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

目次

概要

この資料はステップを AnyConnect の Advanced Malware Protection （ AMP ）コネクタをインストールすることを通過します。

メディアとして AnyConnect AMP イネーブラーが AMP for Endpoints を展開するのに使用されています。 自体それはファイル 開封を有罪と決定する機能をありません。 それは ASA からのエンドポイントに AMP for Endpoints ソフトウェアを押します。 AMP がインストールされていればクラウド キャパシティをファイル開封があるように確認するのに使用します。 AMP それ以上のサービスは ThreatGrid と呼ばれる動的解析に未知ファイル動作を記録するためにファイルを入れることができます。 これらのファイルは悪意のあるようにある特定の成果物が会う場合有罪と決定することができます。 これはゼロ日不正侵入に広く役立ちます。

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 または それ 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くものです。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）ソフトウェア バージョン 9.5.1 との 5525
- Microsoft Windows 7 専門 64 ビットの 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)

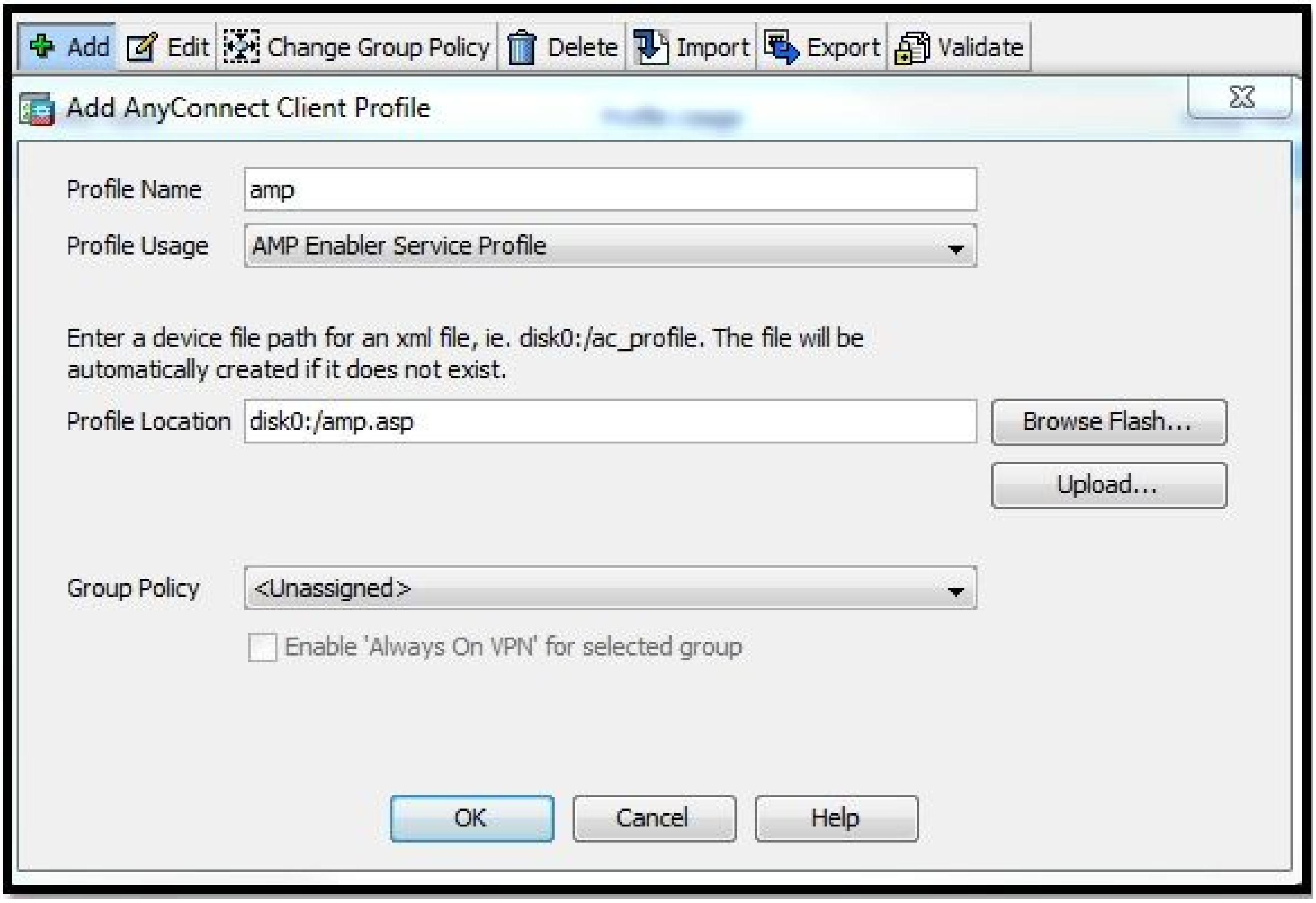
ASA を介した AMP イネーブラのための AnyConnect の導入

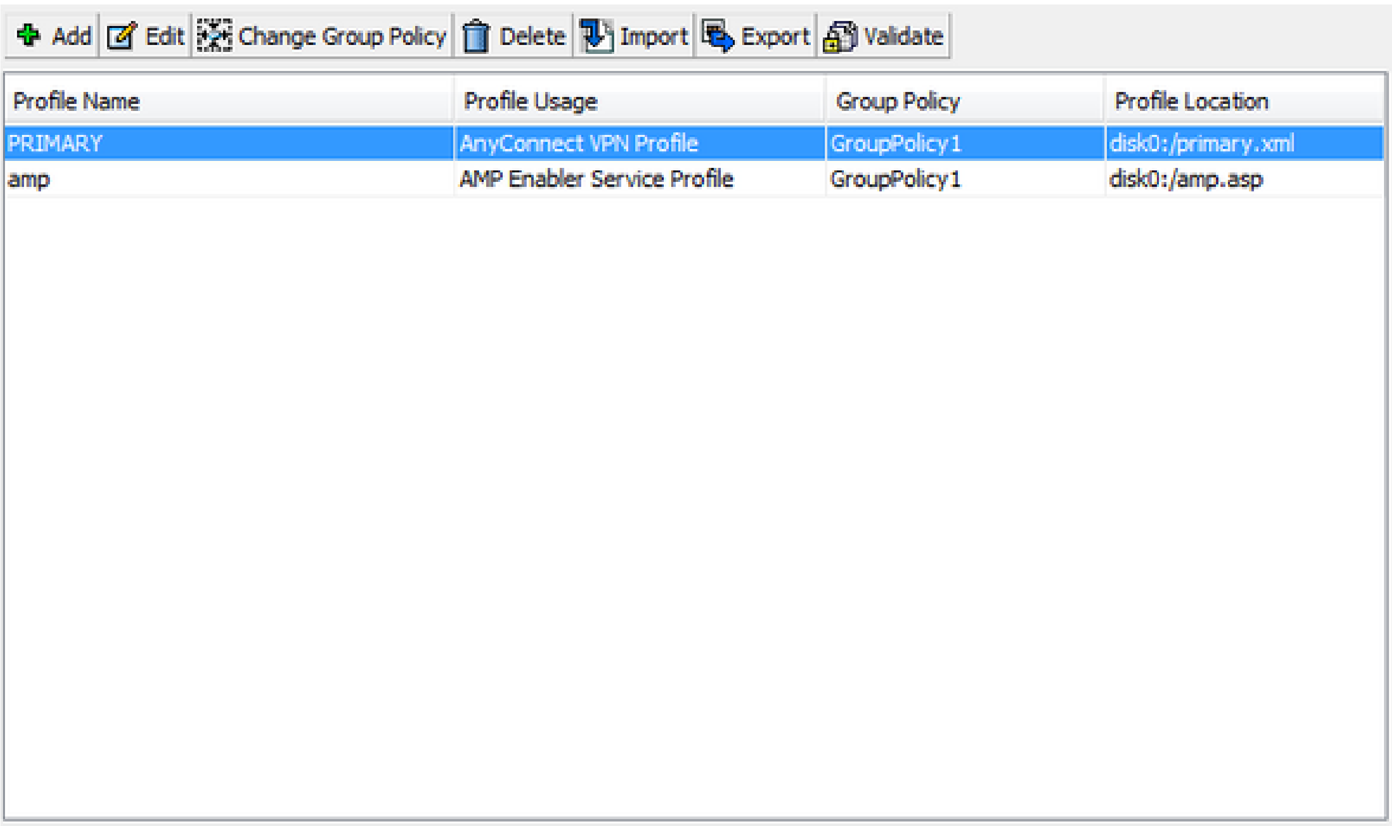
設定の手順は次の通りです:

- AnyConnect AMP イネーブラー クライアント プロファイルを設定して下さい。
- AnyConnect VPNグループ ポリシーを編集し、AMP イネーブラー サービス プロファイルをダウンロードして下さい。
- コネクタ URL ダウンロード リンクを得るために AMP ダッシュボードにログインして下さい。
- 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 イネーブラー クライアント プロファイルを設定して下さい

- **設定 > リモートアクセス VPN > ネットワーク（クライアント）アクセス > AnyConnect クライアント プロファイル**へのナビゲート。
- **AMP イネーブラー サービス プロファイルを**追加して下さい。

