Installazione e configurazione del modulo AMP con AnyConnect 4.x e AMP Enabler

Sommario

Introduzione

In questo documento viene descritto come installare il connettore Advanced Malware Protection (AMP) con AnyConnect.

AnyConnect AMP Enabler viene utilizzato come supporto per l'implementazione di AMP for Endpoints. Di per sé non ha la capacità di condannare l'eliminazione dei file. Il software AMP for Endpoints viene spostato su un endpoint dall'appliance ASA. Una volta installato, l'AMP utilizza la capacità del cloud per verificare l'eliminazione dei file. Un altro servizio AMP può inviare i file all'analisi dinamica chiamata ThreatGrid, per valutare il comportamento dei file sconosciuti. Questi file possono essere condannati come dannosi se si verificano determinati artefatti. Questo è ampiamente utile per gli attacchi zero-day.

Prerequisiti

Requisiti

- AnyConnect Secure Mobility Client versione 4.x
- FireAMP/AMP for Endpoints

- Adaptive Security Device Manager (ASDM) versione 7.3.2 o successive

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Adaptive Security Appliance (ASA) 5525 con software versione 9.5.1
- AnyConnect Secure Mobility Client 4.2.00096 su Microsoft Windows 7 Professional a 64 bit
- ASDM versione 7.5.1(12)

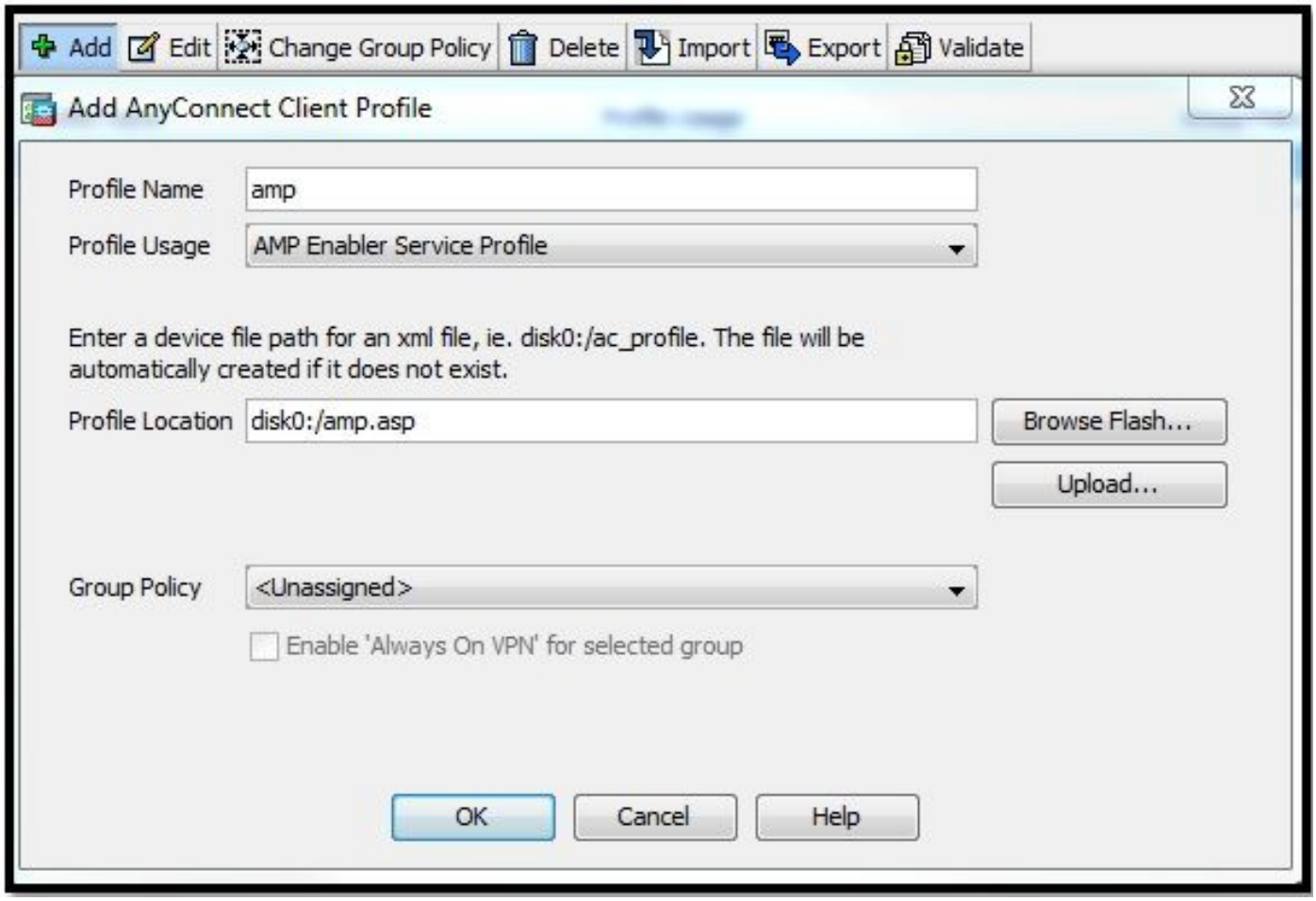
Implementazione di AnyConnect per AMP Enabler tramite ASA

