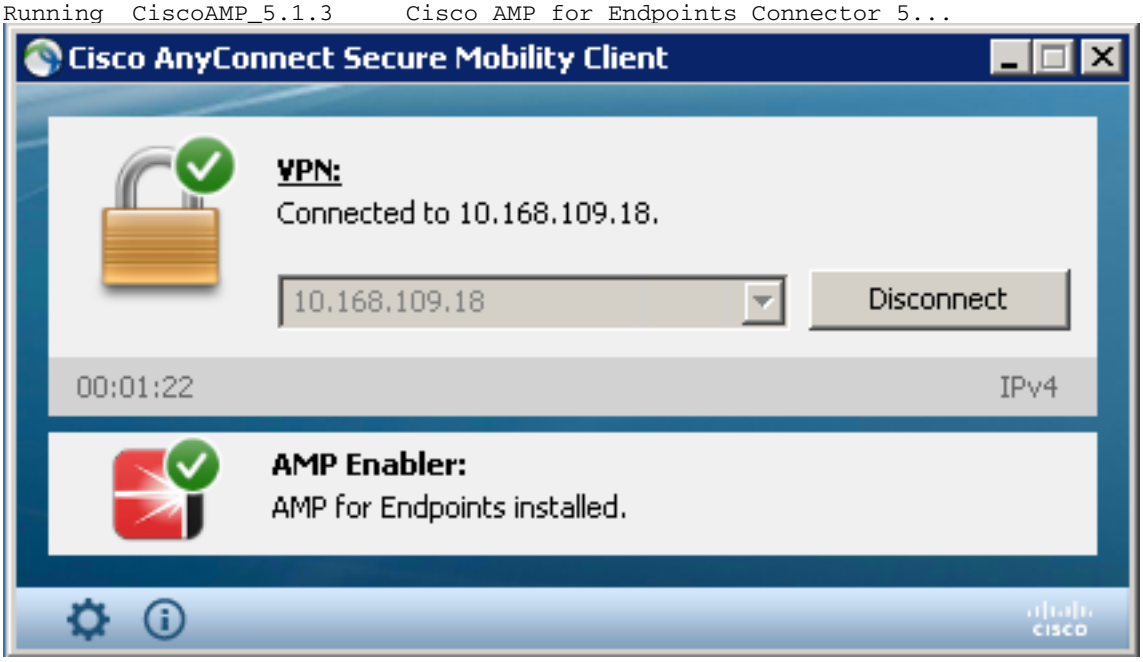
第7步：檢查AnyConnect並驗證是否已安裝所有裝置

連線VPN並安裝Web伺服器配置後，請檢查AnyConnect並驗證是否正確安裝了所有裝置。

在services.msc中，您可以找到名為CiscoAMP_5.1.3的新服務。在Powershell命令中，我們可以看到：

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

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



AMP安裝程式將新驅動程式新增到Windows作業系統。您可以使用driverquery命令列出驅動程式。

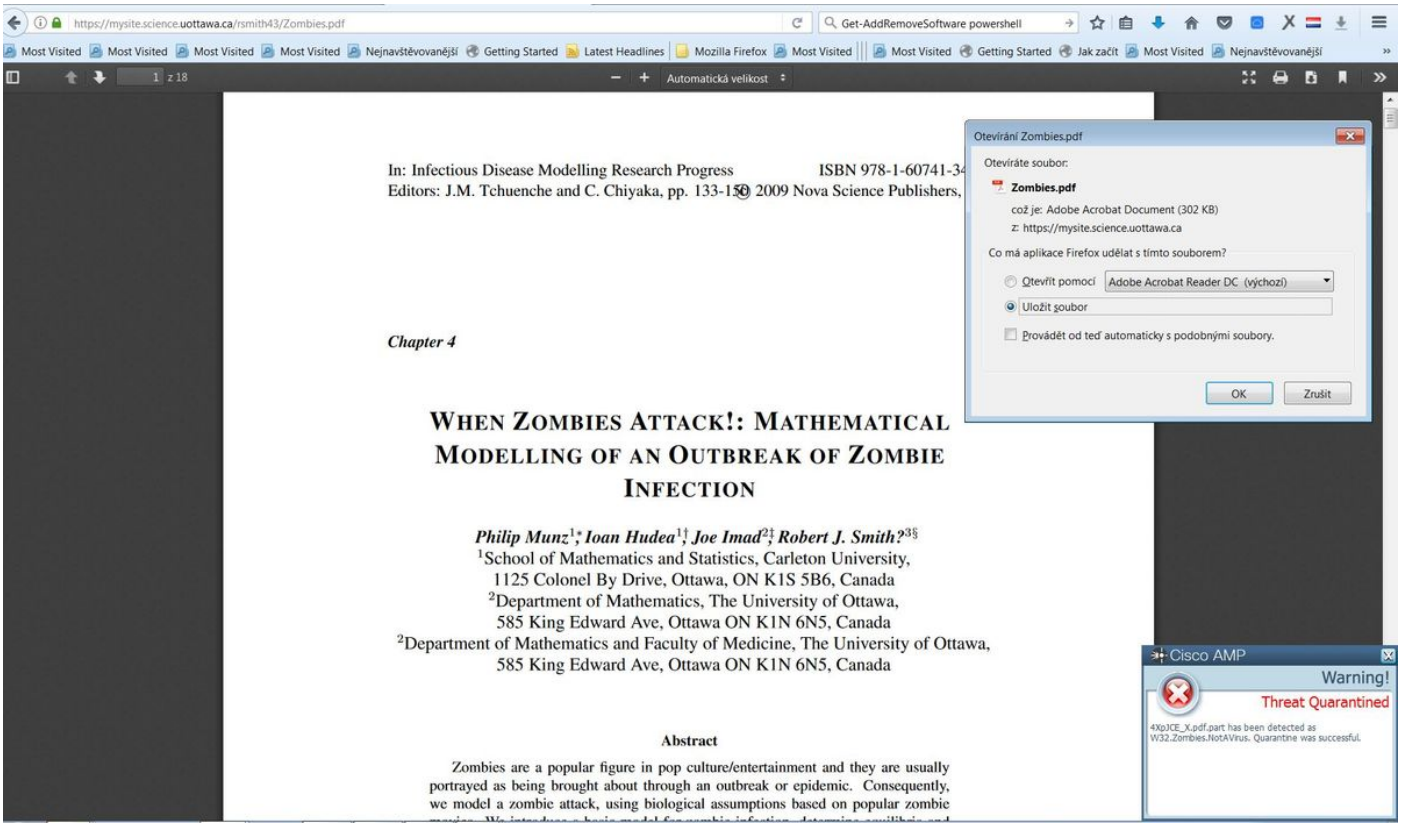
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

