AnyConnect 4.x および AMP イネーブラを介した AMP モジュールのインストールと設定

内容

概要

このドキュメントでは、高度なマルウェア防御(AMP)コネクタをAnyConnectとともにインストールする手順を説明します。

AnyConnect AMPイネーブラは、エンドポイント向けAMPを導入するためのメディアとして使用されます。それ自体はファイルの性質を証明する能力を持っていません。AMP for Endpointsソフトウェアを ASAからエンドポイントにプッシュします。AMPがインストールされると、クラウド容量を使用してファイルの性質を確認します。さらにAMPサービスは、ThreatGridと呼ばれる動的な分析にファイルを送信して、未知のファイルの動作をスコア化できます。これらのファイルは、特定のアーティファクトが満たされると、悪意があると判断される可能性があります。これは、ゼロデイ攻撃に広く使用されています。

前提条件

要件

- AnyConnectセキュアモビリティクライアントバージョン4.x
- FireAMP / エンドポイント向け AMP
- Adaptive Security Device Manager(ASDM)バージョン7.3.2以降

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン9.5.1が稼働する適応型セキュリティアプライアンス(ASA)5525
- Microsoft Windows 7 Professional 64ビット上のAnyConnectセキュアモビリティクライアント4.2.00096
- ASDM バージョン 7.5.1(112)

