Installation et configuration du module AMP via AnyConnect 4.x et AMP Enabler

Contenu

Introduction

Ce document décrit les étapes à suivre pour installer le connecteur AMP (Advanced Malware Protection) avec AnyConnect.

AnyConnect AMP Enabler est utilisé comme support pour déployer AMP for Endpoints. En soi, il n'a aucune capacité de déclarer coupable la disposition des dossiers. Il pousse le logiciel AMP for Endpoints à un point d'extrémité à partir d'ASA. Une fois qu'AMP est installé, il utilise la capacité du cloud pour vérifier la destruction des fichiers. Un autre service AMP peut soumettre des fichiers à une analyse dynamique appelée ThreatGrid, afin de noter le comportement des fichiers inconnus. Ces fichiers peuvent être reconnus malveillants si certains artefacts sont rencontrés. Ceci est très utile pour les attaques de type zero-day.

Conditions préalables

Conditions requises

- AnyConnect Secure Mobility Client version 4.x
- FireAMP / AMP pour terminaux
- Adaptive Security Device Manager (ASDM) version 7.3.2 ou ultérieure

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Adaptive Security Appliance (ASA) 5525 avec la version 9.5.1 du logiciel
- AnyConnect Secure Mobility Client 4.2.00096 sur Microsoft Windows 7 Professionnel 64 bits
- ASDM version 7.5.1(112)

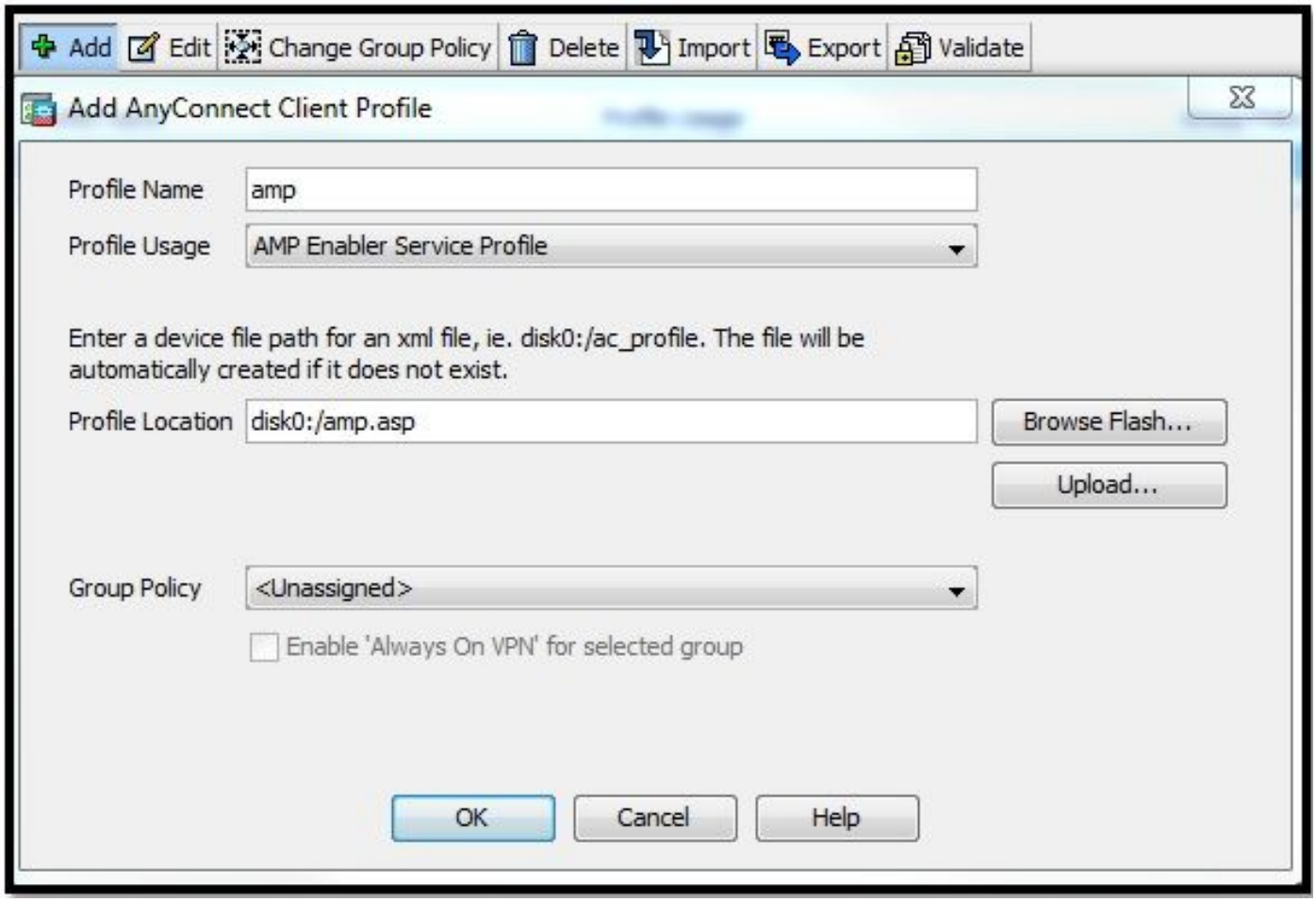
Déploiement d'AnyConnect pour AMP Enabler via ASA