第8步：使用殭屍PDF檔案中包含的Eicar字串進行測試

在測試電腦中使用殭屍PDF檔案中包含的Eicar字串進行測試，以驗證是否已隔離惡意檔案。



In: Infectious Disease Modelling Research Progress ISBN 978-1-60741-3
Editors: J.M. Tchuenche and C. Chiyaka, pp. 133-150 © 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

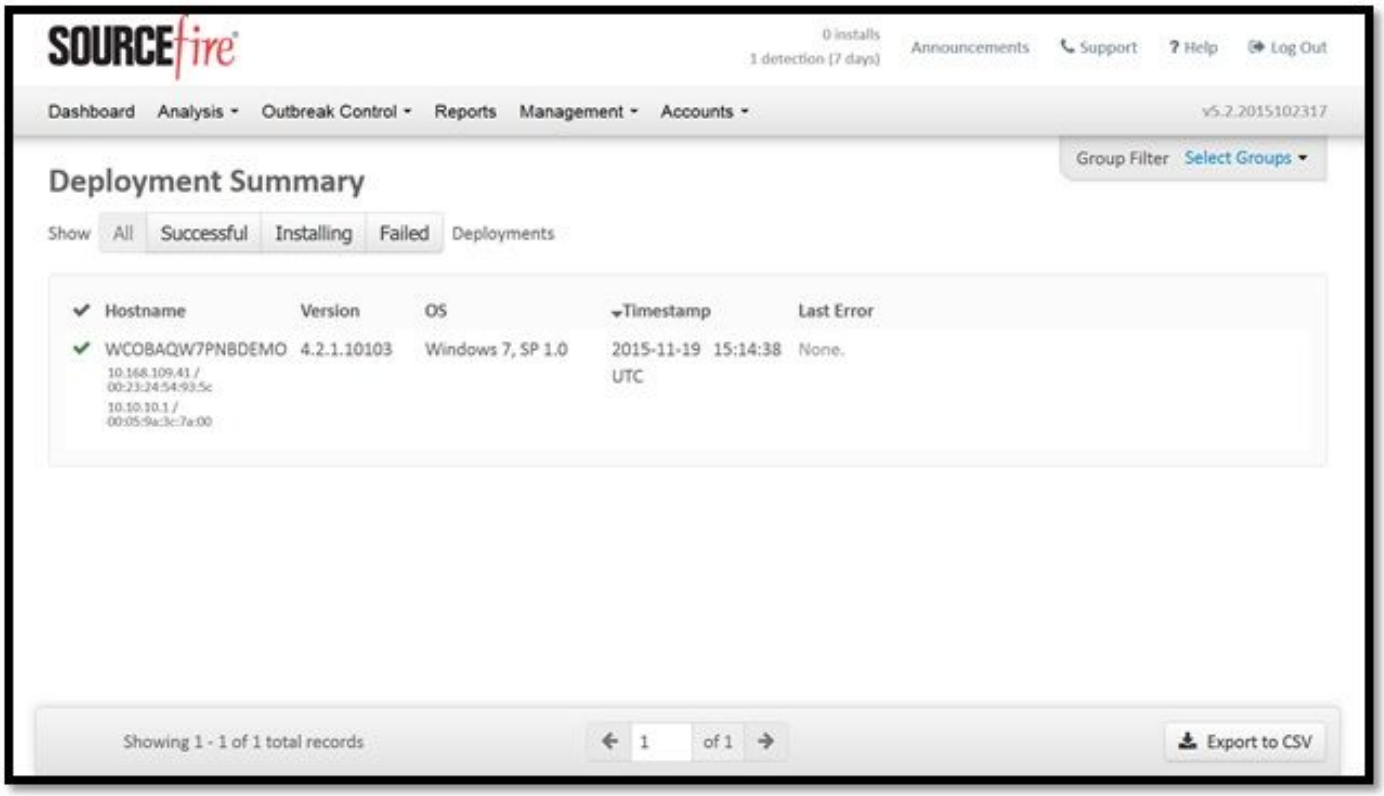
Abstract