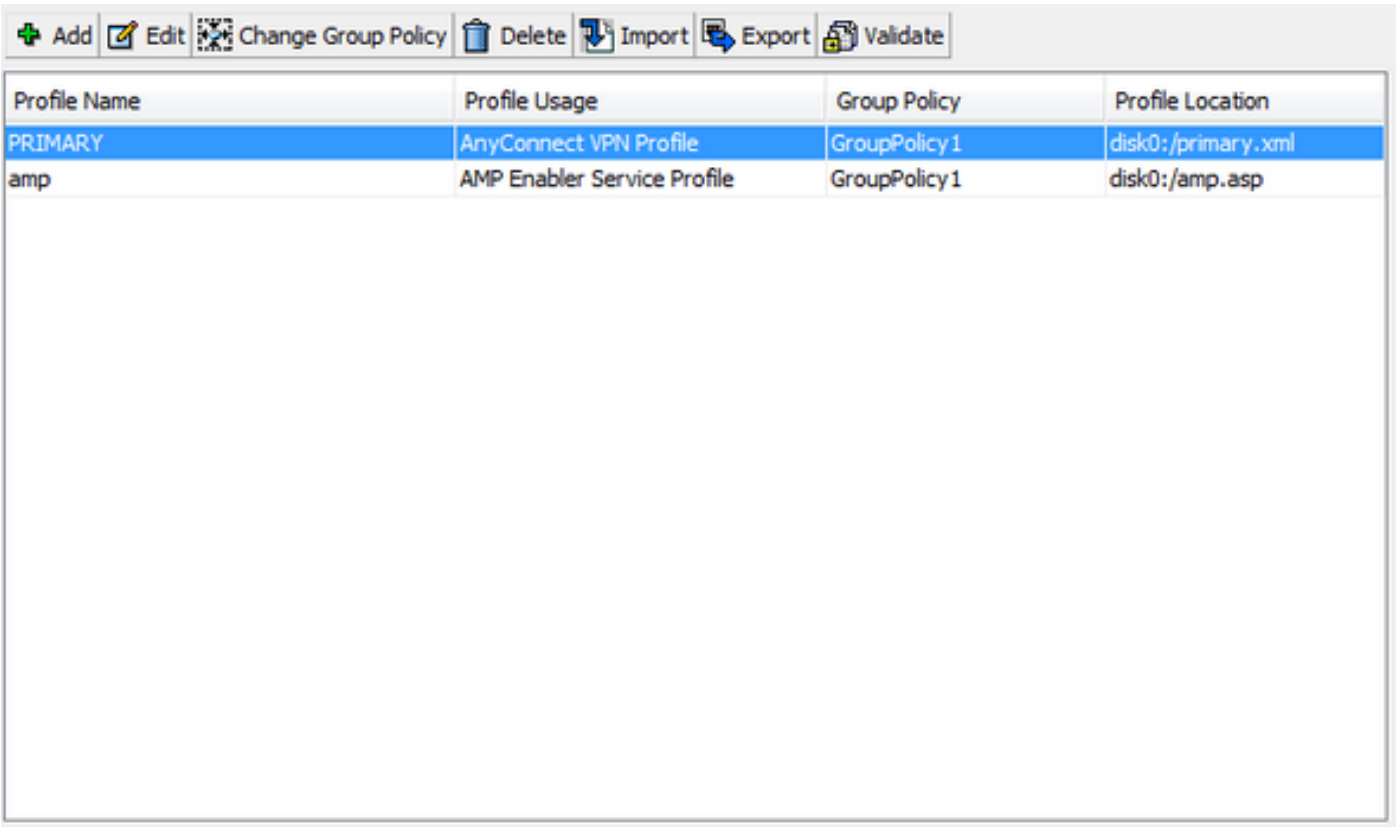
Di seguito sono riportati i passi da eseguire per la configurazione.

- Configurare il profilo client di AnyConnect AMP Enabler.
- Modificare i criteri di gruppo di AnyConnect VPN e scaricare AMP Enabler Service Profile.
- Accedere al dashboard AMP per ottenere il collegamento di download dell'URL del connettore.
- Verificare l'installazione nel computer dell'utente.

Passaggio 1: Configurazione del profilo client di AnyConnect AMP Enabler

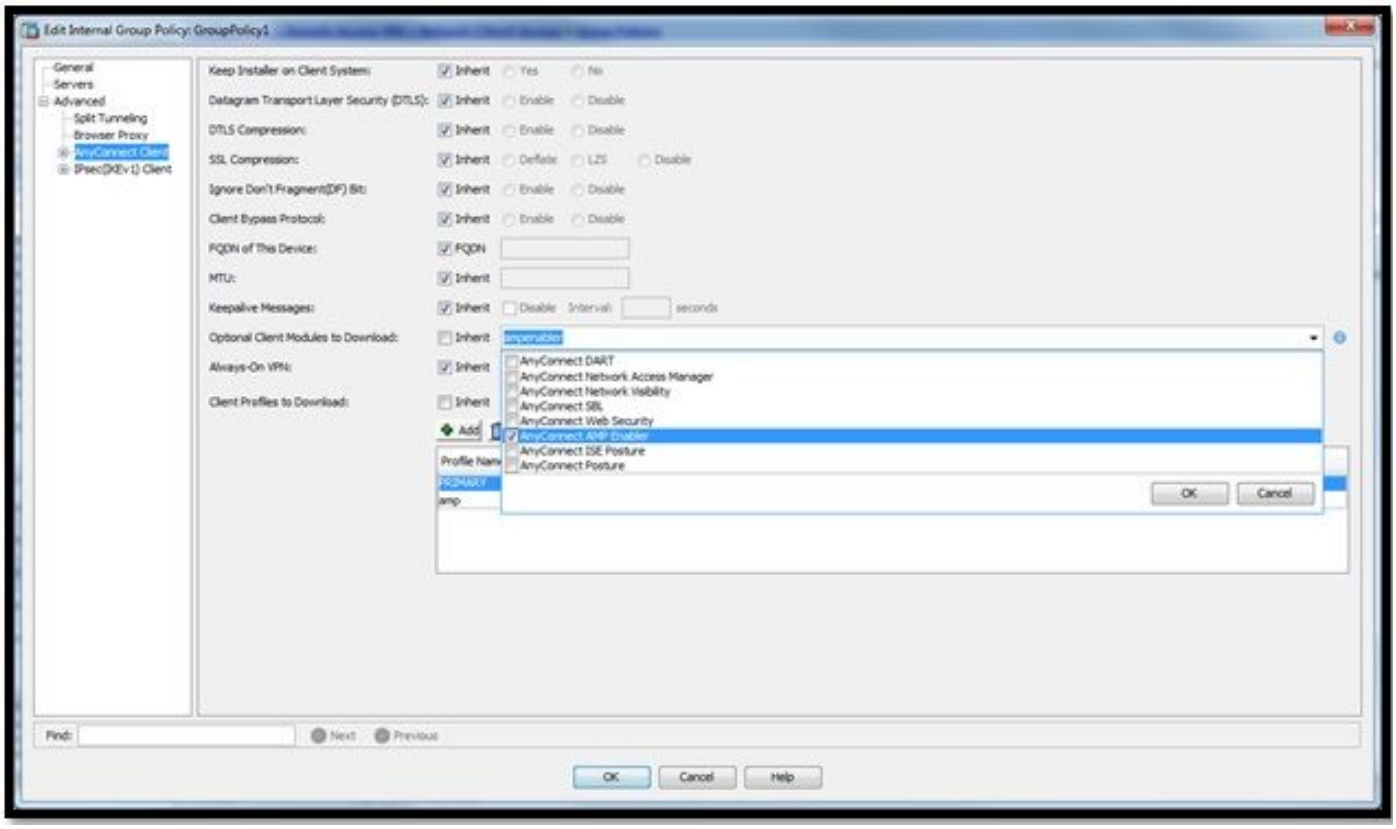
- Selezionare Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profilo client AnyConnect.
- Aggiungere AMP Enabler Service Profile.