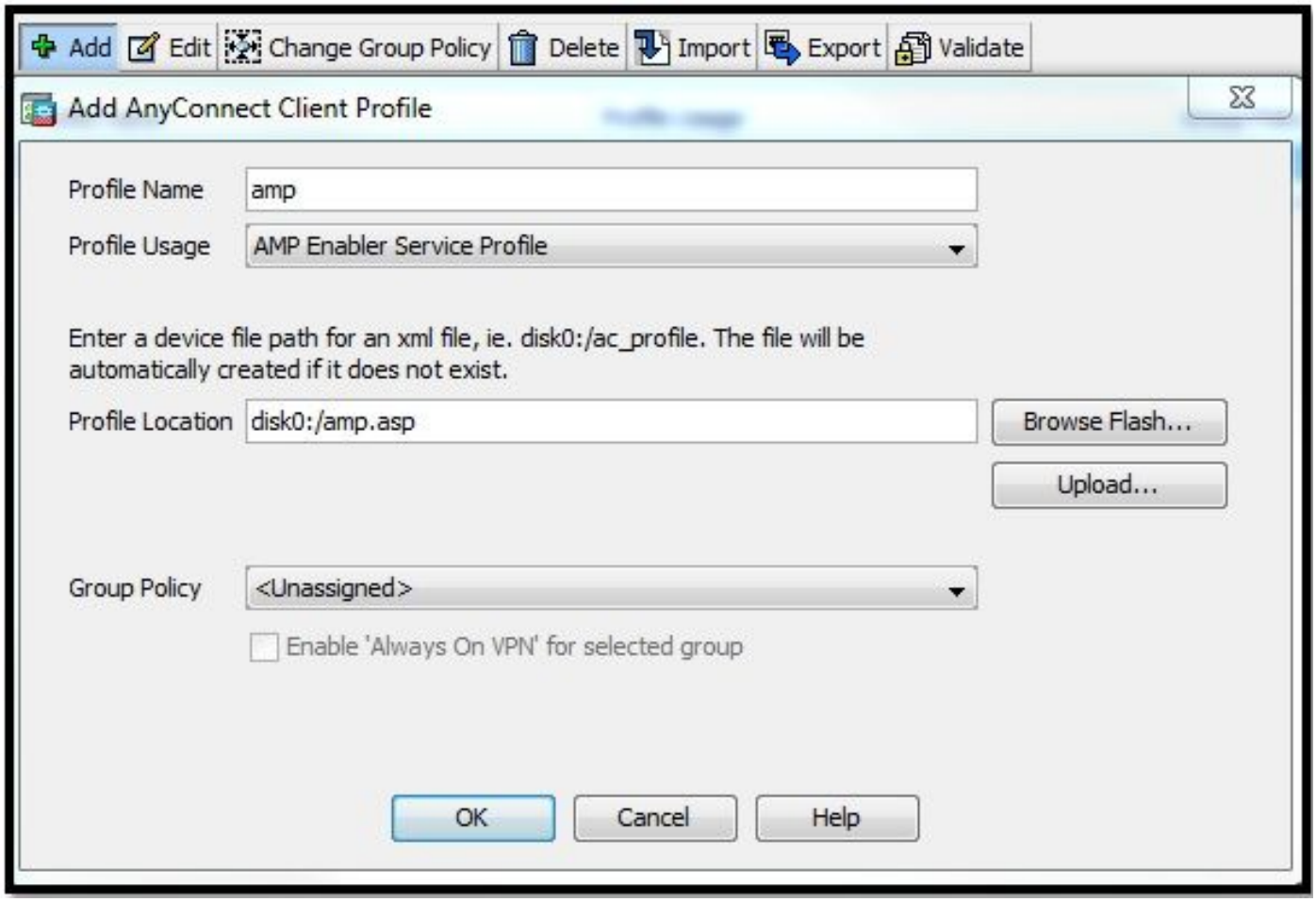
ASA を介した AMP イネーブラのための AnyConnect の導入

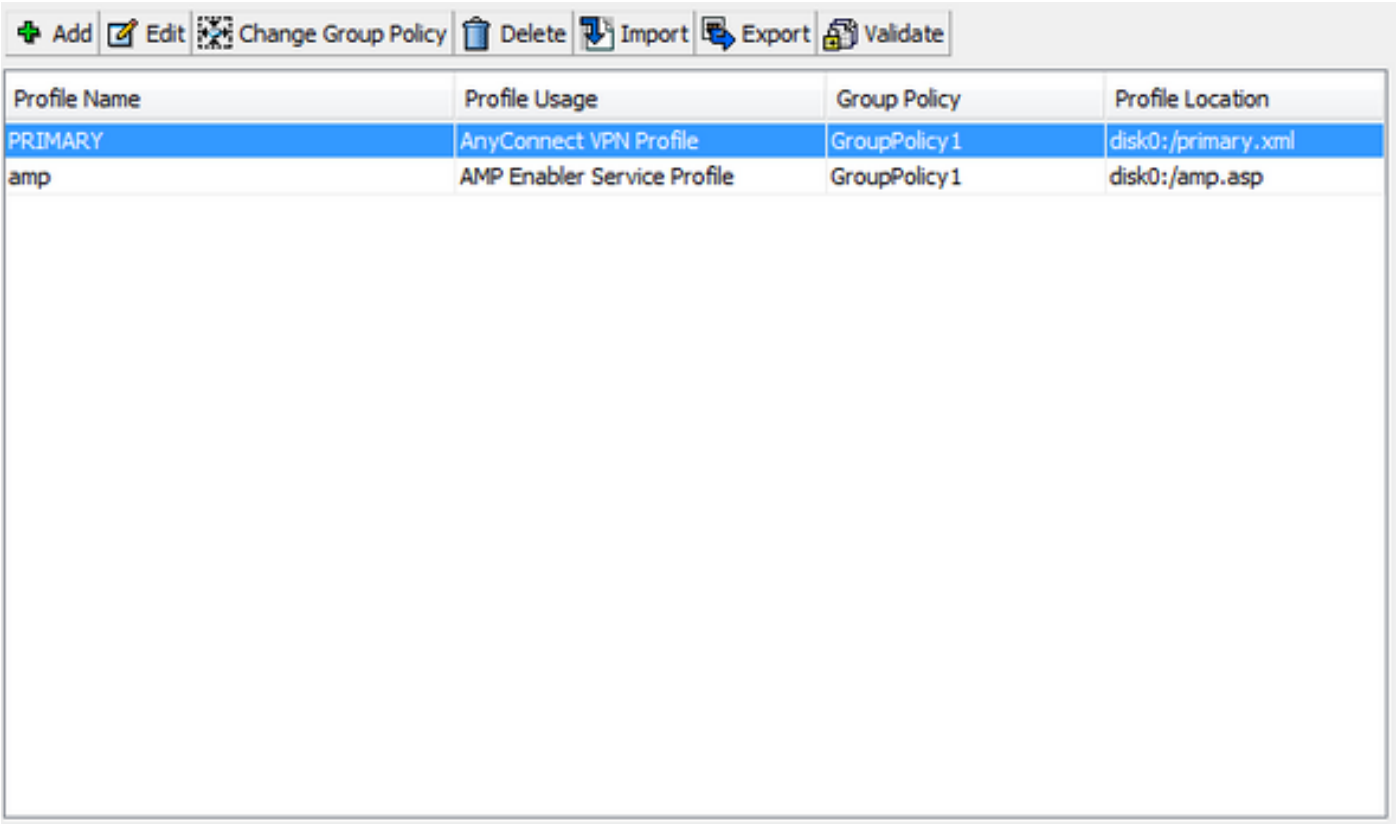
設定に含まれる手順は次のとおりです。

- AnyConnect AMPイネーブラクライアントプロファイルを設定します。
- AnyConnect VPNグループポリシーを編集し、AMPイネーブラサービスプロファイルをダウンロードします。
- AMPダッシュボードにログインして、コネクタURLダウンロードリンクを取得します。
- ユーザ マシンでインストールを検証します。

ステップ 1：AnyConnect AMPイネーブラクライアントプロファイルの設定

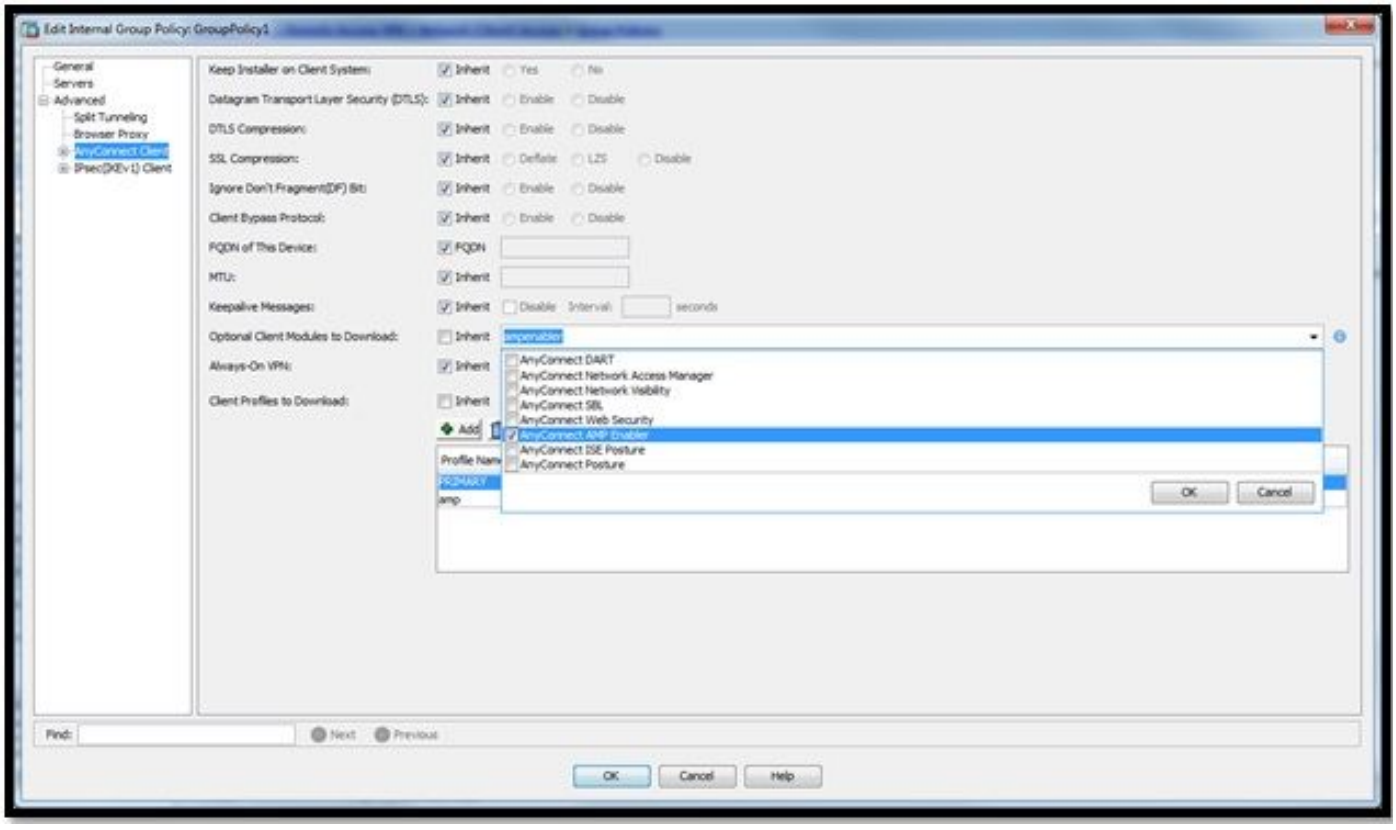
- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile]に移動します。
- AMP Enablerサービス・プロファイルを追加します。