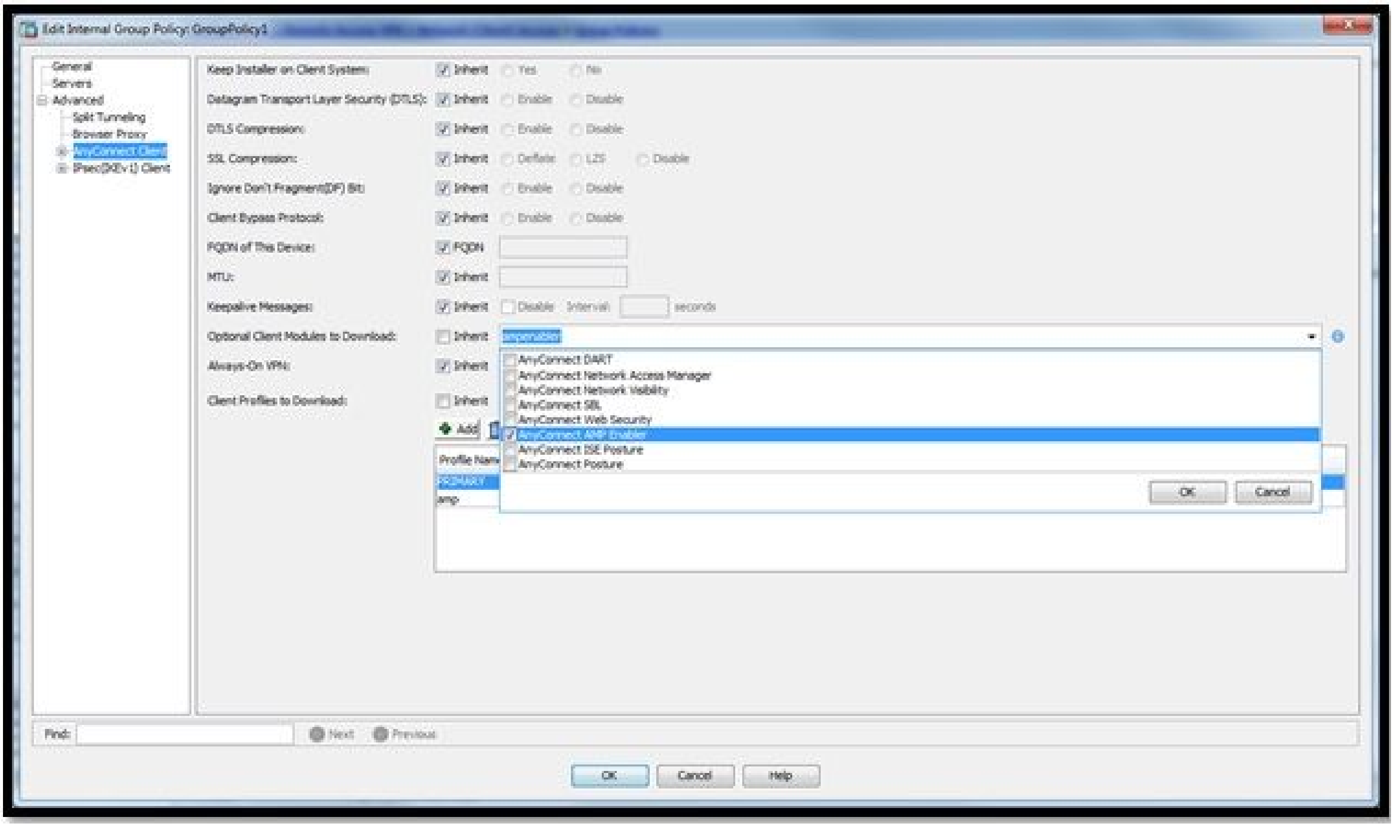




ステップ２： AnyConnect AMP イネーブラをダウンロードするためのグループ ポリシーの編集

- [Configuration] > [Remove Access VPN] > [Group Policies] > [Edit] の順に移動します。

- > AnyConnect クライアントは高度に > ダウンロードするべきオプションのクライアント モジュール行きます。
- AnyConnect AMP イネーブラーを選択して下さい。



ステップ3： FireAMP ポリシーのダウンロード

注: 続行する前に、システムがエンドポイント Windows コネクタの AMP のための必要条件を満たすかどうか確認して下さい。

AMP for Endpoints Windows Connector のシステム要件

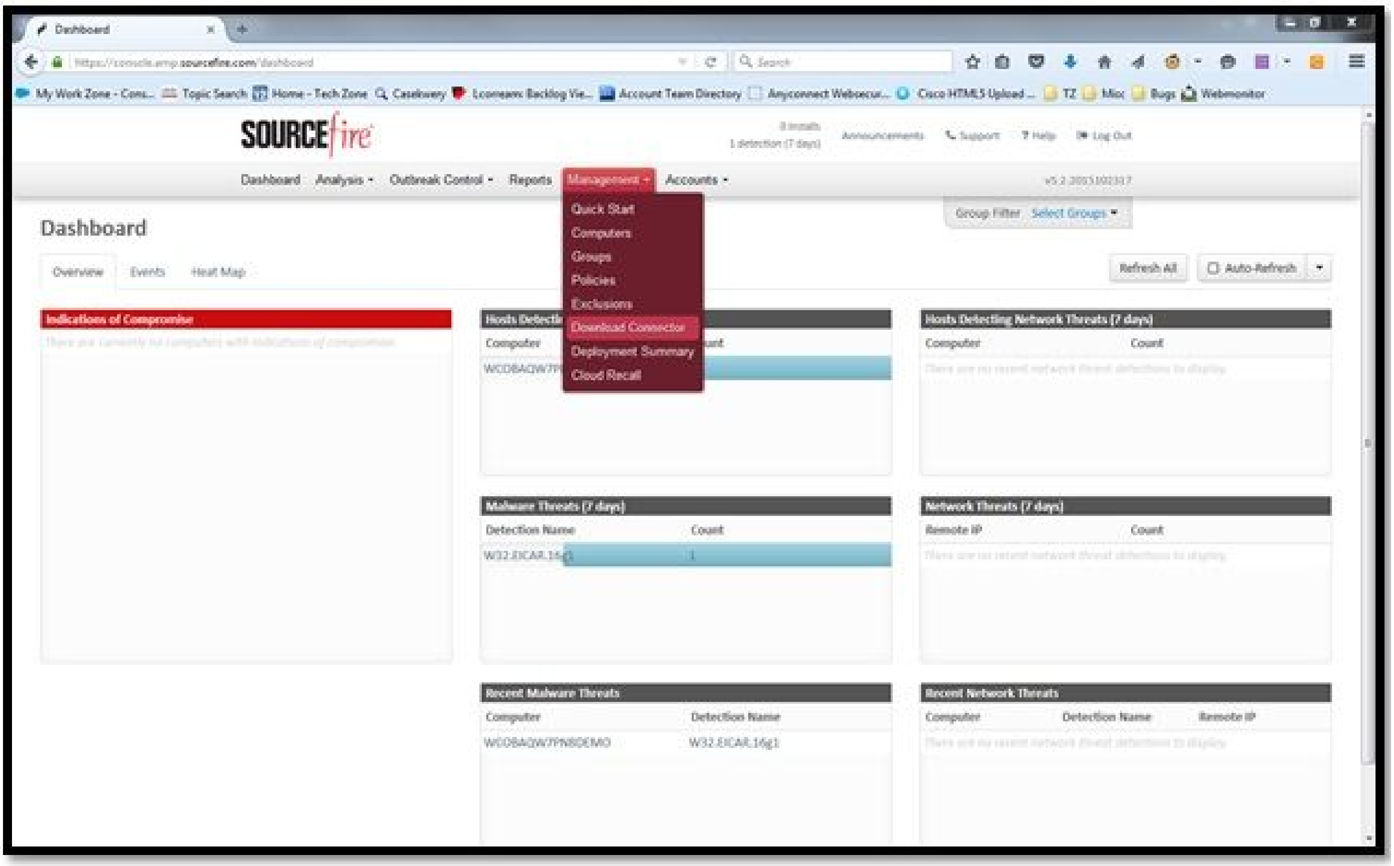
これらはウィンドウズオペレーティングシステムに基づいて FireAMP コネクタ用の最小システム要件です。 FireAMP Connector は、次のオペレーティング システムの 32 ビット バージョンと 64 ビット バージョンをサポートします。 AMP 最新のドキュメントは AMP 配備で見つけることができます