Passaggio 2: Modificare i Criteri di gruppo per scaricare AnyConnect AMP Enabler

- Selezionare Configurazione > Rimuovi VPN di accesso > Criteri di gruppo > Modifica.
- Selezionare Advanced > AnyConnect Client > Optional Client Module da scaricare.
- Scegliere AnyConnect AMP Enabler.



Passaggio 3: Scarica criteri FireAMP

Nota: Prima di procedere, verificare che il sistema soddisfi i requisiti per AMP of Endpoints Windows Connector.

Requisiti di sistema per AMP for Endpoints Windows Connector

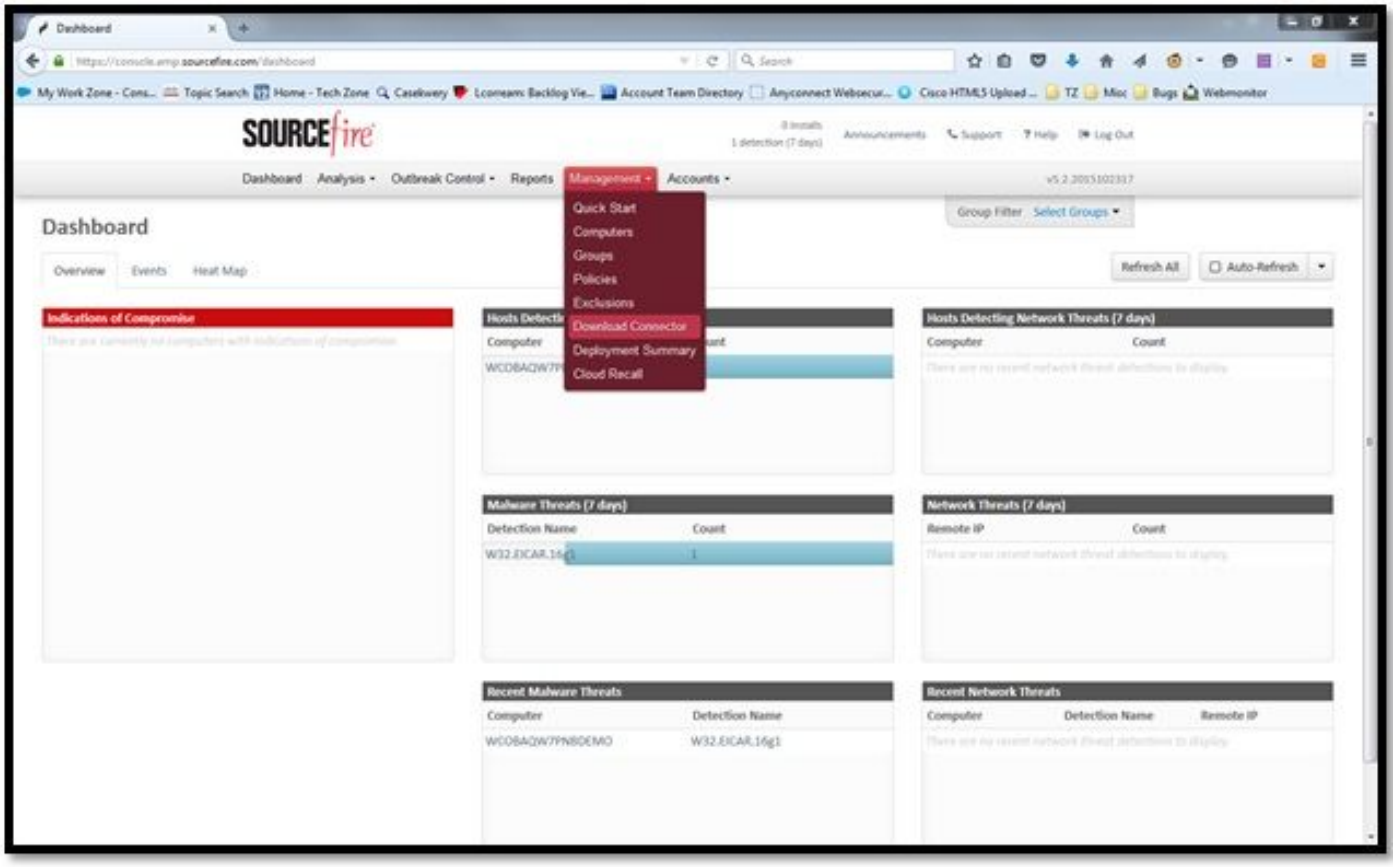
Questi sono i requisiti minimi di sistema per il connettore FireAMP basato sul sistema operativo Windows. Il connettore FireAMP supporta le versioni a 32 bit e a 64 bit di questi sistemi operativi. L'ultima documentazione di AMP è disponibile nell'implementazione di AMP

Sistema operativo	Processore	Memoria	Spazio su disco, Modalità solo cloud	Spazio su disco
Microsoft Windows 7	Processore da 1 GHz o superiore	1 GB di RAM	150 MB di spazio disponibile sul disco rigido - Modalità solo	1 GB di spazio disponibile sul disco rigido - TETRA