ステップ 2：AnyConnect AMP イネーブラをダウンロードするためのグループ ポリシーの編集

- [Configuration] > [Remove Access VPN] > [Group Policies] > [Edit] の順に移動します。
- [Advanced] > [AnyConnect Client] > [Optional Client Modules to Download]に移動します。
- [AnyConnect AMP Enabler]を選択します。



ステップ 3：FireAMP ポリシーのダウンロード

注：続行する前に、システムがAMP of Endpoints Windows Connectorの要件を満たしているかどうかを確認してください。

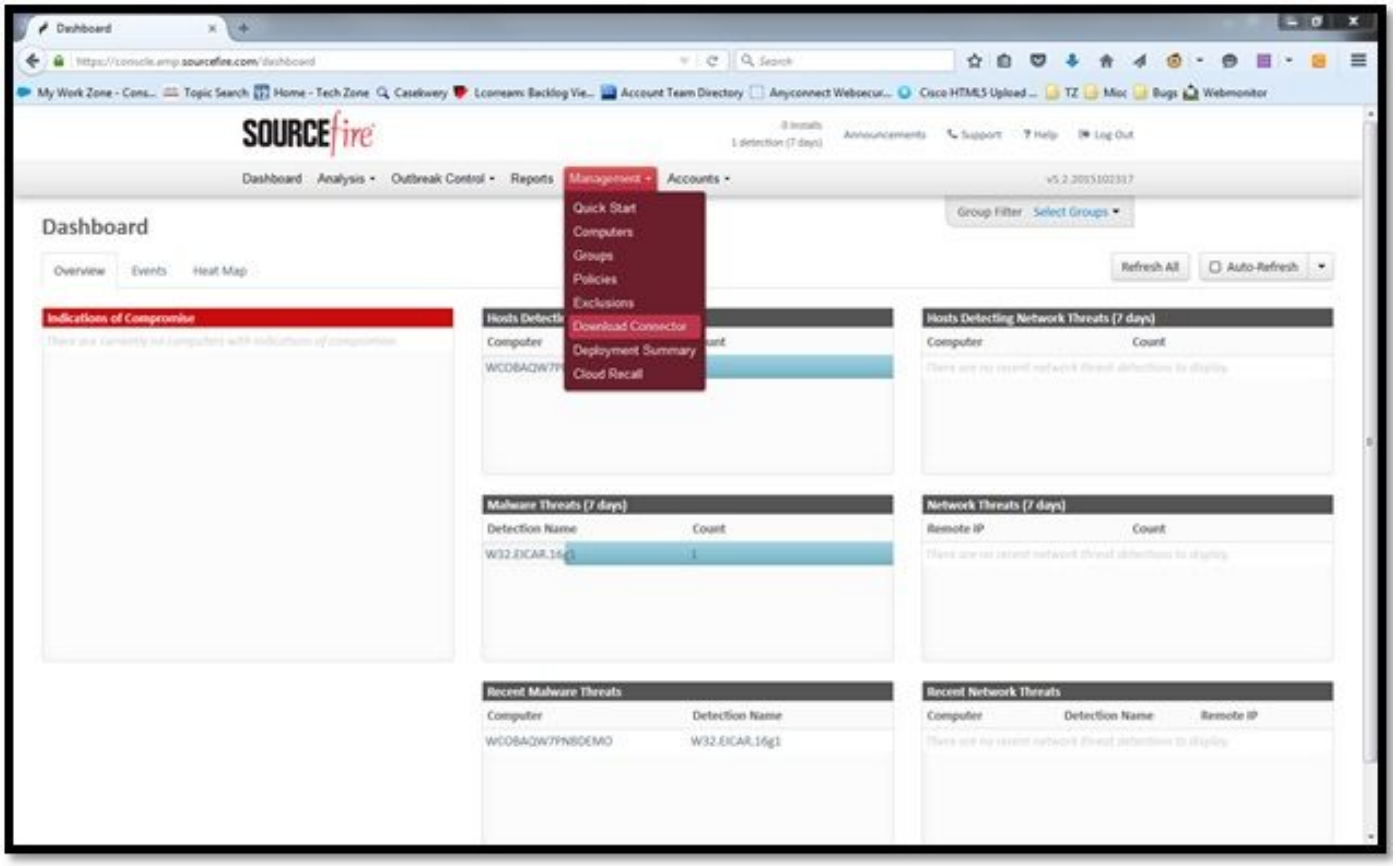
AMP for Endpoints Windows Connector のシステム要件