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 コネクタ 5.1.3 またはそれ以降を必要とします)	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

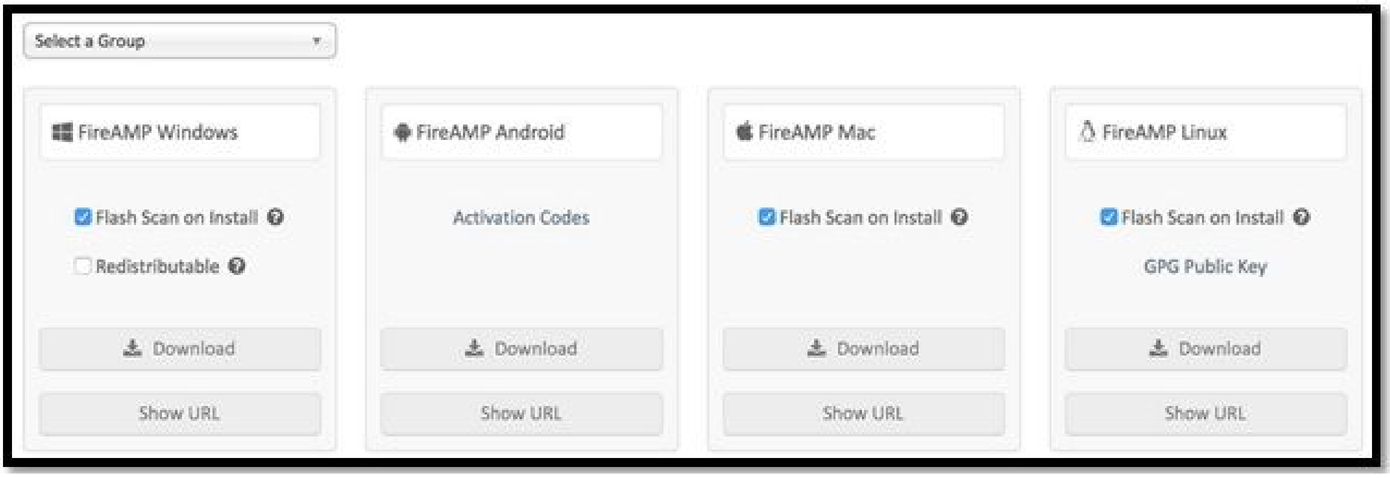
Microsoft Windows Server 2003	1 GHz 以上のプロセッサ	メモリ 512 MB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows Server 2008	2 GHz 以上のプロセッサ	メモリ 2 GB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows サーバ 2012（FireAMP コネクタ 5.1.3 またはそれ以降を必要とします）	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 の使用可能なハード ディスク領域 - TETRA

もっとも一般的なはエンタープライズ Webサーバに置かれる AMP インストーラを持つことです。

コネクタをダウンロードするには、[Management] > [Download Connector] に移動します。 それから『Type』 を選択 し、FireAMP（Windows、Android、Mac、Linux）を**ダウンロードして下さい。**



ダウンロード コネクタ ページは FireAMP コネクタの各型のためのインストール パッケージをダウンロードすることを可能にします。 このパッケージはネットワーク共有に置かれるか、または管理用ソフトによって配ることができます。



[Select a Group]

- **[Audit Only]：** SHA-256 に基づいてシステムを監視することは各ファイルに計算しました。 この監査 モードだけ malware を検疫しませんが、アラートとしてイベントを送信 します。
- **[Protect]：** 検疫悪意のあるファイルとのモードを保護して下さい。 ファイルのコピーを監視し、移動して下さい。
- **[Triage]：** これは既に危殆化された/感染させたコンピュータの使用のためです。
- **[Server]：** コネクタが Tetra エンジンおよび DFC ドライバなしでインストールする Windows サーバのためのインストール スイート。 このグループは非ドメイン コントローラ サーバの名前によって設計されています。
- **[Domain Controller]：** このグループのためのデフォルトポリシーは監査 モード 次 サーバグループに設定 されます。 コネクタが Windows ドメインコントローラで動作することをこのグループのアクティブディレクトリサーバをすべて、それ意味します関連付けて下さい。

AMP に完全なウイルス対策エンジンである TETRA と呼ばれる機能があります。 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]：** インストールの間のスキャン プロセス実行。 それは実行することは比較的に高速一度だけ動作することを推奨されてであり。
- **[Redistributable]：** 32ビットおよび 64 ビット インストーラが含まれている 1 つの一つのパッケージをダウンロードする必要があります。 実行される利用可能であるブートストラップよりもむしろ、このオプションを残しますインストーラー ファイルを unticked、ダウンロードします。

> **注:** あなた自身のグループを作成し、それに関連するポリシーを設定できます。 目的はポリシーが監査 モードにある 1 グループにすべてを例えばアクティブディレクトリサーバ置くことです。
> AMP コネクタ用にコンフィギュレーション ファイルとして使用するブートストラップおよび redistributable インストーラは両方また `policy.xml` 含まれています。