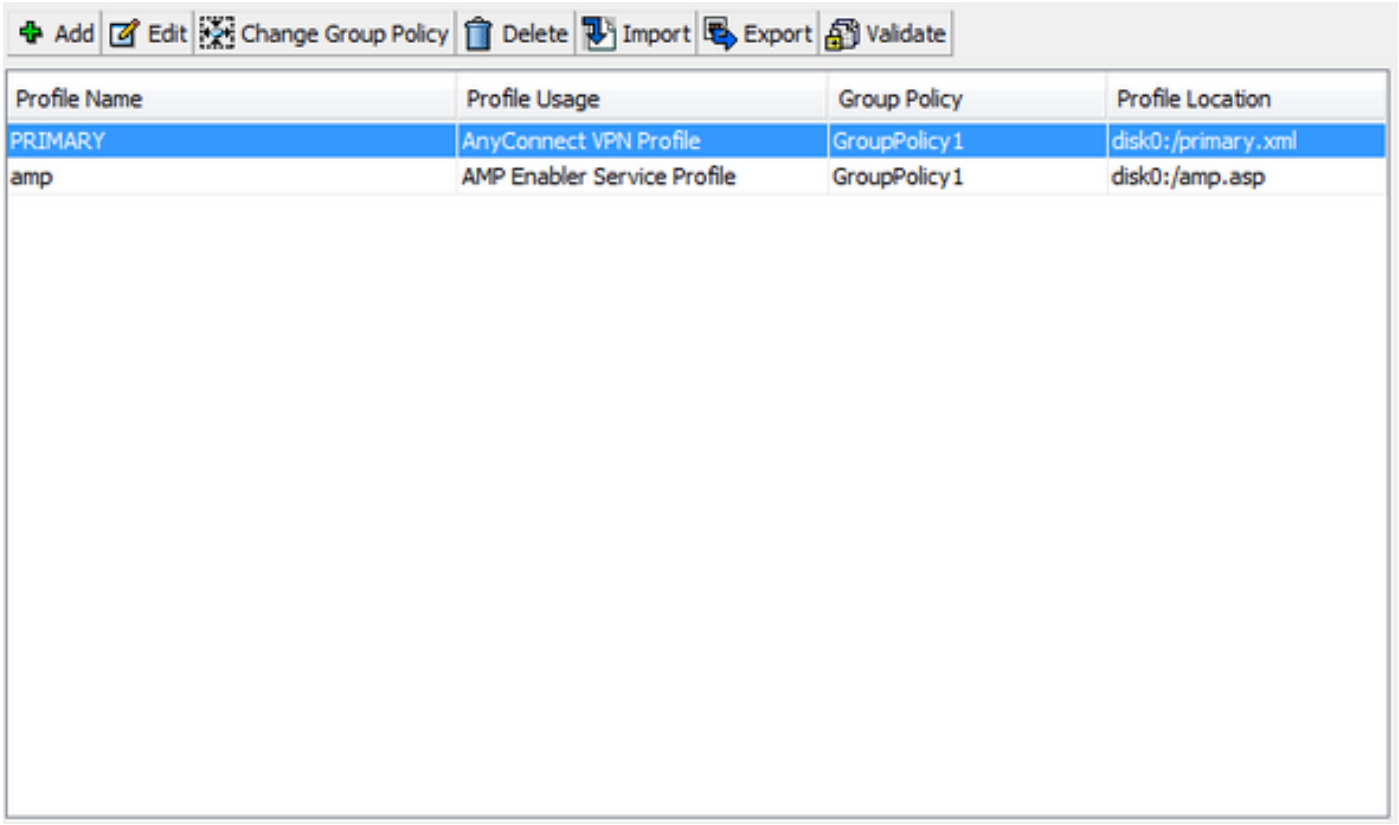
Les étapes de la configuration sont les suivantes :

- Configurez le profil client AnyConnect AMP Enabler.
- Modifiez la stratégie de groupe VPN AnyConnect et téléchargez le profil de service AMP Enabler.
- Connectez-vous au tableau de bord AMP afin d'obtenir le lien de téléchargement de l'URL du connecteur.
- Vérifiez l'installation sur l'ordinateur de l'utilisateur.

Étape 1 : Configurer le profil client AnyConnect AMP Enabler

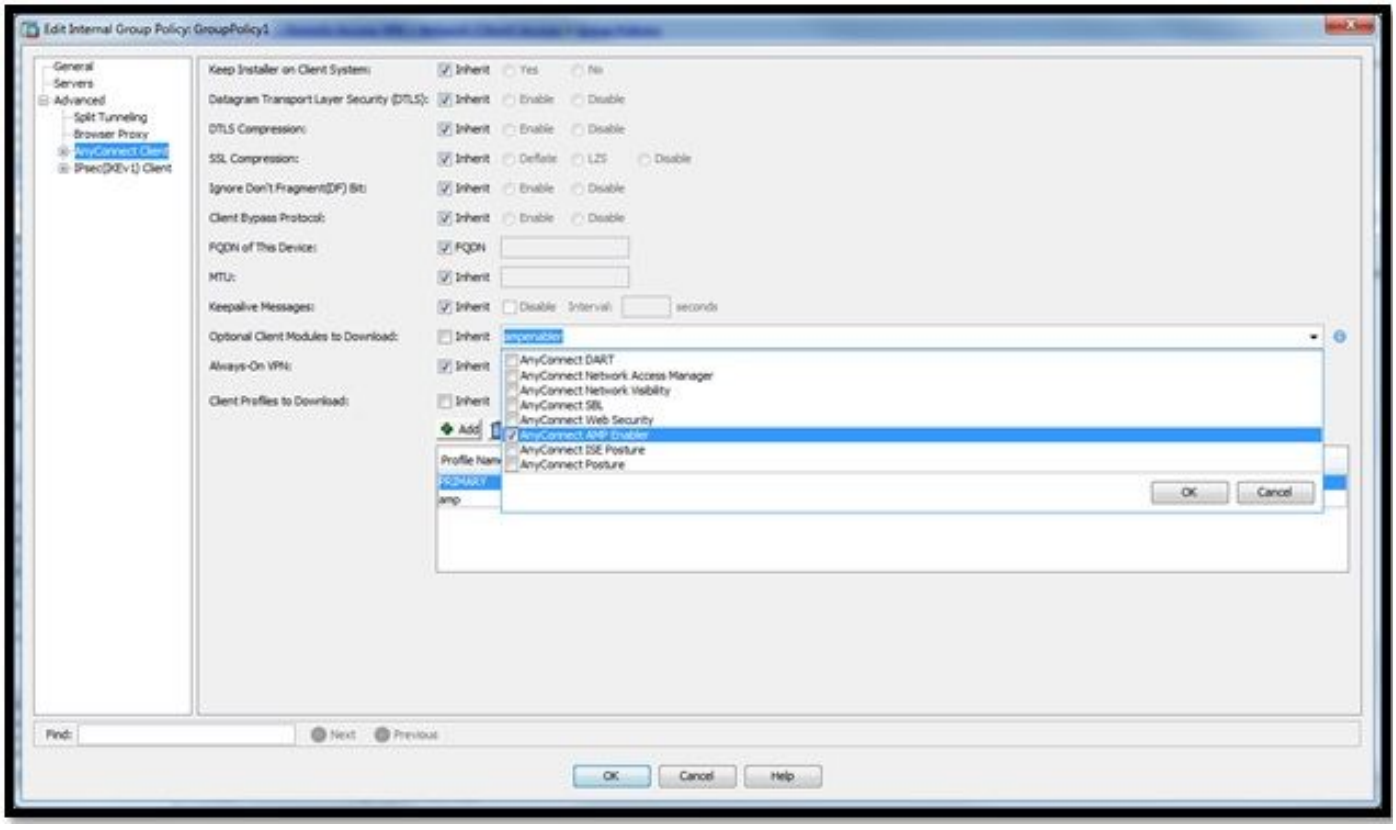
- Accédez à **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Ajoutez le **profil de service AMP Enabler**.