これらは、Windowsオペレーティングシステムに基づくFireAMPコネクタの最小システム要件です。FireAMP Connector は、次のオペレーティング システムの 32 ビット バージョンと 64 ビット バージョンをサポートします。最新のAMPドキュメントは、AMPの導入で入手できます

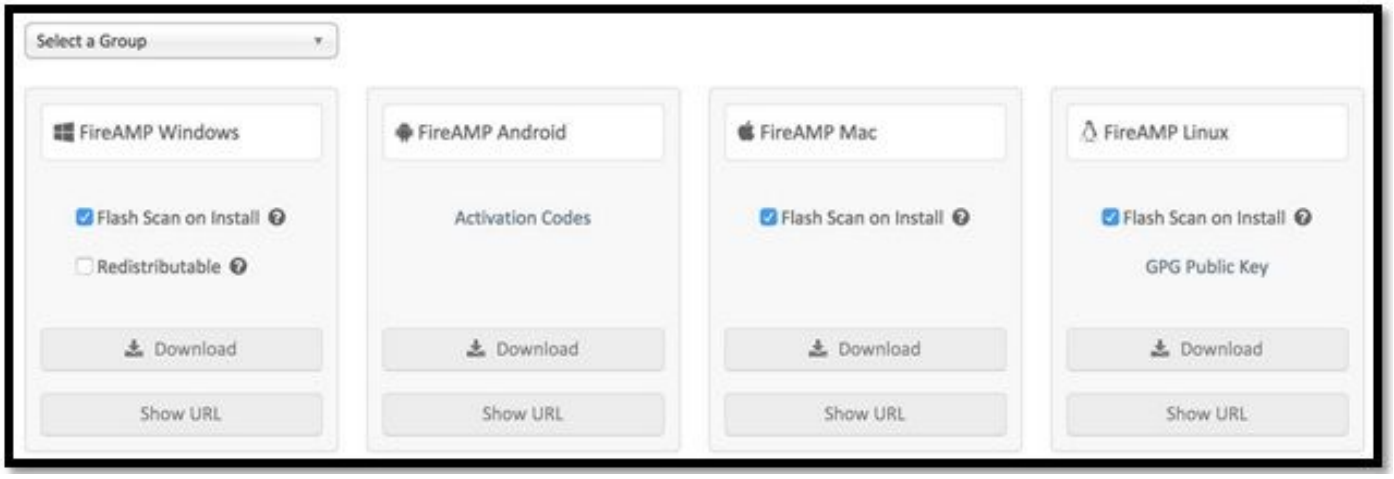
オペレーティング システム	プロセッサ	メモリ	ディスク領域、クラウド専用モード	ディスク領域
Microsoft Windows 7	1 GHz 以上のプロセッサ	メモリ 1 GB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows 8 および 8.1 (FireAMP Connector 5.1.3 以降が必要)	1 GHz 以上のプロセッサ	メモリ 512 MB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GBのハードディスク空き容量 – TETRA
Microsoft Windows Server 2003	1 GHz 以上のプロセッサ	メモリ 512 MB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows Server 2008	2 GHz 以上のプロセッサ	メモリ 2 GB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GBのハードディスク空き容量 – TETRA
Microsoft Windows Server 2012 (FireAMP Connector 5.1.3 以降が必要)	2 GHz 以上のプロセッサ	メモリ 2 GB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GBのハードディスク空き容量 – TETRA

最も一般的なのは、AMPインストーラをエンタープライズWebサーバに配置することです。

コネクタをダウンロードするには、[Management] > [Download Connector] に移動します。次に、[type]を選択し、**[Download** FireAMP (Windows、Android、Mac、Linux)]を選択します。



[Download Connector]ページでは、FireAMPコネクタのタイプごとにインストールパッケージをダウンロードできます。このパッケージは、ネットワーク共有に配置することも、管理ソフトウェアを介して配布することもできます。



[Select a Group]

- **[Audit Only]**：各ファイルで計算されたSHA-256に基づいてシステムを監視します。この監査のみのモードでは、マルウェアは検疫されず、アラートとしてイベントが送信されます。
- **[Protect]**：悪意のあるファイルを隔離する保護モード。ファイルのコピーと移動を監視します。
- **[Triage]**：これは、すでに感染または感染しているコンピュータで使用されます。
- **[Server]**：Windowsサーバ用のインストールスイート。コネクタはTetraエンジンとDFCドライバなしでインストールされます。このグループは、非ドメインコントローラサーバの名前で設計されています。
- **[Domain Controller]**：このグループのデフォルトポリシーは、サーバグループのように監査モ

ードに設定されます。このグループ内のすべてのActive Directoryサーバを関連付けます。これは、コネクタがWindowsドメインコントローラで実行されることを意味します。

AMPには、完全なウイルス対策エンジンであるTETRAという機能があります。このオプションは、ポリシーごとにオプションです。

機能

- **[Flash Scan on Install]**：インストール中にスキャンプロセスが実行されます。比較的迅速に実行でき、1回だけ実行することを推奨します。
- **[Redistributable]**：32ビットおよび64ビットのインストーラを含む1つのパッケージをダウンロードする必要があります。このオプションをオフのままにして、インストーラのファイルをダウンロードするブートストラッパは実行されません。

注：独自のグループを作成し、それに関連付けられたポリシーを設定できます。この目的は、ポリシーが監査モードになっている1つのグループにすべてのActive Directoryサーバを配置することです。
ブートストラッパと再頒布可能インストーラの両方にpolicy.xmlファイルが含まれ、AMPコネクタの設定ファイルとして使用されます。