ステップ 4： Web セキュリティ クライアント プロファイルをダウンロードして下さい

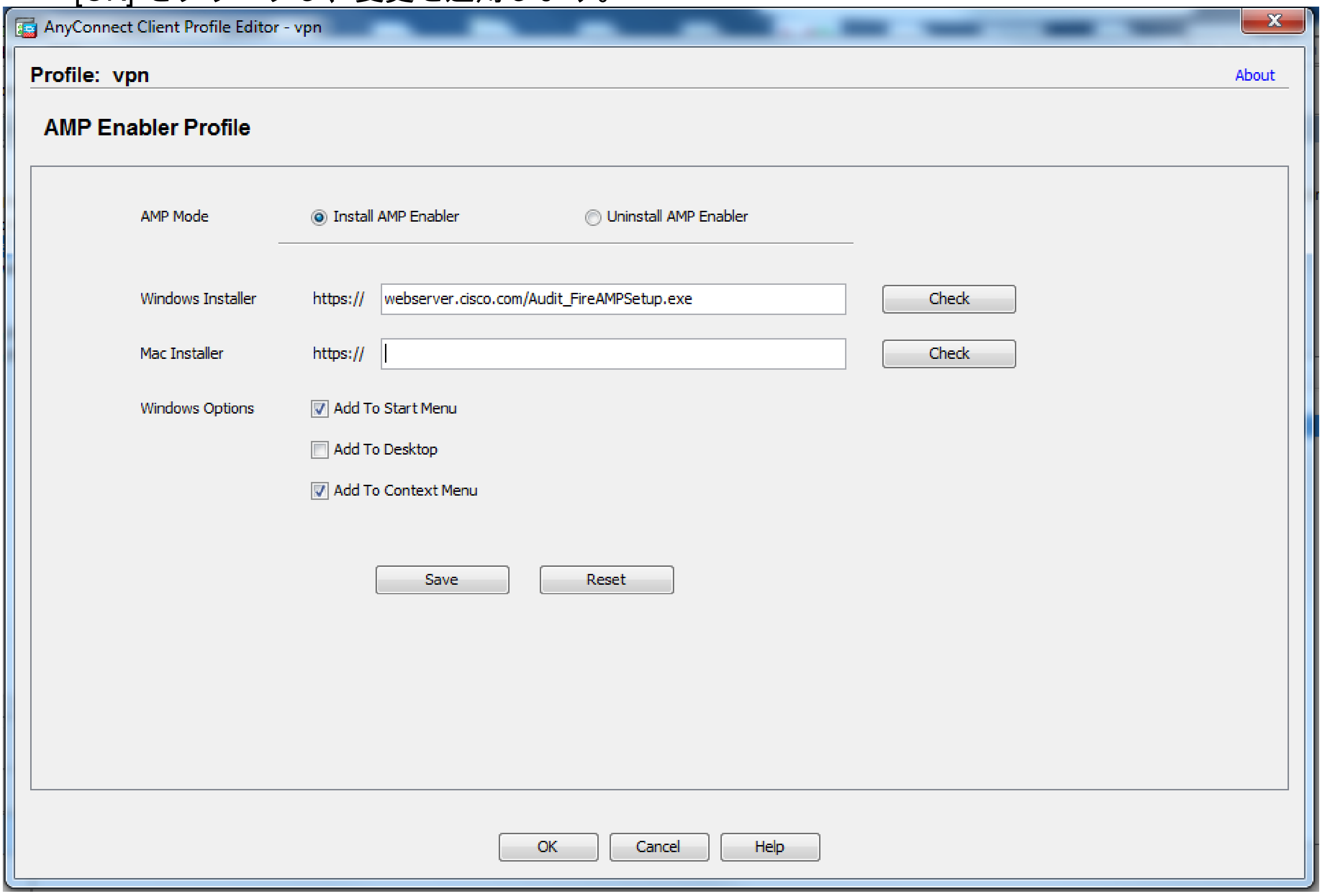
AMP インストーラが付いている会社 Webサーバかネットワーク共有を規定 して下さい。 これは会社を渡って最も広く使われています帯域幅を保存し、中央集中型ロケーションに信頼されたインストーラを置くために。

HTTPS リンクが Certificate エラーなしでエンドポイントで達することができること、そしてルート証明がマシン ストアにインストールされていることを確かめて下さい。

ASA で前に作成される AMP プロファイルに戻って下さい（1）ステップは **AMP イネーブラー プロファイルを**編集し、：

1. AMP モードに関しては、**インストール AMP イネーブラー** Radio ボタンをクリックして下さい。
2. **Windows インストーラ** フィールドでは、Webサーバのための IP および FireAMP のためのファイルを追加して下さい。
3. [Windows Options] はオプションです。

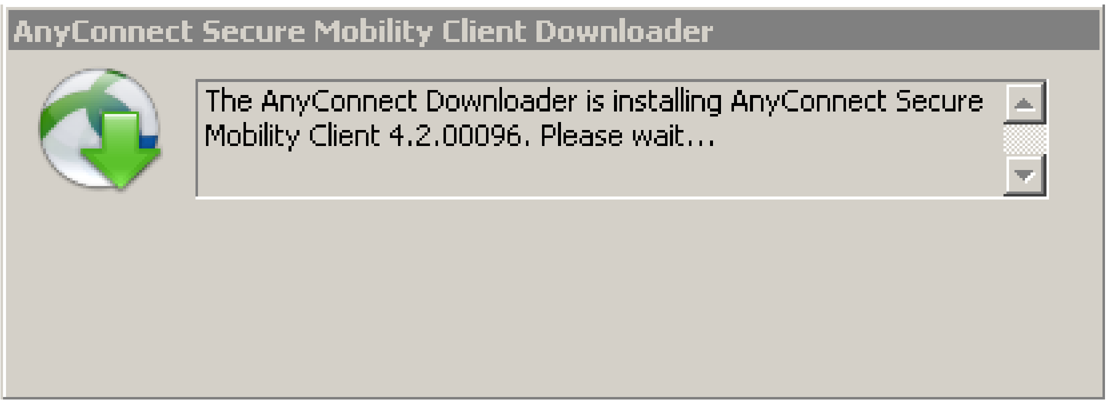
   [OK] をクリックし、変更を適用します。



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]