Étape 2 : Modifier la stratégie de groupe pour télécharger l'activateur AMP AnyConnect

- Accédez à **Configuration > Remove Access VPN > Group Policies > Edit**.
- Accédez à **Advanced > AnyConnect Client > Optional Client Modules to Download.**
- Choisissez **AnyConnect AMP Enabler.**



Étape 3 : Télécharger la stratégie FireAMP

Note: Avant de continuer, vérifiez si votre système répond aux exigences d'AMP of Endpoints Windows Connector.

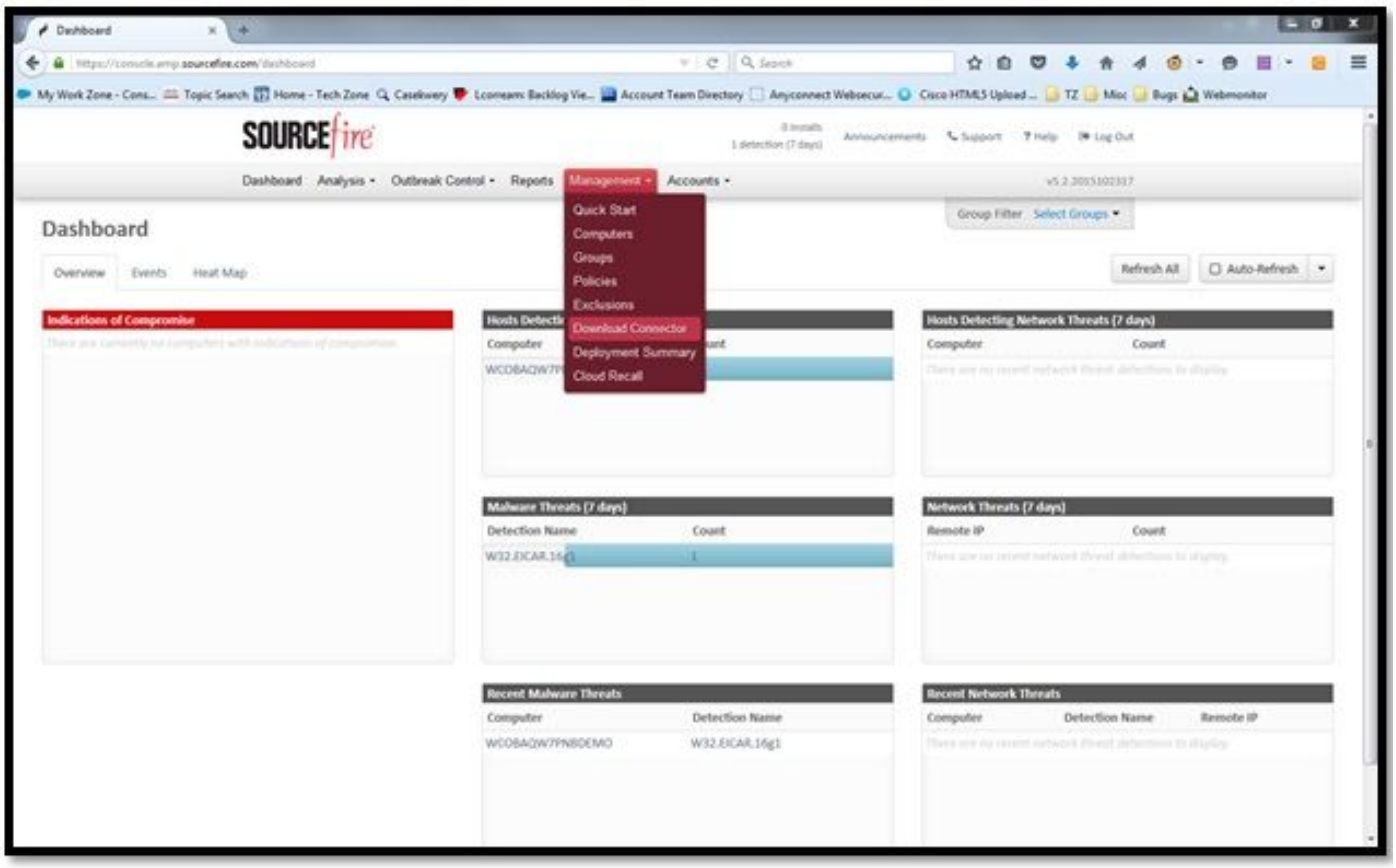
Configuration système requise pour AMP for Endpoints Connecteur Windows

Il s'agit de la configuration système minimale requise pour le connecteur FireAMP basé sur le système d'exploitation Windows. Le connecteur FireAMP prend en charge les versions 32 bits et 64 bits de ces systèmes d'exploitation. La documentation la plus récente d'AMP se trouve dans le déploiement d'AMP