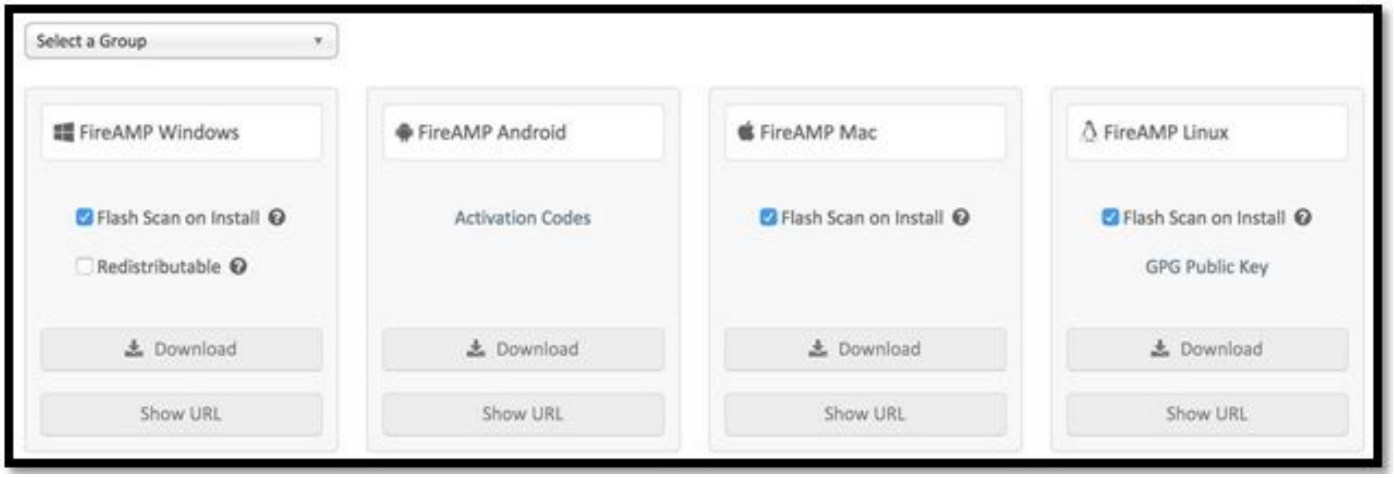
			cloud	
Microsoft Windows 8 e 8.1 (richiede FireAMP Connector 5.1.3 o versione successiva)	Processore da 1 GHz o superiore	512 MB	150 MB di spazio disponibile sul disco rigido - Modalità solo cloud	1 GB di spazio disponibile sul disco rigido - TETRA
Microsoft Windows Server 2003	Processore da 1 GHz o superiore	512 MB	150 MB di spazio disponibile sul disco rigido - Modalità solo cloud	1 GB di spazio disponibile sul disco rigido - TETRA
Microsoft Windows Server 2008	Processore a 2 GHz o superiore	2 GB di RAM	150 MB di spazio disponibile sul disco rigido - Modalità solo cloud	1 GB di spazio disponibile sul disco rigido - TETRA
Microsoft Windows Server 2012 (richiede FireAMP Connector 5.1.3 o versione successiva)	Processore a 2 GHz o superiore	2 GB di RAM	150 MB di spazio disponibile sul disco rigido - Modalità solo cloud	1 GB di spazio disponibile sul disco rigido - TETRA

In genere, il programma di installazione di AMP viene posizionato sul server Web dell'organizzazione.

Per scaricare il connettore, selezionare Gestione > Scarica connettore. Quindi scegliere tipo e scaricare FireAMP (Windows, Android, Mac, Linux).



La pagina Download Connector consente di scaricare i pacchetti di installazione per ciascun tipo di connettore FireAMP. Il pacchetto può essere inserito in una condivisione di rete o distribuito tramite il software di gestione.



Seleziona un gruppo

- Solo controllo: Monitoraggio del sistema basato su SHA-256 calcolato su ciascun file. Questa modalità di solo controllo non mette in quarantena il malware, ma invia un evento come avviso.
- Protezione: Modalità di protezione con la quarantena di file dannosi. Monitorare la copia e lo spostamento dei file.
- Valutazione: Questa opzione può essere utilizzata su computer già compromessi/infetti.
- Server: Suite di installazione per server Windows, in cui il connettore viene installato senza

motore Tetra e driver DFC. Questo gruppo è progettato in base al nome per server non controller di dominio.
- Controller di dominio: Il criterio predefinito per questo gruppo è impostato sulla modalità di controllo come nel gruppo Server. Associare tutti i server Active Directory in questo gruppo, ovvero il connettore verrà eseguito in un controller di dominio di Windows.

L'AMP ha la funzione chiamata TETRA, che è un motore antivirus completo. Questa opzione è facoltativa in base ai criteri.

Caratteristiche

- Flash Scan all'installazione: Il processo di analisi viene eseguito durante l'installazione. L'esecuzione è relativamente rapida e si consiglia di eseguirla una sola volta.
- Ridistribuibile: È consigliabile scaricare un singolo pacchetto contenente programmi di installazione a 32 e a 64 bit. Piuttosto che un programma di avvio automatico, che è disponibile lasciando questa opzione deselezionata e scarica i file del programma di installazione, una volta eseguito.

Nota: È possibile creare un proprio gruppo e configurarvi i criteri associati. Lo scopo è quello di inserire tutti i server Active Directory, ad esempio in un unico gruppo, in cui il criterio è in modalità di controllo.
Il programma di avvio automatico e il programma di installazione ridistribuibile contengono inoltre un file policy.xml utilizzato come file di configurazione per il connettore AMP.

Passaggio 4: Scarica il profilo client di Web Security

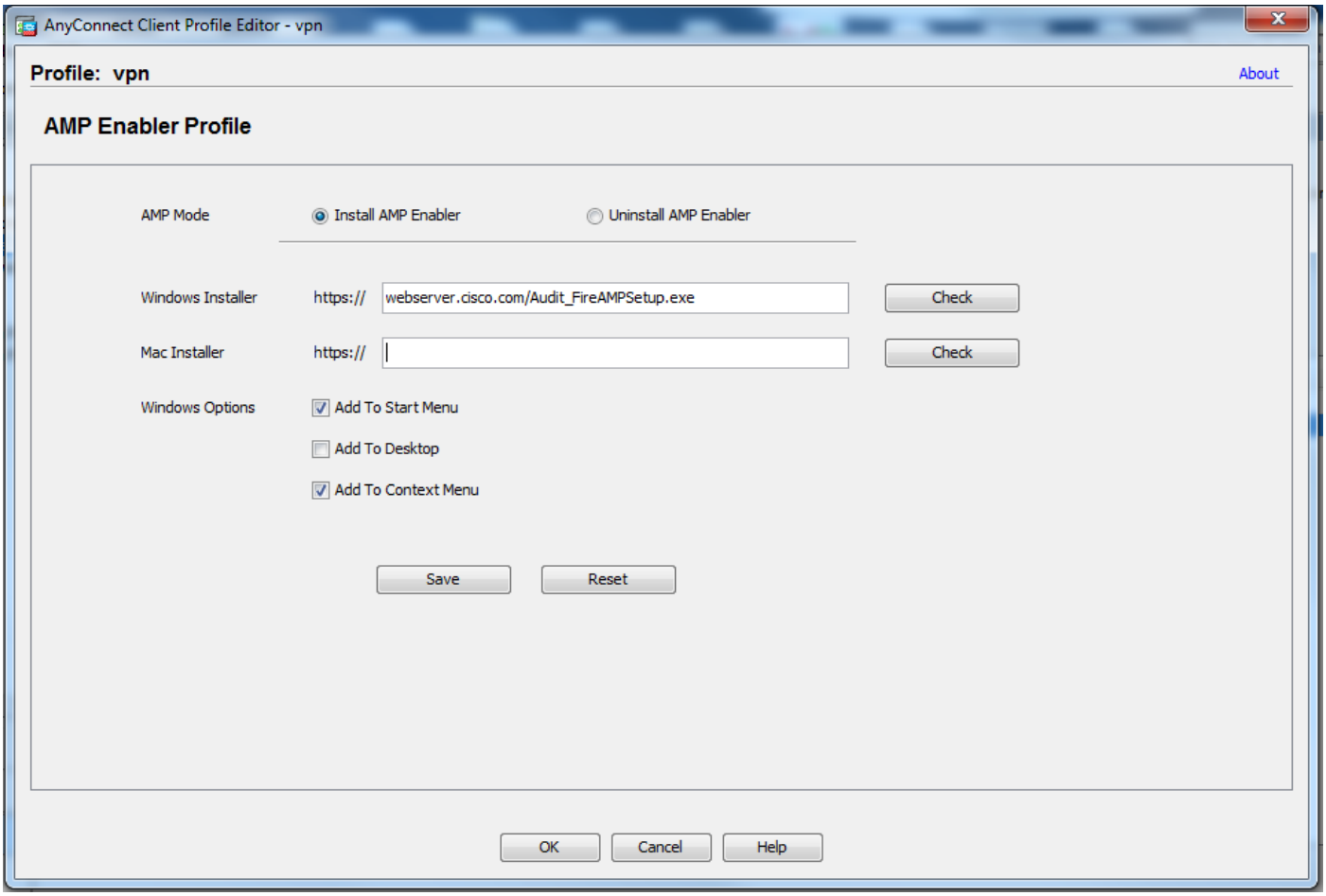
Specificare il server Web della società o una condivisione di rete con il programma di installazione di AMP. Questo metodo viene utilizzato in genere nelle aziende per risparmiare larghezza di banda e collocare gli installatori attendibili in una posizione centralizzata.