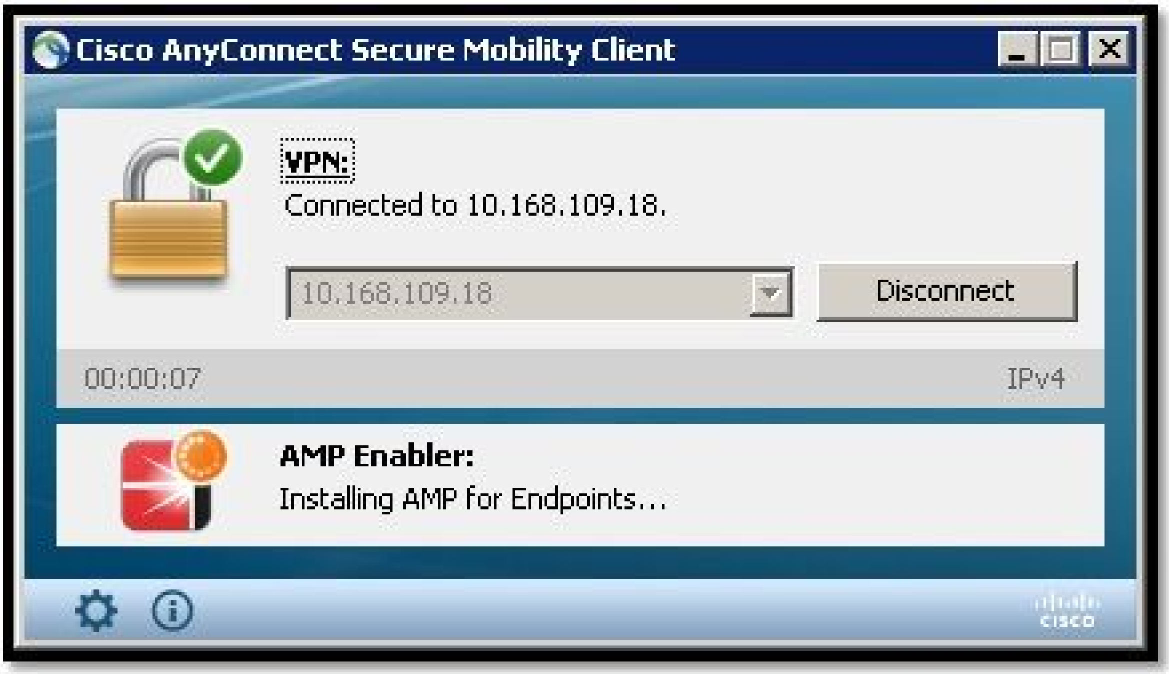
Anyconnect VPN ユーザが接続するとき、ASA は VPN に AnyConnect AMP イネーブラー モジュールを押通します。 既にログイン ユーザ向けに、ログオフし、次に機能性のためのログイン背部有効に なることを推奨します。

```
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 接続インストール AMP イネーブラーおよび AMP コネクタを開始して下さい

ボタンを VPN を開始するために押したらそれダウンロードします新しい Downloader モジュールを接続して下さい。 これに AMP イネーブラーがあり、ステップのカップルを前に規定 した URL パスから AMP パッケージをダウンロードします。




```
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]
```

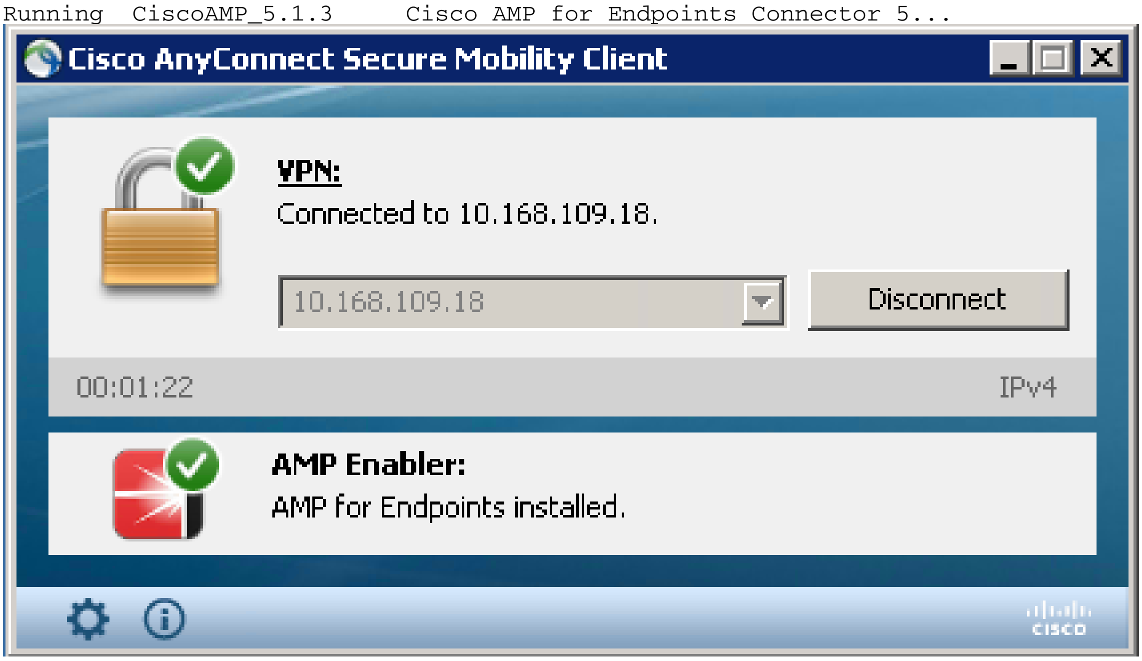
ステップ 7： AnyConnect の確認とすべてのコンポーネントがインストールされているかどうかの検証

VPN が接続され、Webサーバの設定がインストールされていたら、AnyConnect をチェックし、すべてがきちんとインストールされていることを確認して下さい。

services.msc で新しいサービスを CiscoAMP_5.1.3 と呼ばれて見つけることができます。Powershell コマンドで見ます:

```
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。 dirvers をリストするのに driverquery コマンドを使用するかもしれません。