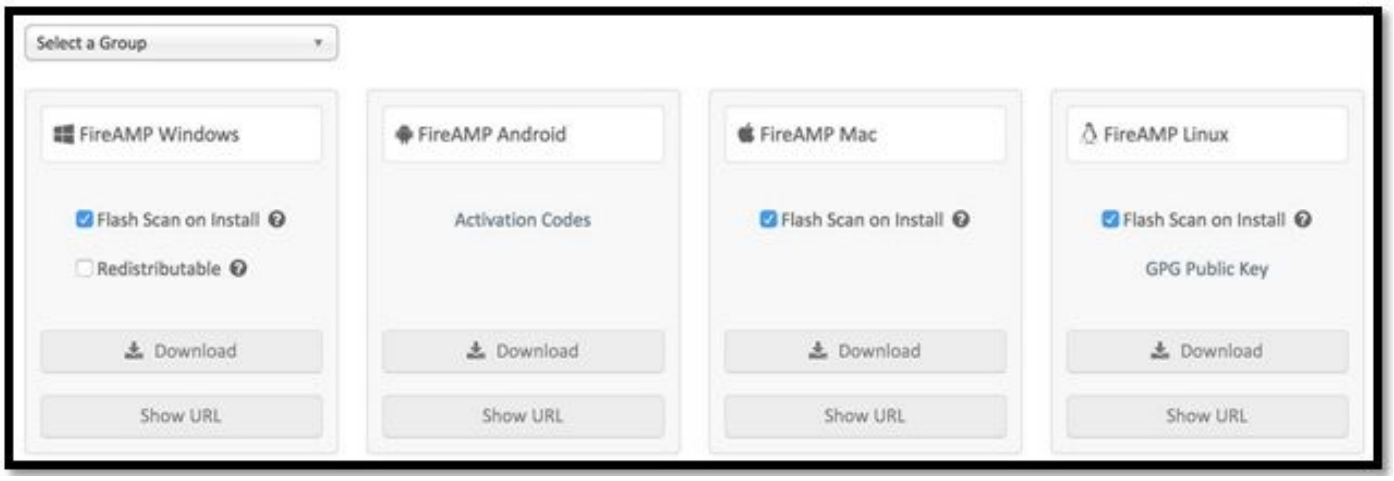
Système d'exploitation	Processeur	Mémoire	Espace disque, Mode cloud uniquement	Espace disque
Microsoft Windows 7	Processeur 1 GHz ou plus rapide	1 Go de RAM	150 Mo d'espace disque disponible - mode Cloud uniquement	Espace disque disponible de 1 Go - TETRA
Microsoft Windows 8 et 8.1 (nécessite FireAMP Connector 5.1.3 ou version ultérieure)	Processeur 1 GHz ou plus rapide	512 Mo de RAM	150 Mo d'espace disque disponible - mode Cloud uniquement	Espace disque disponible de 1 Go - TETRA
Microsoft Windows Server 2003	Processeur 1 GHz ou plus rapide	512 Mo de RAM	150 Mo d'espace disque disponible - mode Cloud uniquement	Espace disque disponible de 1 Go - TETRA
Microsoft Windows Server 2008	Processeur 2 GHz ou plus rapide	2 Go de RAM	150 Mo d'espace disque disponible - mode cloud uniquement	Espace disque disponible de 1 Go - TETRA
Microsoft Windows Server 2012 (nécessite FireAMP Connector 5.1.3 ou version ultérieure)	Processeur 2 GHz ou plus rapide	2 Go de RAM	150 Mo d'espace disque disponible - mode cloud uniquement	1 Go d'espace disque disponible - TETRA

Le plus courant est de placer le programme d'installation AMP sur le serveur Web d'entreprise.

Pour télécharger le connecteur, accédez à **Management > Download Connector**. Puis choisissez type, et **Télécharger** FireAMP (Windows, Android, Mac, Linux).



La page Download Connector vous permet de télécharger les packages d'installation pour chaque type de connecteur FireAMP. Ce package peut être placé sur un partage réseau ou distribué via un logiciel de gestion.



Sélectionner un groupe

- **Audit uniquement :** Surveillance du système basée sur SHA-256 calculée sur chaque fichier. Ce mode Audit uniquement ne met pas en quarantaine le programme malveillant, mais envoie un événement en tant qu'alerte.
- **Protéger :** Protection du mode avec mise en quarantaine des fichiers malveillants. Surveillez la copie et le déplacement du fichier.
- **Triage :** Ceci est à utiliser sur un ordinateur déjà compromis/infecté.
- **Serveur :** Suite d'installation pour le serveur Windows, où le connecteur s'installe sans moteur Tetra et pilote DFC. Ce groupe est conçu par son nom pour les serveurs de contrôleurs non-domaine.

- **Contrôleur de domaine :** La stratégie par défaut de ce groupe est définie en mode audit comme dans le groupe Serveur. Associez tous vos serveurs Active Directory dans ce groupe, ce qui signifie que le connecteur sera exécuté sur un contrôleur de domaine Windows.

L'AMP a la fonctionnalité appelée TETRA, qui est un moteur antivirus complet. Cette option est facultative par stratégie.

Fonctionnalités

- **Analyse Flash lors de l'installation :** Le processus d'analyse s'exécute pendant l'installation. Il est relativement rapide à exécuter et recommandé de ne l'exécuter qu'une seule fois.
- **Redistribuable :** Vous devez télécharger un seul package, qui contient des installateurs 32 bits et 64 bits. Plutôt qu'un bootstrapper, qui est disponible en ne cochant pas cette option et télécharge les fichiers de l'installateur, une fois exécuté.

> **Note**: Vous pouvez créer votre propre groupe et lui configurer la stratégie associée. L'objectif est de placer tous les serveurs Active Directory, par exemple, dans un groupe, où la stratégie est en mode audit.
> Le programme d'amorçage et le programme d'installation redistribuable contiennent également un fichier policy.xml utilisé comme fichier de configuration pour le connecteur AMP.