ステップ 4：Webセキュリティクライアントプロファイルのダウンロード

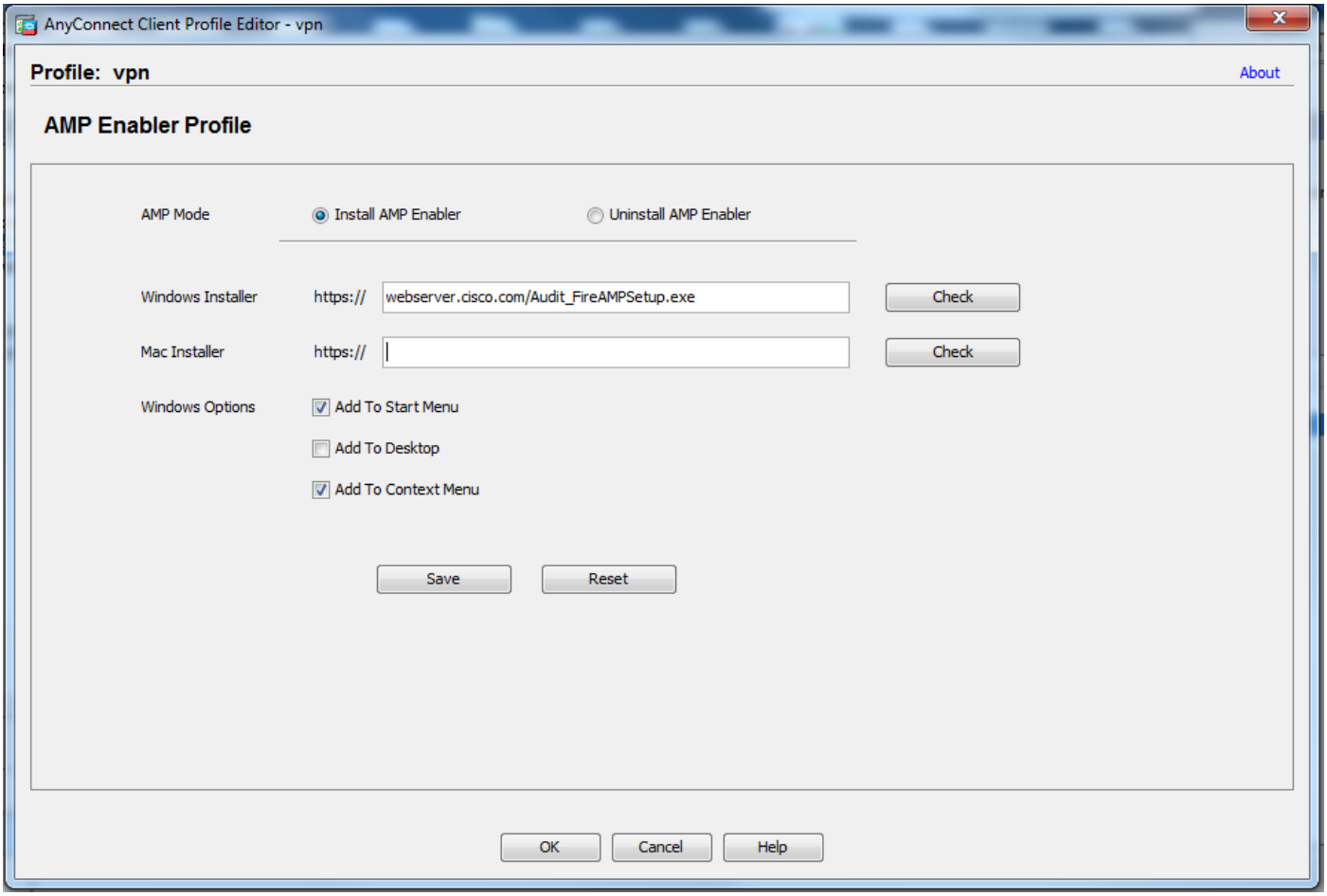
AMPインストーラで会社のWebサーバまたはネットワーク共有を指定します。これは、帯域幅を節約し、信頼できるインストーラを一元化された場所に配置するために、企業で最も一般的に使用されます。

エンドポイントで証明書エラーなしでHTTPSリンクに到達でき、ルート証明書がマシンストアにインストールされていることを確認してください。

ASAで以前に作成したAMPプロファイルに戻り（ステップ1）、AMPイネーブラプロファイルを**編集します**。

1. AMPモードの場合は、[AMPイネーブラのインスト**ール]ラジオ・ボタン**をクリックします。
2. [**Windows Installer**]フィールドに、WebサーバのIPとFireAMPのファイルを追加します。
3. [Windows Options] はオプションです。