Verificare che sia possibile raggiungere il collegamento HTTPS sugli endpoint senza errori di certificato e che il certificato radice sia installato nell'archivio del computer.

Tornare al profilo AMP creato in precedenza sull'appliance ASA (passaggio 1) e modificare il profilo AMP Enabler:

1. Per la modalità AMP, fare clic sul pulsante di opzione Installa AMP Enabler.
2. Nel campo Windows Installer, aggiungere l'indirizzo IP per il server Web e il file per FireAMP.
3. Le opzioni di Windows sono facoltative.

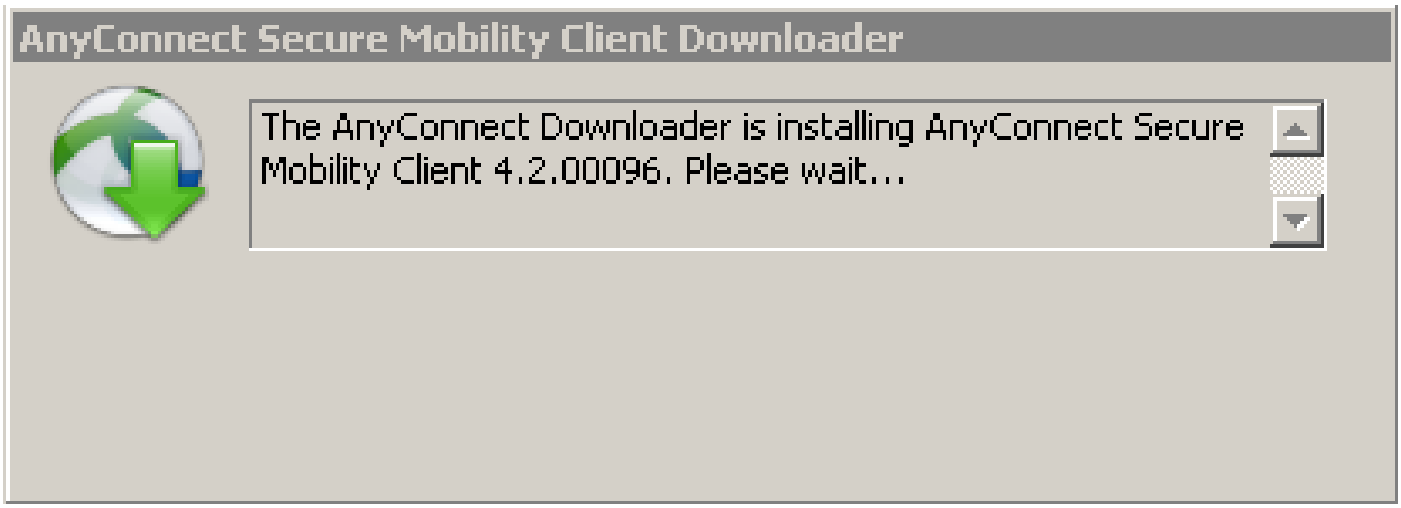
   Fare clic su OK e applicare le modifiche.