Étape 4 : Télécharger le profil du client de sécurité Web

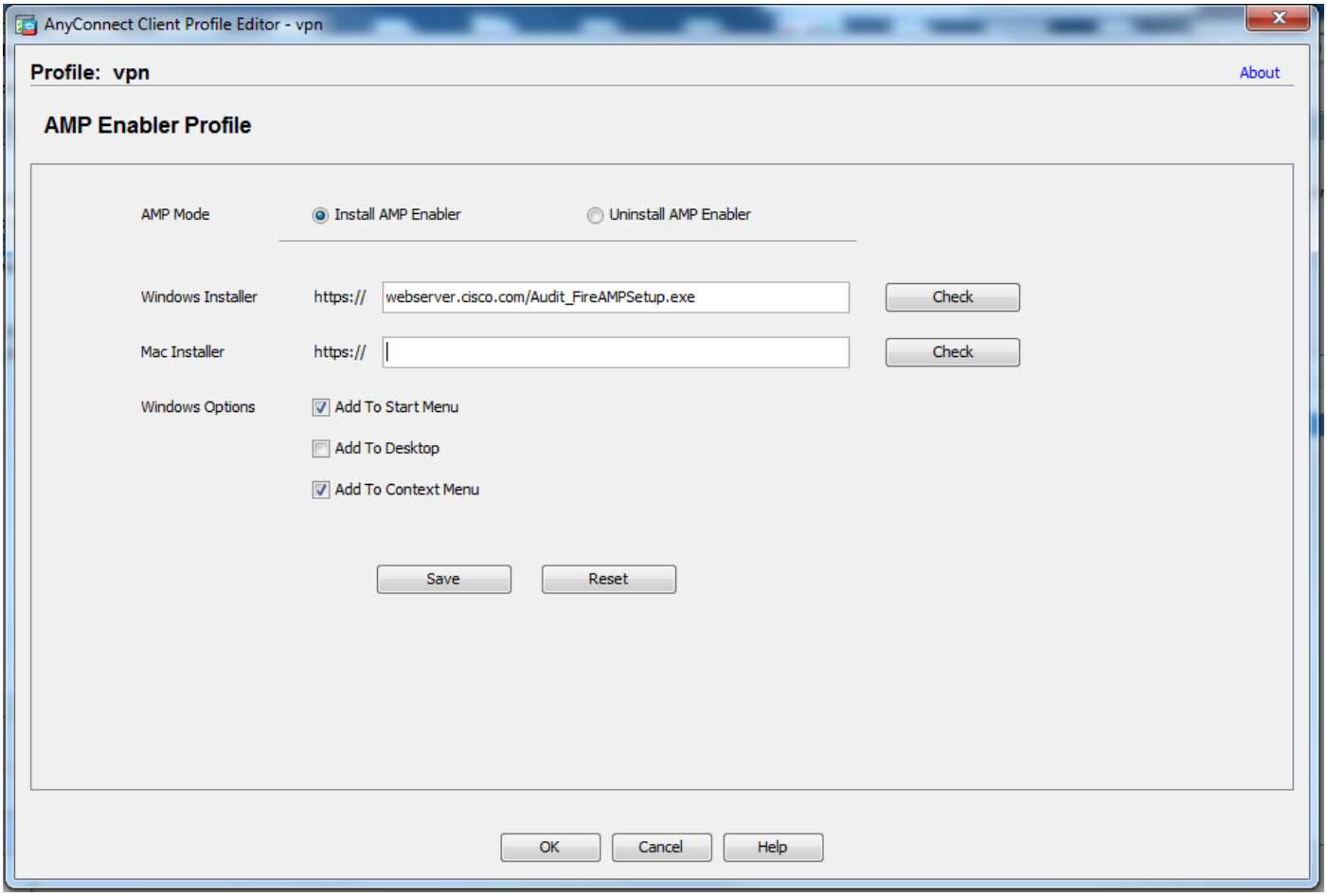
Spécifiez un serveur Web d'entreprise ou un partage réseau avec le programme d'installation AMP. Il est généralement utilisé dans toutes les entreprises pour économiser de la bande passante et placer les installateurs de confiance dans un emplacement centralisé.

Assurez-vous que la liaison HTTPS peut être atteinte sur les points de terminaison sans aucune erreur de certificat et que le certificat racine est installé dans le magasin d'ordinateurs.

Revenez au profil AMP créé précédemment sur l'ASA (étape 1) et modifiez le **profil AMP Enabler** :

1. Pour le mode AMP, cliquez sur la case d'option **Installer AMP Enabler**.
2. Dans le champ **Windows Installer**, ajoutez l'adresse IP du serveur Web et le fichier de FireAMP.
3. Les options de Windows sont facultatives.

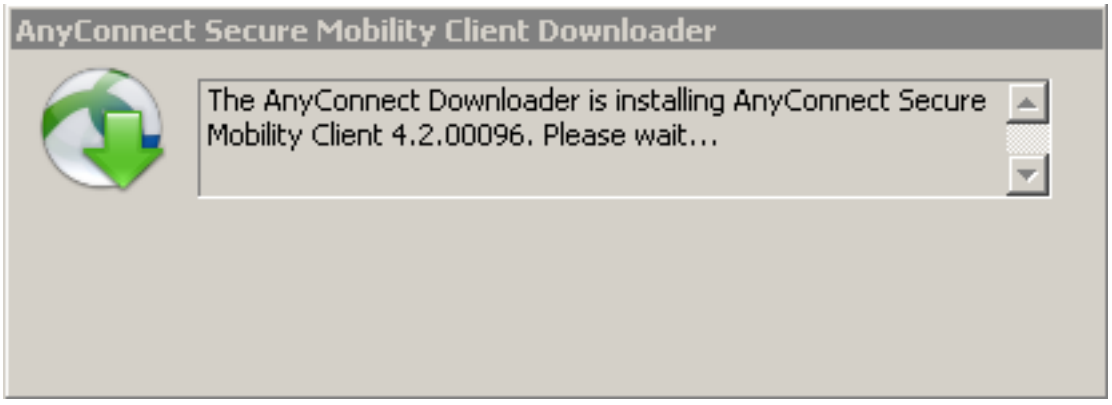
   Cliquez sur **OK** et appliquez les modifications.