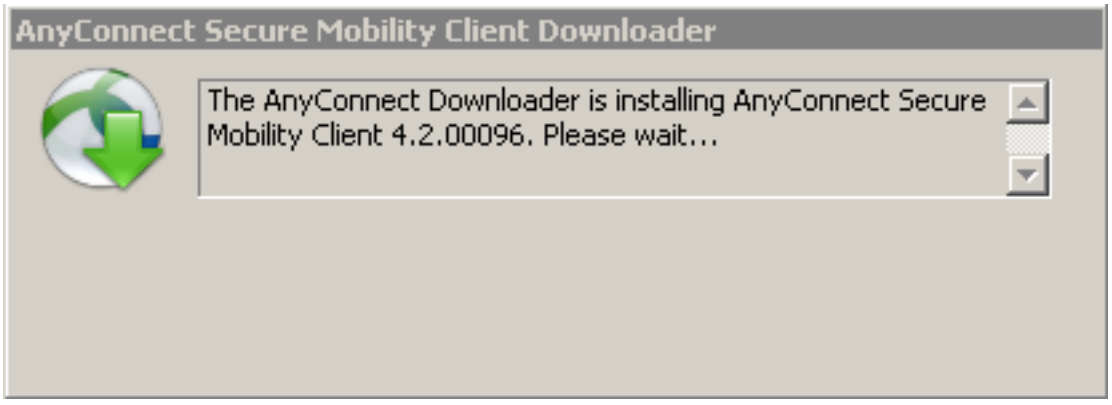
[OK] をクリックし、変更を適用します。



ステップ 5：AnyConnect への接続とモジュールのインストールの検証

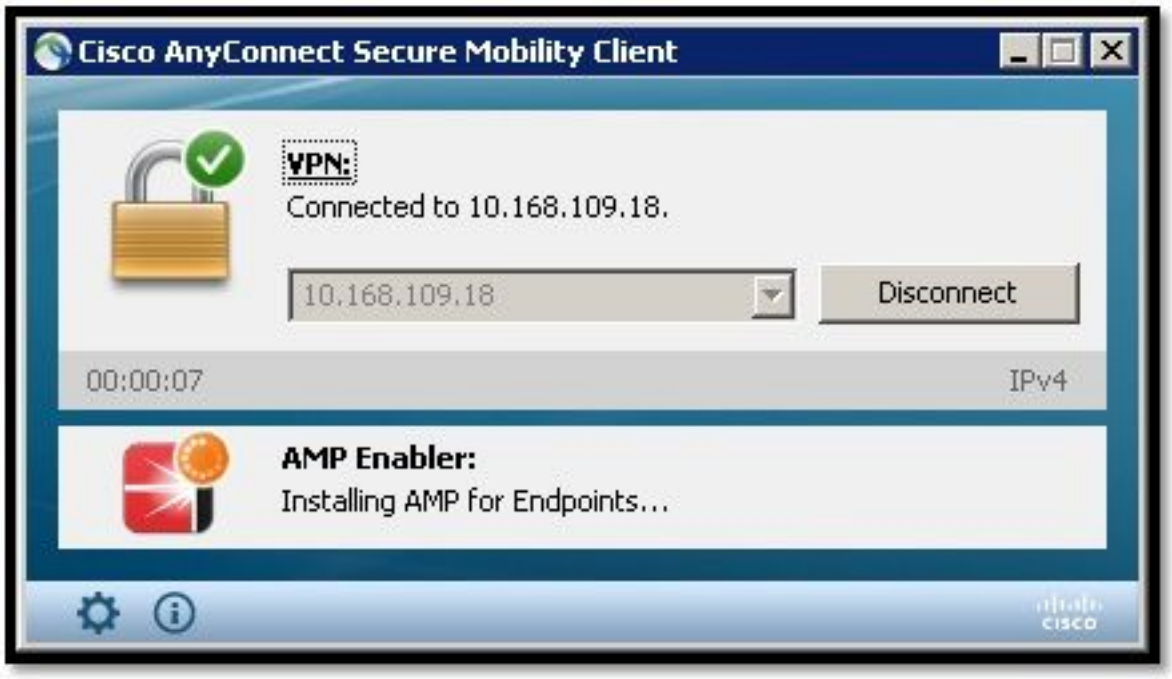
Anyconnect VPNユーザが接続すると、ASAはAnyConnect AMPイネーブラモジュールをVPN経由でプッシュします。すでにログインしているユーザの場合は、機能を有効にするために、ログオフしてから再度ログインすることをお勧めします。

```
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%
```



ステップ 6：VPN接続の開始AMPイネーブラとAMPコネクタのインストール

ボタン[connect]を押してVPNを開始すると、新しいダウンローダモジュールがダウンロードされます。これにより、AMPイネーブラが作成され、以前に指定したURLパスからAMPパッケージがダウンロードされます。




```
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]
```

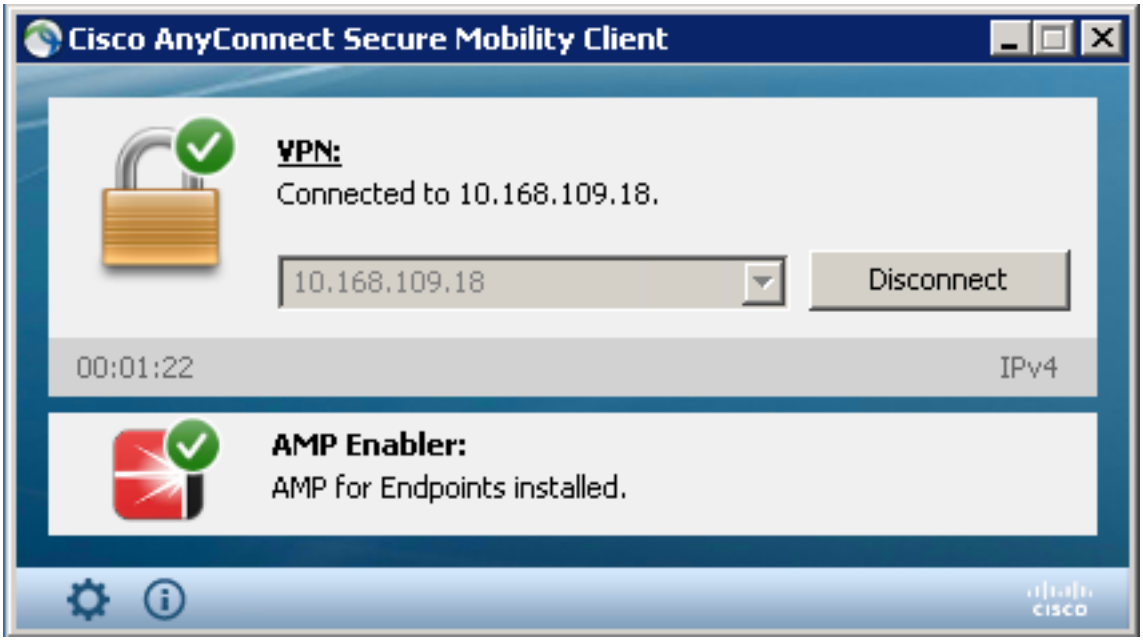
手順 7：AnyConnect の確認とすべてのコンポーネントがインストールされているかどうかの検証