Passaggio 5: Collegarsi a AnyConnect e verificare l'installazione del modulo

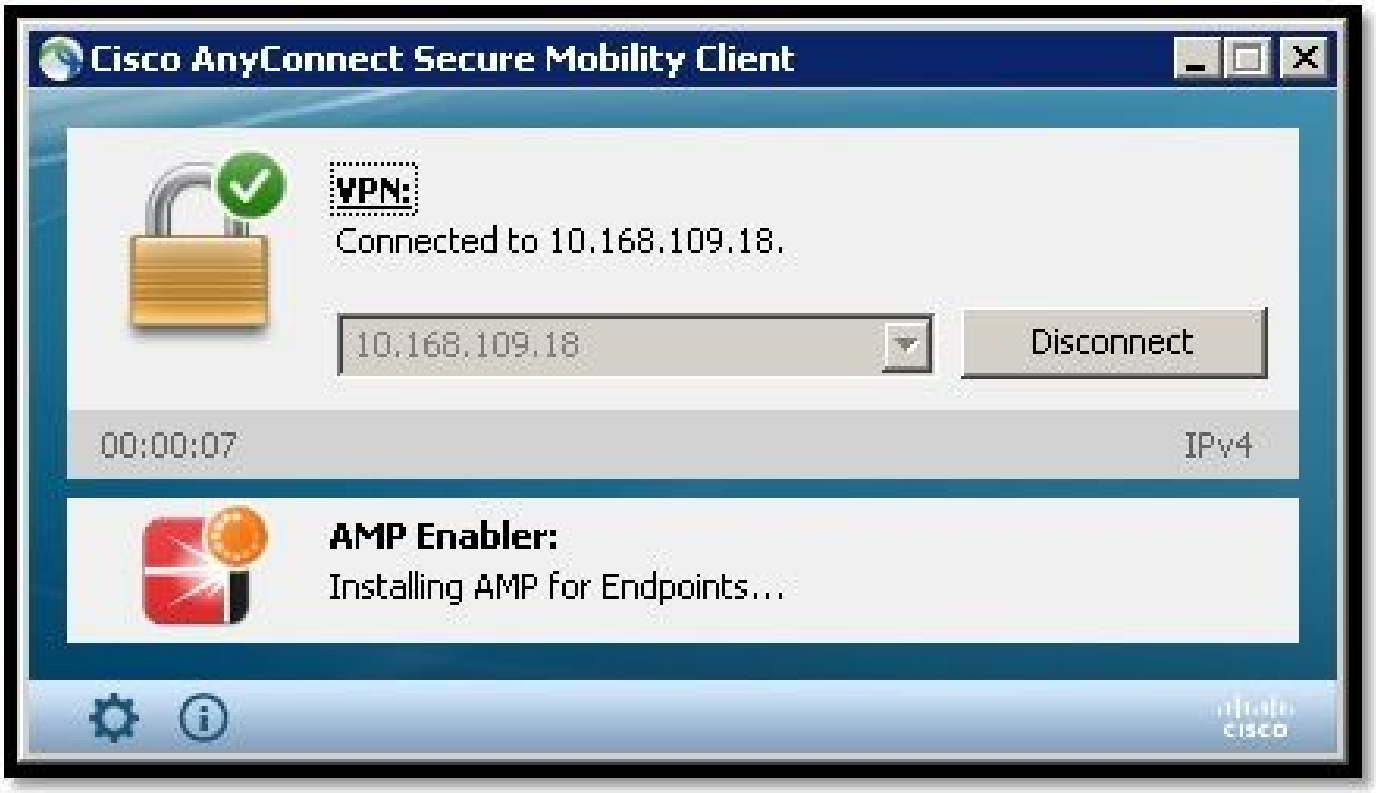
Quando gli utenti si connettono a una VPN, ASA spinge il modulo AnyConnect AMP Enabler attraverso la VPN. Per gli utenti già connessi, è consigliabile disconnettersi e quindi riconnettersi per abilitare la funzionalità.

```
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%
```



Passaggio 6: Avvio dell'installazione di VPN Connection AMP Enabler e AMP Connector

Dopo aver premuto il pulsante connect per avviare la VPN, scarica il nuovo modulo di download. In questo modo AMP Enabler verrà scaricato dal percorso URL specificato due volte prima.




```
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 , retur
```

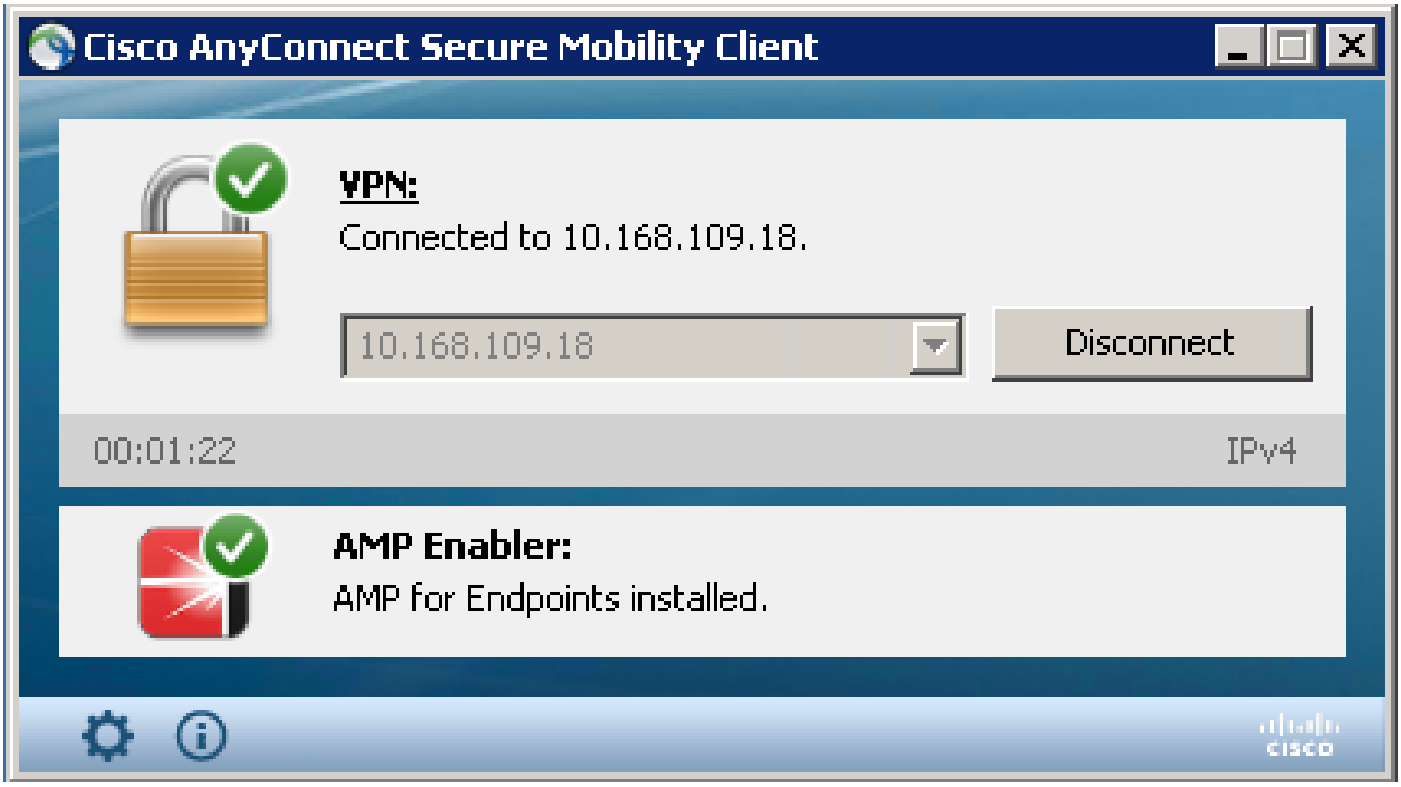
Passaggio 7: Controlla AnyConnect e verifica che tutto sia installato

Dopo aver connesso la VPN e installato la configurazione del server Web, controllare AnyConnect e verificare che tutti i componenti siano installati correttamente.