Étape 5 : Connexion avec AnyConnect et vérification de l'installation du module

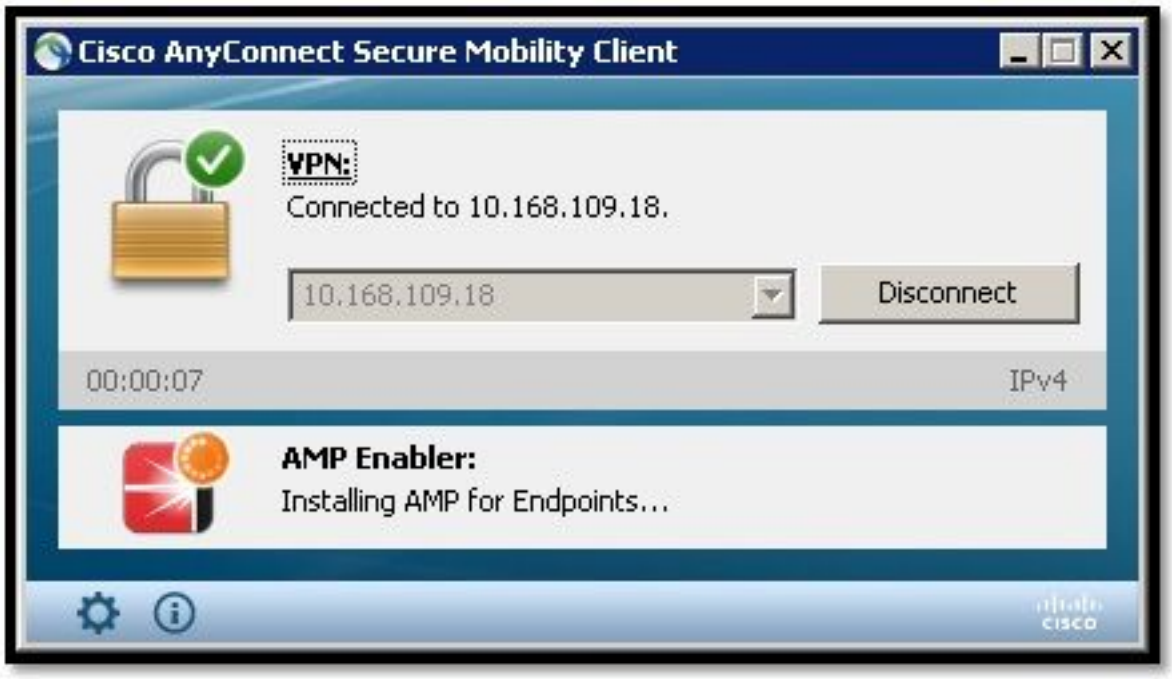
Lorsqu'un utilisateur VPN Anyconnect se connecte, ASA pousse le module AnyConnect AMP Enabler à travers le VPN. Pour les utilisateurs déjà connectés, il est recommandé de se déconnecter, puis de se reconnecter pour que la fonctionnalité soit activée.

```
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%
```



Étape 6 : Démarrer VPN Connection installer AMP Enabler et le connecteur AMP

Une fois que vous avez cliqué sur le bouton connect pour démarrer le VPN, il télécharge le nouveau module de téléchargement. Cela aura un activateur AMP et téléchargera le package AMP à partir du chemin d'URL que vous avez spécifié quelques étapes auparavant.




```
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]
```

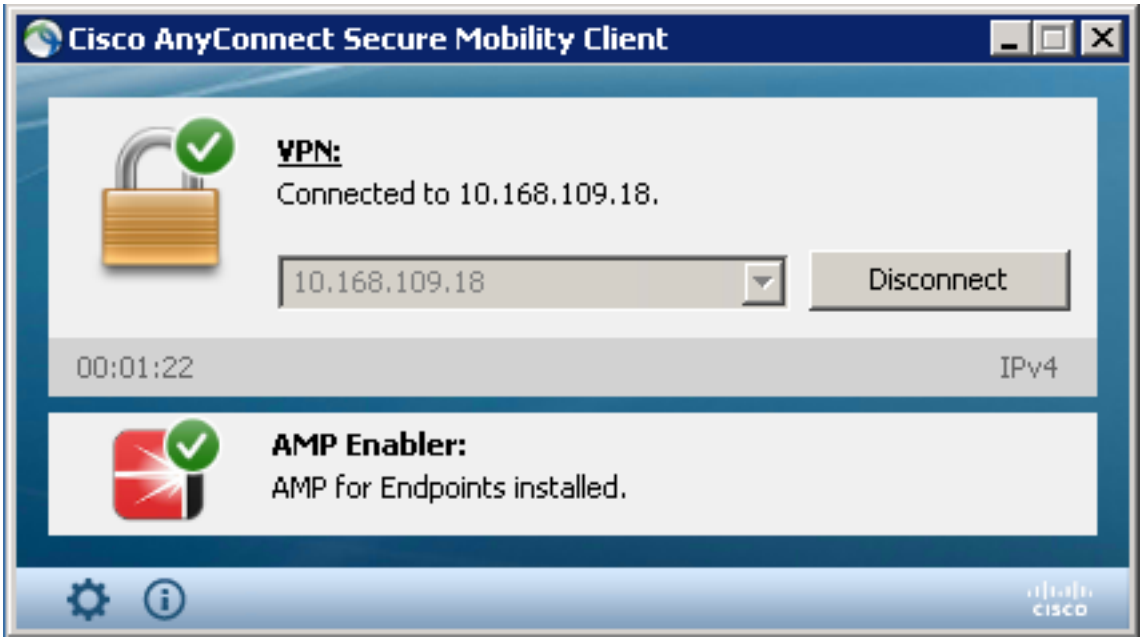
Étape 7 : Vérifier AnyConnect et vérifier si tout est installé

Une fois le VPN connecté et la configuration du serveur Web installée, vérifiez AnyConnect et vérifiez que tout est correctement installé.

Dans le fichier services.msc, vous pouvez trouver un nouveau service appelé CiscoAMP_5.1.3. Dans la commande Powershell, nous voyons :

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

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



AMP Installer ajoute de nouveaux pilotes au système d'exploitation Windows. Vous pouvez utiliser la commande driverquery pour répertorier les pilotes.