VPNが接続され、Webサーバの設定がインストールされたら、AnyConnectをチェックして、すべてが正しくインストールされていることを確認します。

services.mscには、CiscoAMP_5.1.3という名前の新しいサービスがあります。Powershellコマンドには次のように表示されます。

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

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



AMPインストーラは、Windows OSに新しいドライバを追加します。driverqueryコマンドを使用してドライバをリストできます。

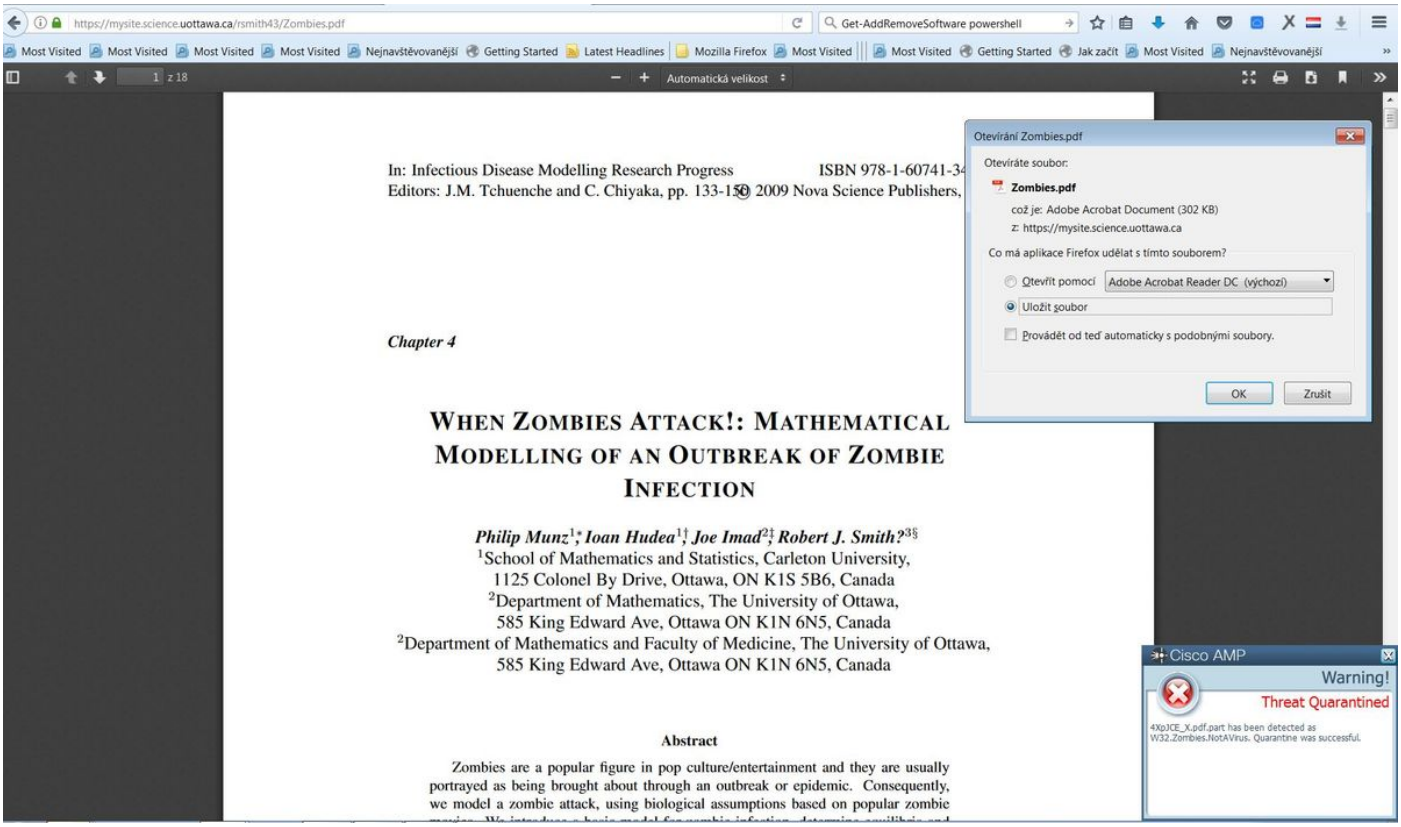
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

ステップ 8：ゾンビPDFファイルに含まれるEicar文字列を使用したテスト

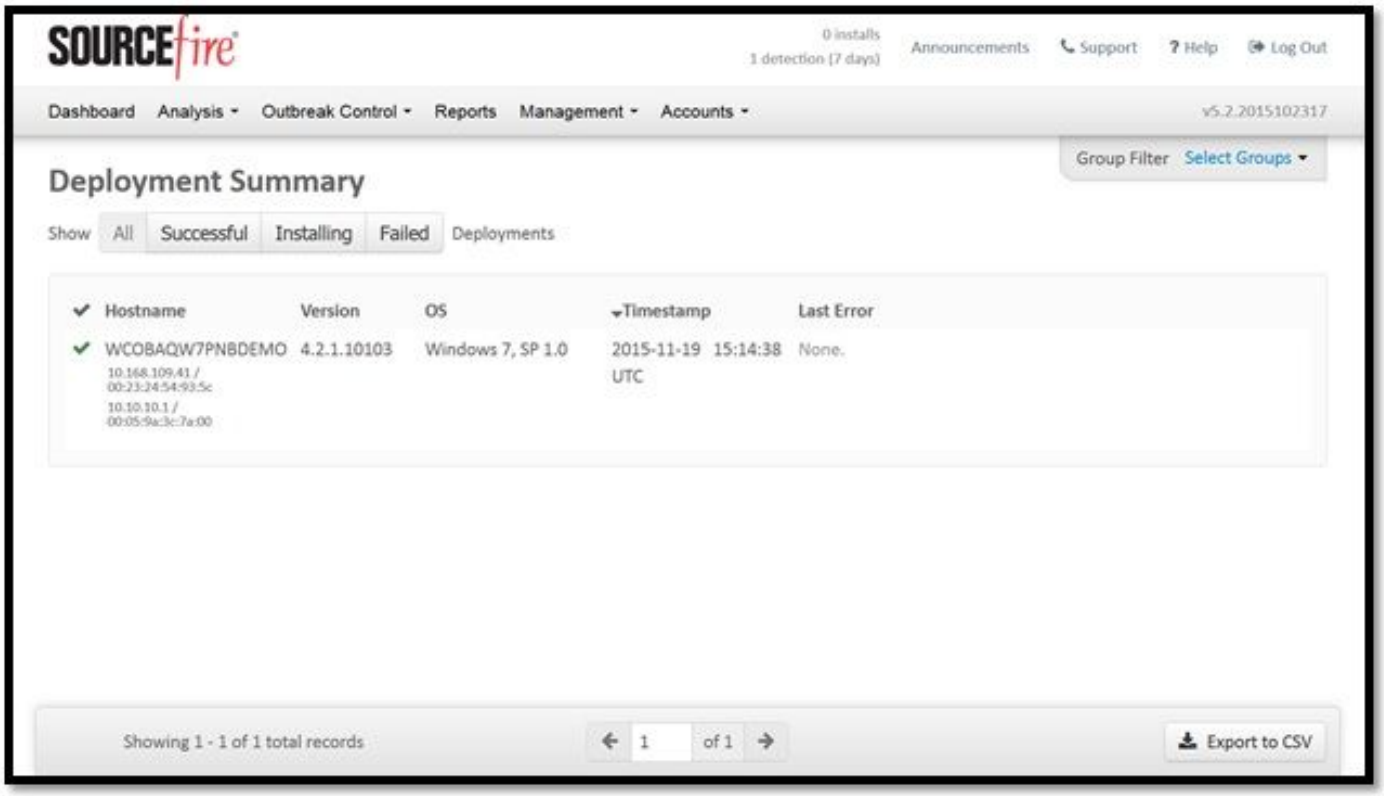
テストコンピュータのZombies PDFファイルに含まれるEicar文字列を使用してテストを行い、悪意のあるファイルが検疫されていることを確認します。