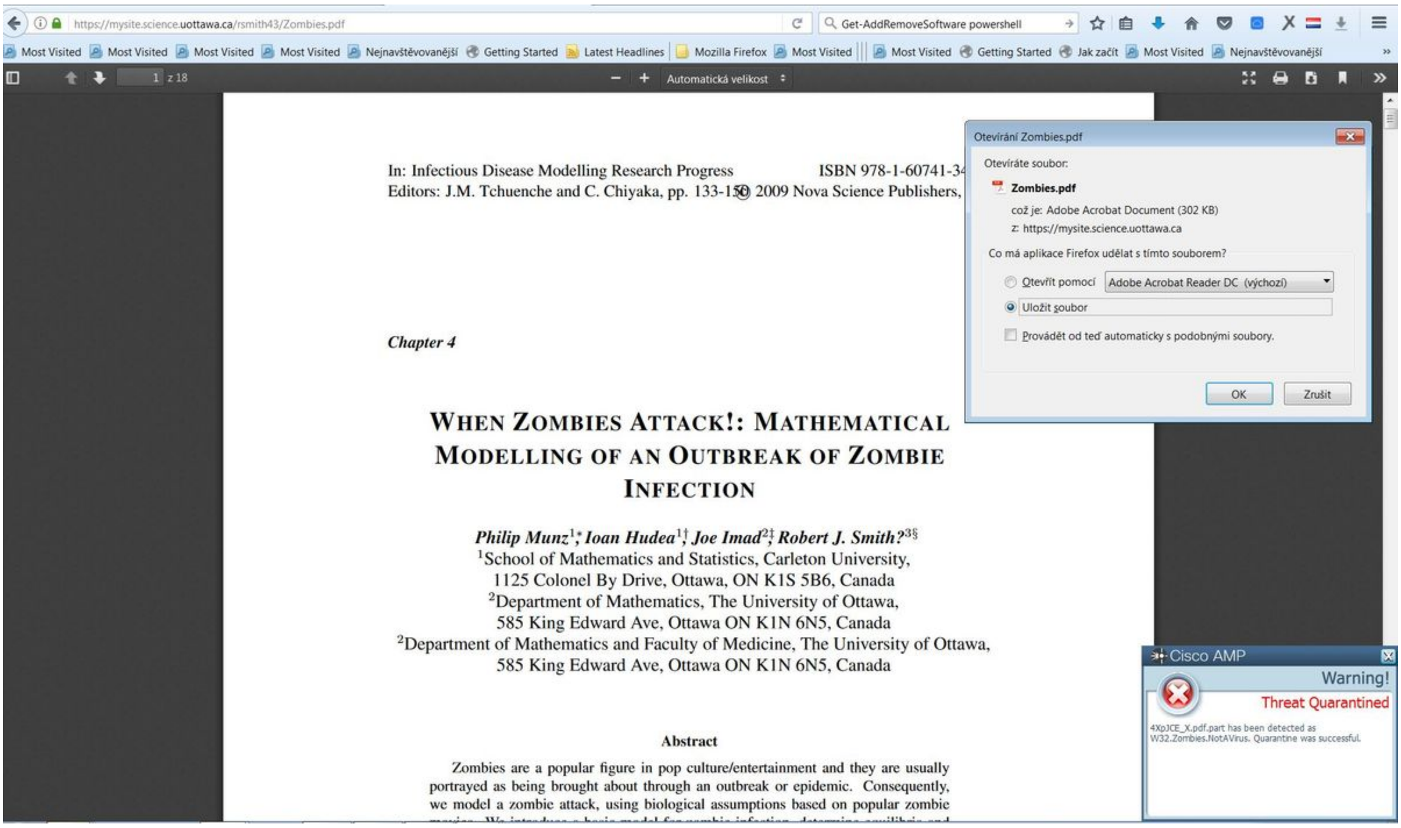
```
C:\Windows\System32>driverquery /v | findstr immunet

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ファイルに示される Eicar ストリングとテストして下さい

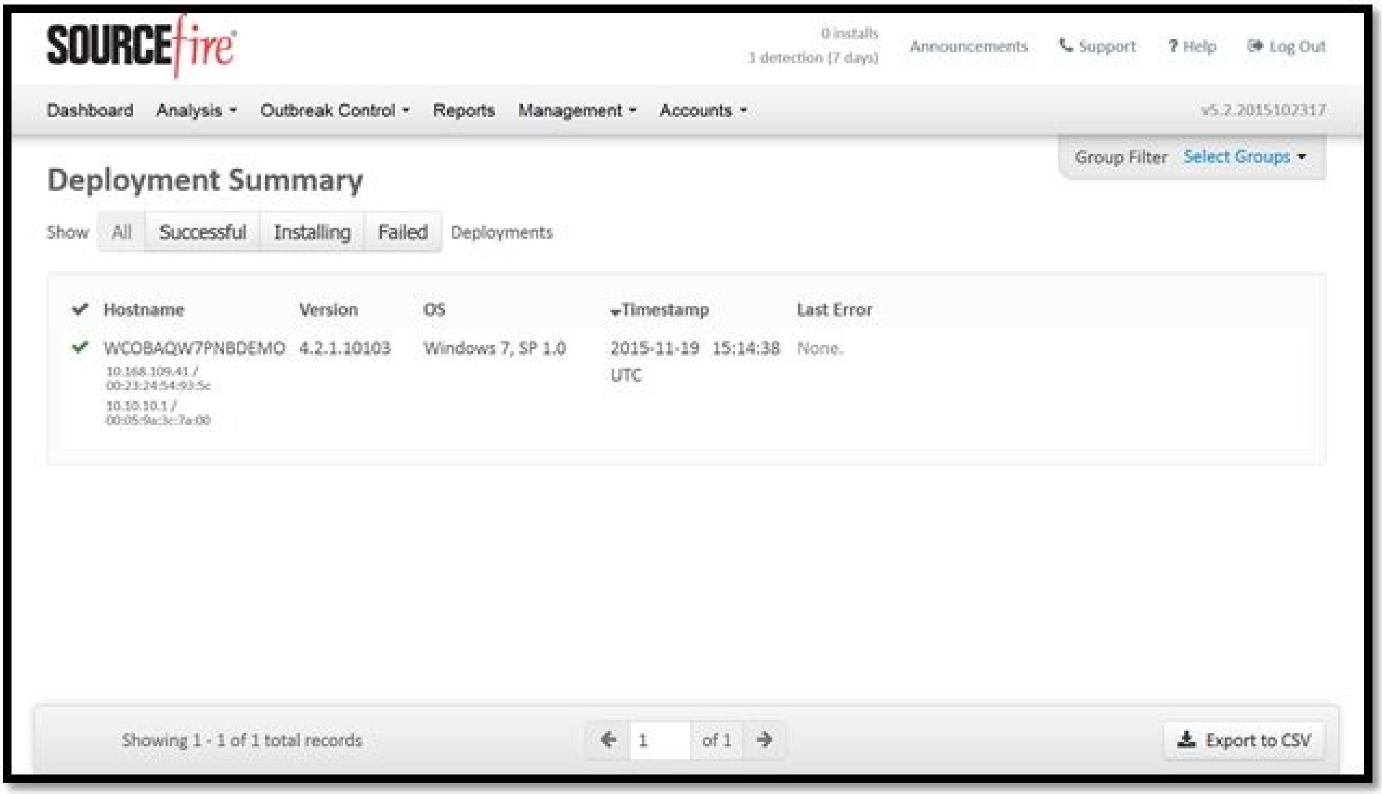
悪意のあるファイルが検疫されることを確認するためにテスト コンピュータのゾンビ PDFファイルに示される Eicar ストリングとテストして下さい。



Zombies.pdf は Eicar ストリングを示します