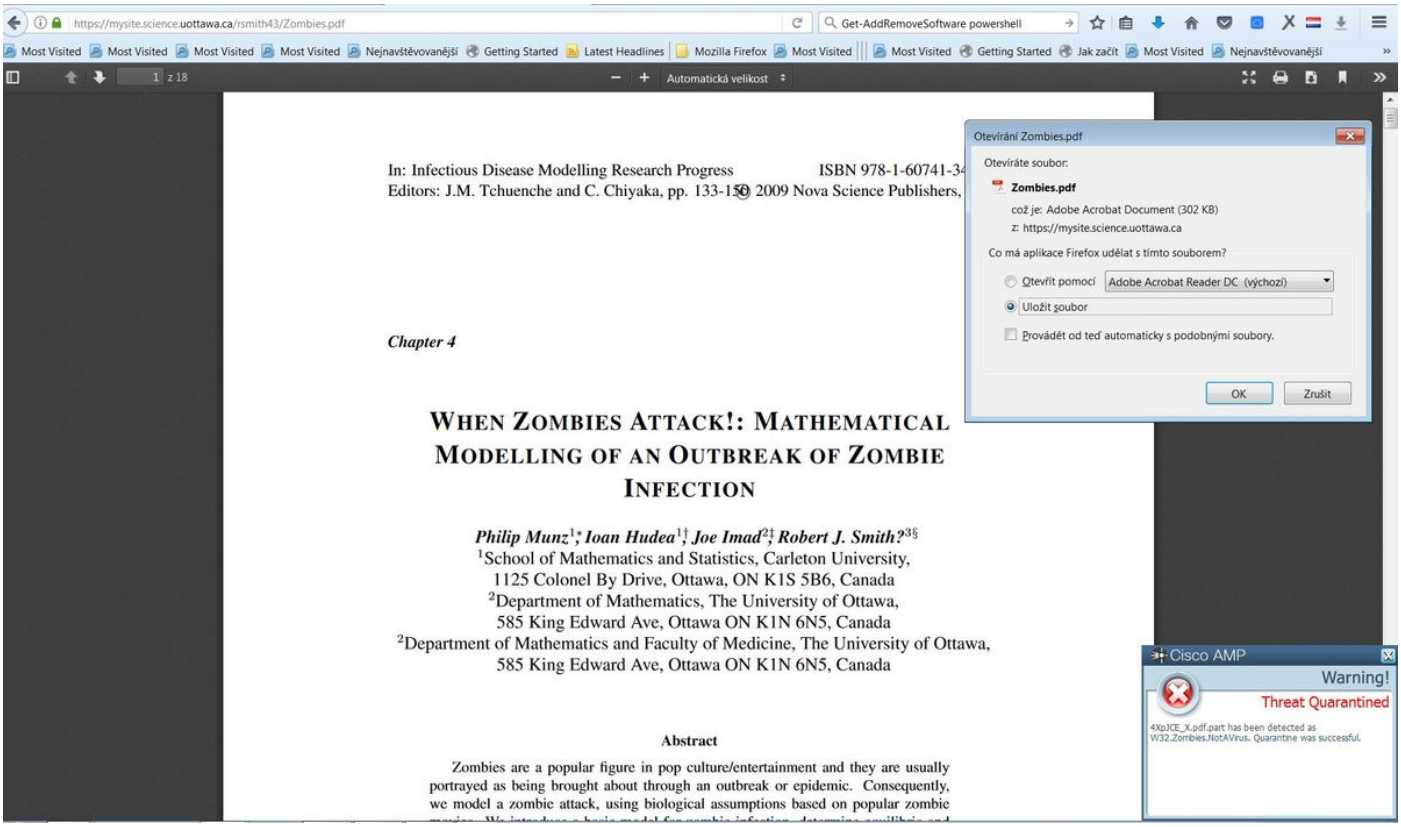
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

Étape 8 : Test avec une chaîne Eicar contenue dans un fichier PDF Zombies

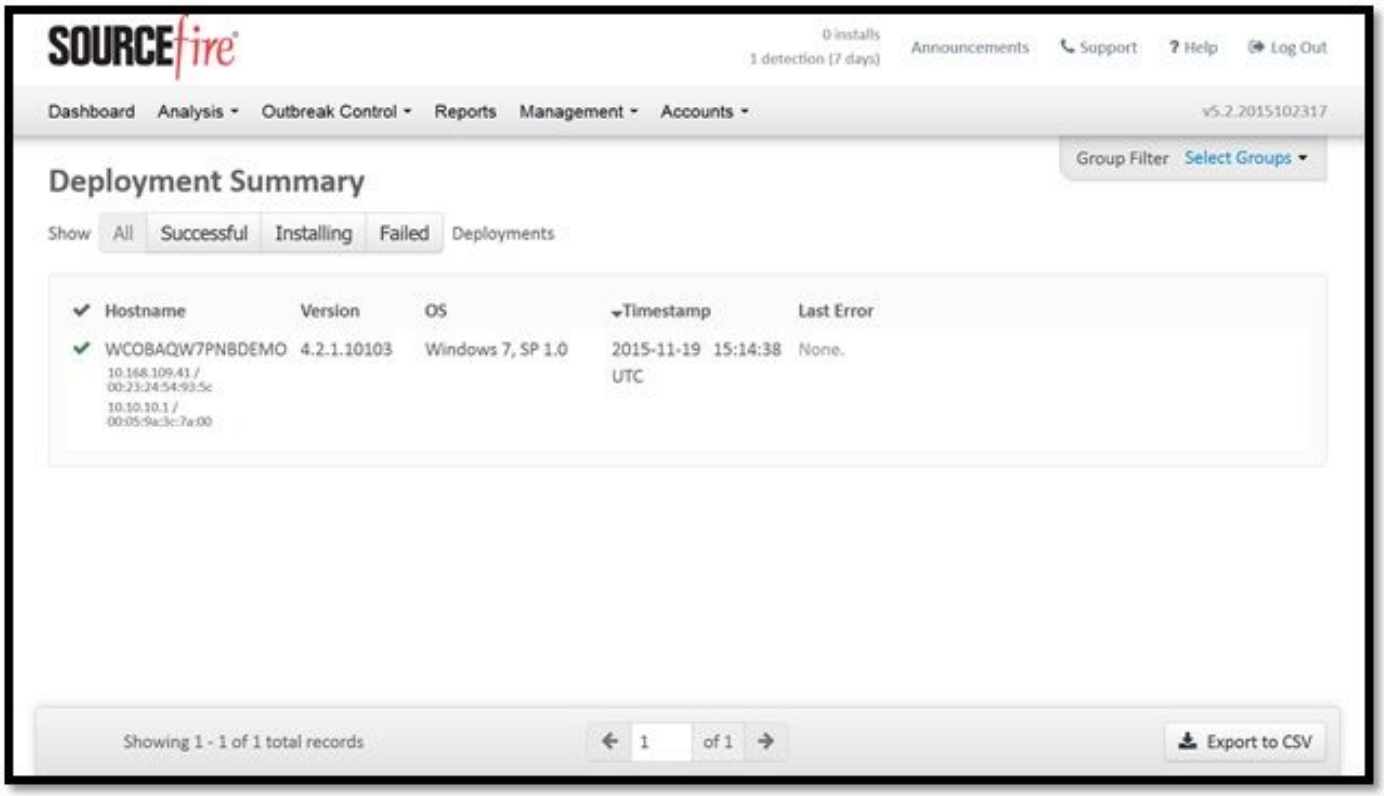
Testez avec une chaîne Eicar contenue dans un fichier PDF Zombies dans un ordinateur de test afin de vérifier que le fichier malveillant est mis en quarantaine.