Zombies.pdfにはEicar文字列が含まれています

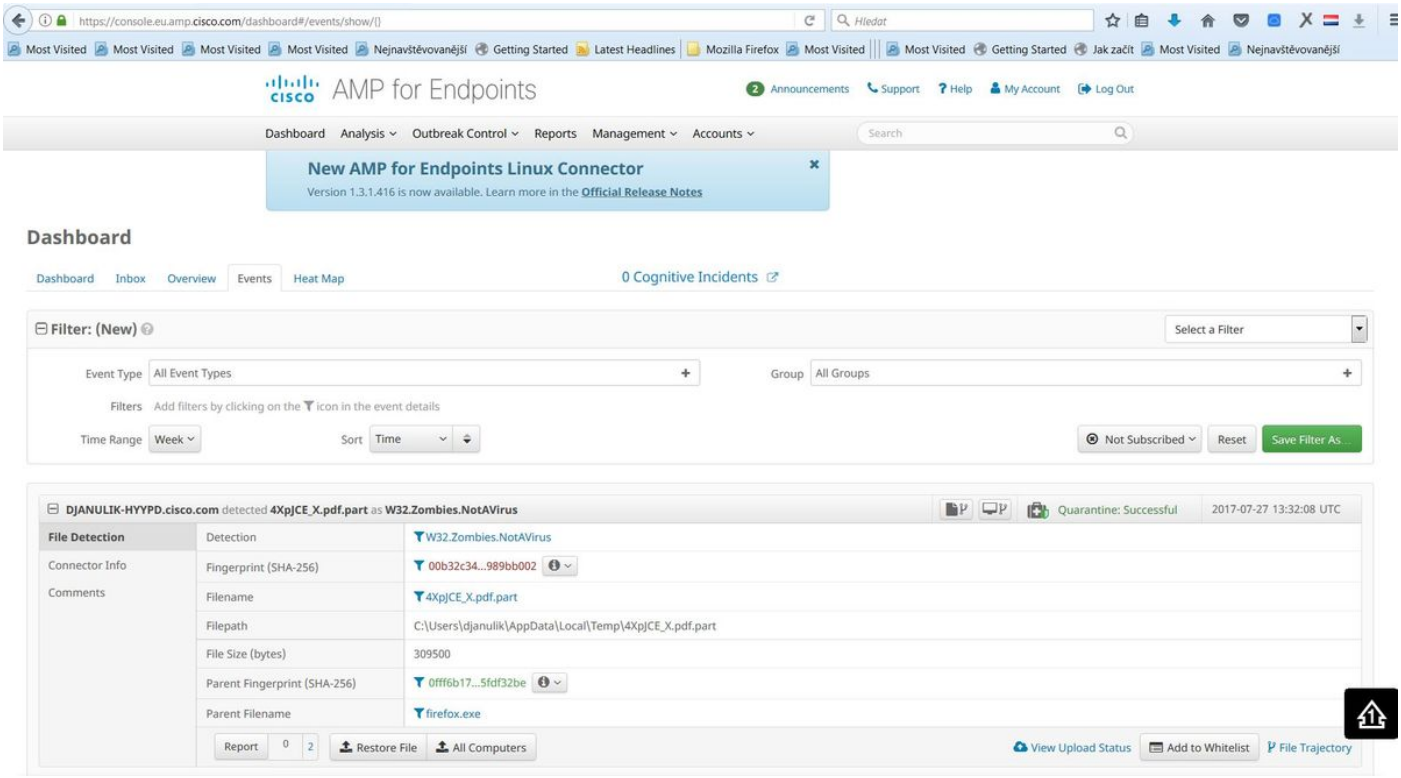
手順 9：導入の概要

このページには、FireAMPコネクタのインストールの成功と失敗、および現在進行中のインストールのリストが表示されます。[Management] > [Deployment Summary] に移動できます。



手順 10：スレッド検出の検証

Zombies.pdfは検疫イベントをトリガーし、AMPダッシュボードに送信します。



検疫イベント

追加情報

AMPアカウントを取得するには、ATS大学にサインアップできます。これにより、ラボのAMP機能の概要が示されます。

関連情報

- AMP イネーブラの設定
- テクニカル サポートとドキュメント – Cisco Systems