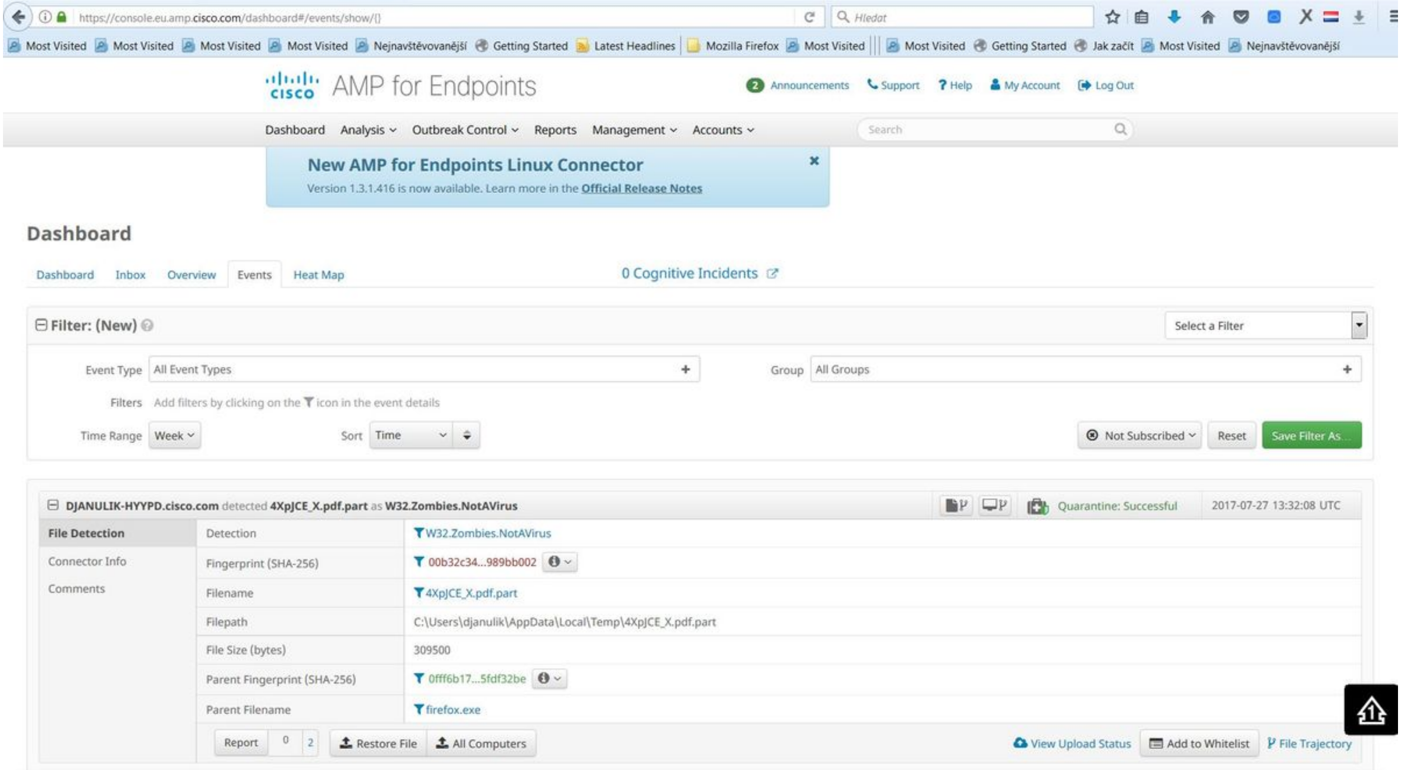
ステップ 9： [導入の概要]

このページは成功したのリストが壊れる FireAMP コネクタ インストールする、また進行中のことを現在それら示し。 [Management] > [Deployment Summary] に移動できます。



ステップ 10： [スレッド検出の検証]

Zombies.pdf は AMP ダッシュボードに検疫イベントを、送信引き起こしました。



検疫イベント

追加情報

AMP アカウントを得るために、ATS 大学に申し込むことができます。 これは LAB の AMP 機能性の外観が示されます。

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]()