Nel file services.msc è possibile trovare un nuovo servizio denominato CiscoAMP_5.1.3. Nel comando Powershell sono disponibili:

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

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



AMP Installer aggiunge nuovi driver al sistema operativo Windows. Per elencare i driver, è possibile utilizzare il comando driverquery.

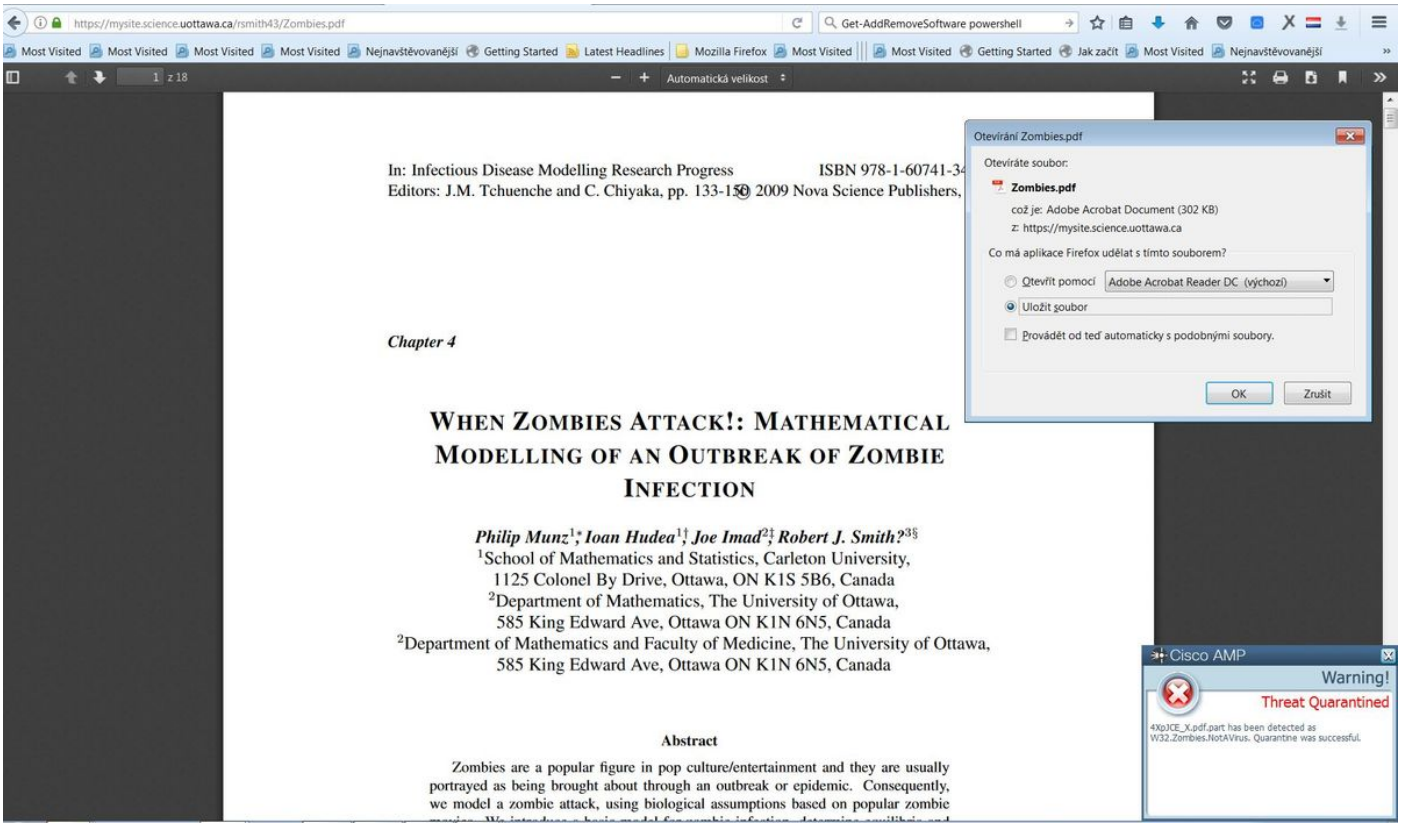
```
C:\Windows\System32>driverquery /v | findstr immunet

ImmunetProte ImmunetProtectDriver   ImmunetProtectDriver   File System   System     Running    OK
LSE          4,096      69,632     0      3/17/2017 5:04:20 PM   \??\C:\WINDOWS\System32\Drivers\immunetp

ImmunetSelfP ImmunetSelfProtectDriv ImmunetSelfProtectDriv File System   System     Running    OK
LSE          4,096      28,672     0      3/17/2017 5:04:08 PM   \??\C:\WINDOWS\System32\Drivers\immunets
```