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包含Eicar字串

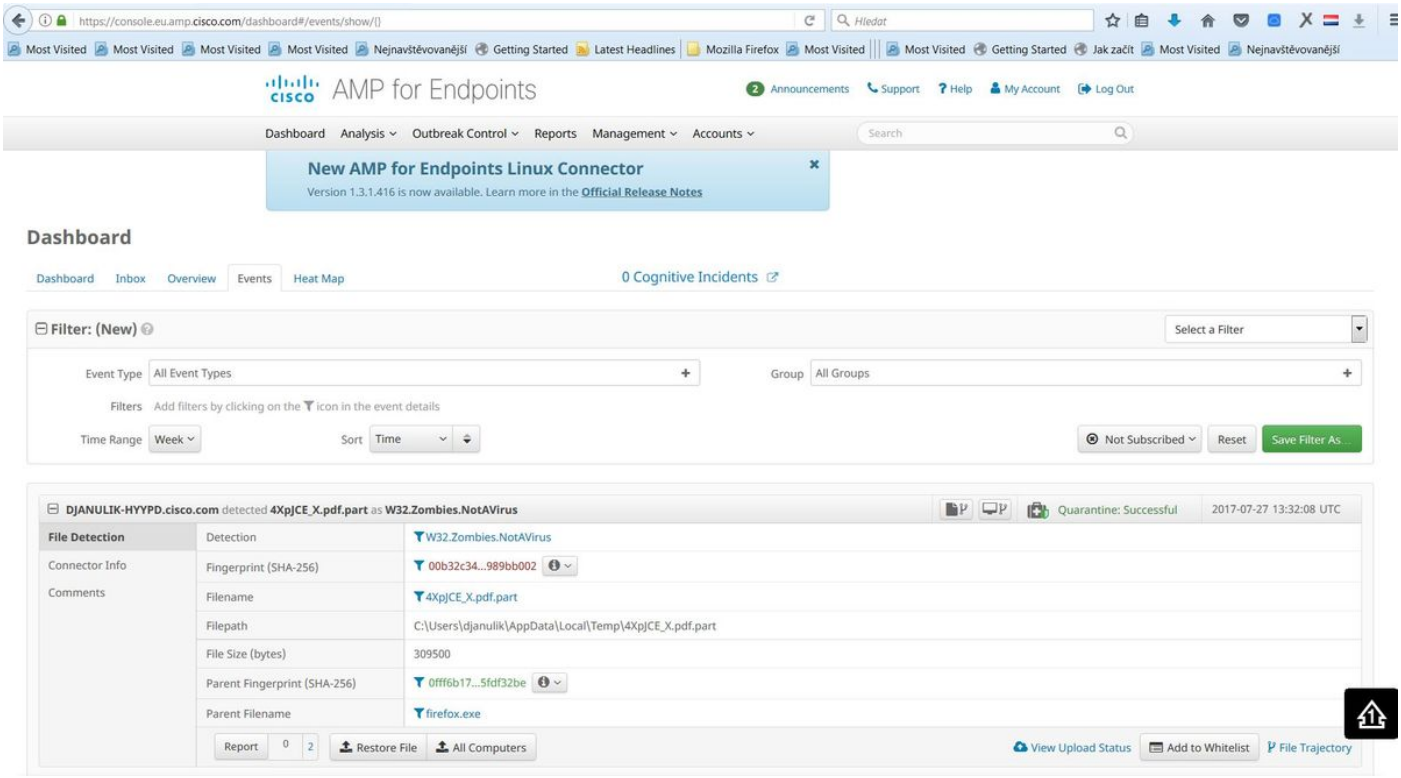
第9步：部署摘要

此頁顯示成功和失敗的FireAMP聯結器安裝以及當前正在進行的安裝清單。您可以轉到**管理>部署摘要**。



步驟10:執行緒檢測驗證

Zombies.pdf觸發隔離事件，傳送到AMP控制面板。



隔離事件

其他資訊

要獲取AMP帳戶，您可以註冊ATS大學。這為您提供了實驗室中的AMP功能的概述。

相關資訊

- 配置AMP啟用程式
- 技術支援與文件 - Cisco Systems