Zombies.pdf contient une chaîne Eicar

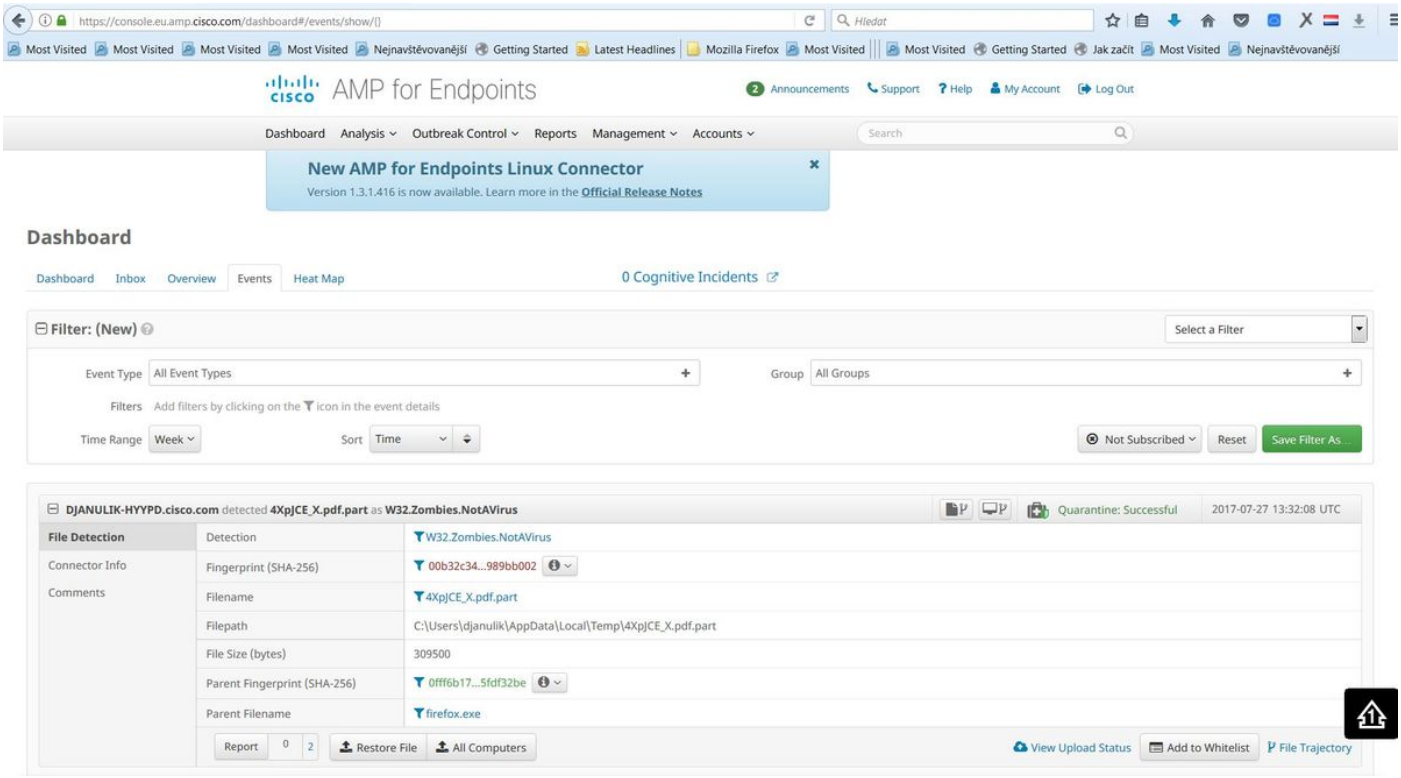
Étape 9 : Résumé du déploiement

Cette page affiche la liste des installations réussies et des échecs du connecteur FireAMP ainsi que celles en cours. Vous pouvez accéder à **Management > Deployment Summary**.



Étape 10 : Vérification de la détection de thread

Zombies.pdf a déclenché un événement de quarantaine, envoyé au tableau de bord AMP.



Événement de quarantaine

Additional Information

Pour obtenir votre compte AMP, vous pouvez vous inscrire à l'université ATS. Ceci vous donne une vue d'ensemble des fonctionnalités AMP dans le TP.

Informations connexes

- Configurer l'activateur AMP
- Support et documentation techniques - Cisco Systems