Passaggio 8: Verifica con una stringa Eicar contenuta in un file PDF Zombies

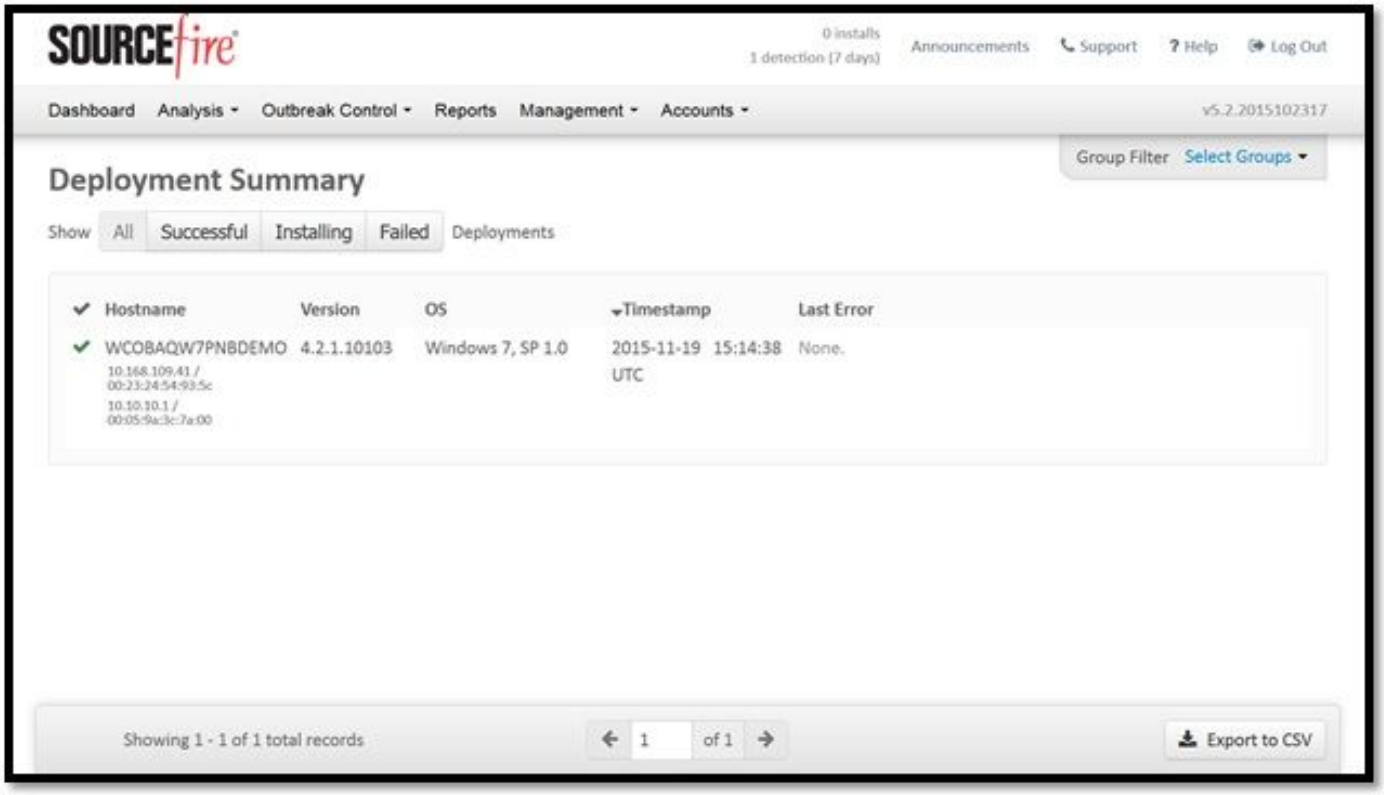
Eseguire il test con una stringa Eicar contenuta in un file PDF Zombies in un computer di test per verificare che il file dannoso sia in quarantena.



Zombies.pdf contiene la stringa Eicar

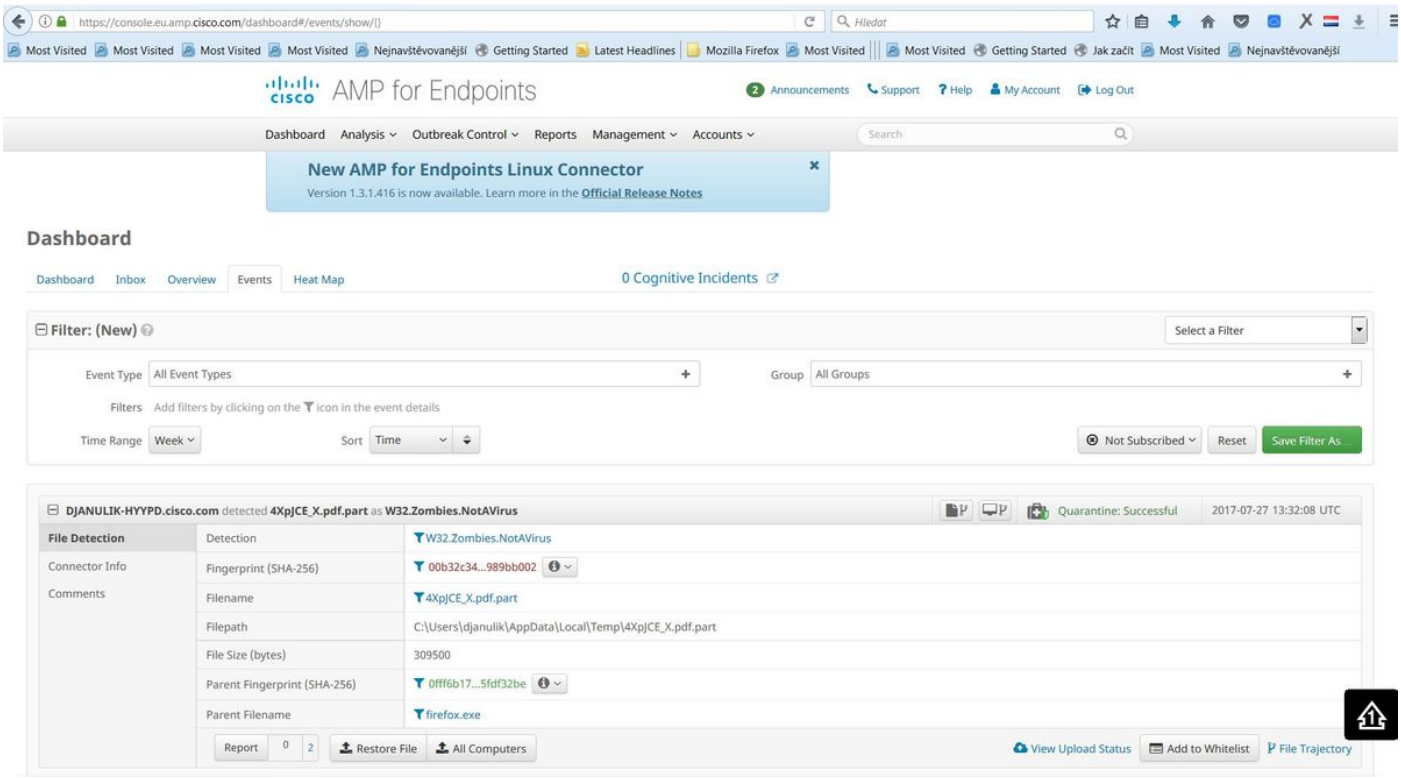
Passaggio 9: Riepilogo della distribuzione

In questa pagina viene visualizzato un elenco delle installazioni riuscite e non riuscite del connettore FireAMP, nonché di quelle attualmente in corso. È possibile passare a Gestione > Riepilogo distribuzione.



Passaggio 10: Verifica rilevamento thread

Zombies.pdf ha attivato un evento di quarantena, da inviare al dashboard AMP.



Evento quarantena

Ulteriori informazioni

Per ottenere il tuo account AMP, puoi iscriverti all'università ATS. Questa pagina offre una panoramica della funzionalità AMP in LAB.

Informazioni correlate

- Configurare AMP Enabler
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).