通过AnyConnect 4.x和AMP Enabler安装和配置AMP模块

目录

简介

本文档将介绍通过AnyConnect安装高级恶意软件防护(AMP)连接器的步骤。

AnyConnect AMP启用程序用作部署面向终端的AMP的介质。它本身没有对文件处置进行定罪的能力。它将面向终端的AMP软件从ASA推送到终端。安装AMP后，它会使用云容量检查文件处置情况。进一步的AMP服务可以将文件提交到名为ThreatGrid的动态分析，以对未知文件行为进行评分。如果满足某些标样，这些文件可被认定为恶意文件。这对零日攻击非常有用。

先决条件

要求

- AnyConnect安全移动客户端版本4.x
- 面向终端的FireAMP/AMP
- 自适应安全设备管理器(ASDM)7.3.2版或更高版本

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 自适应安全设备(ASA)5525，软件版本9.5.1
- Microsoft Windows 7专业版64位版上的AnyConnect安全移动客户端4.2.00096
- ASDM 版本 7.5.1(112)

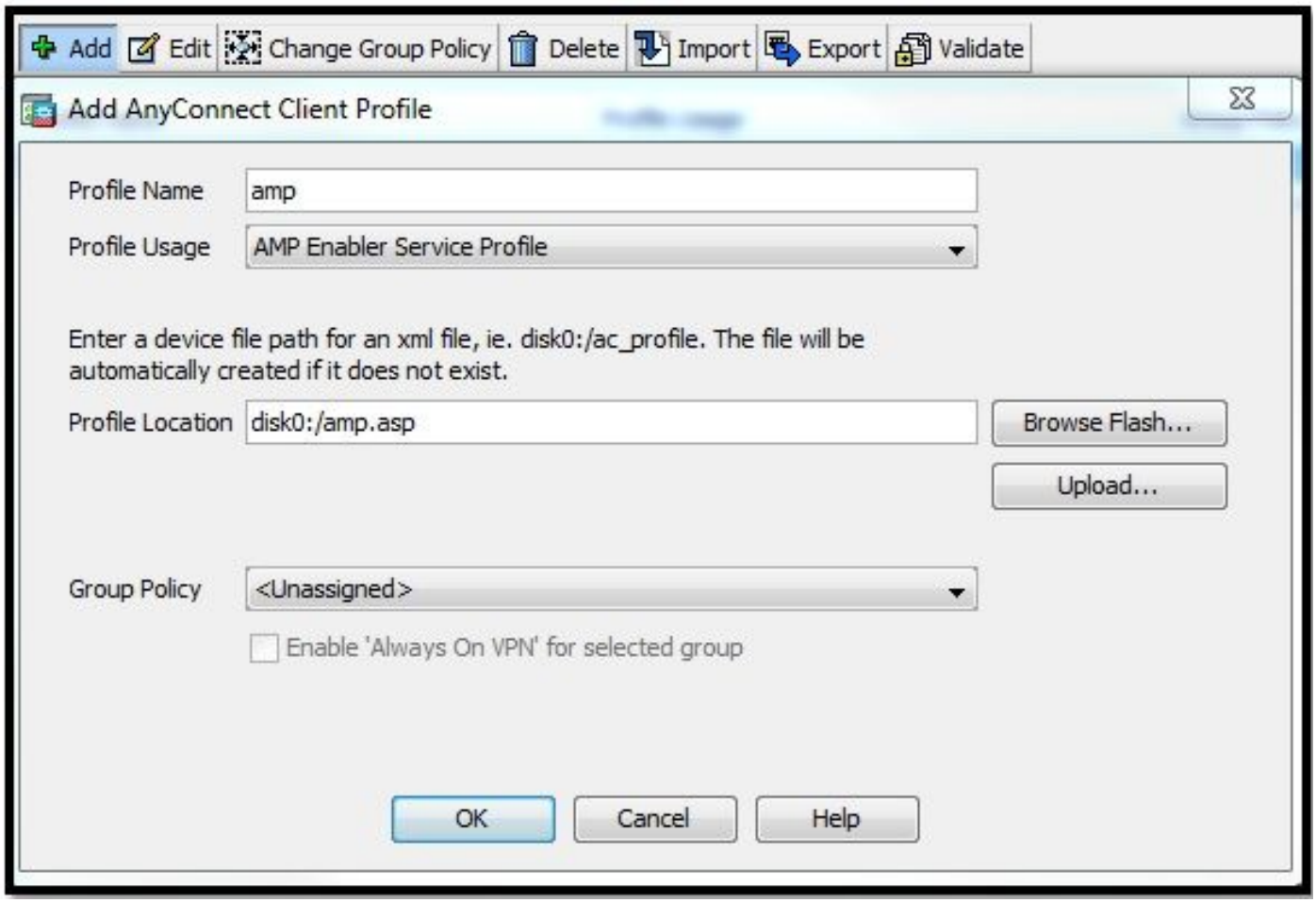
通过ASA为AMP Enabler部署AnyConnect

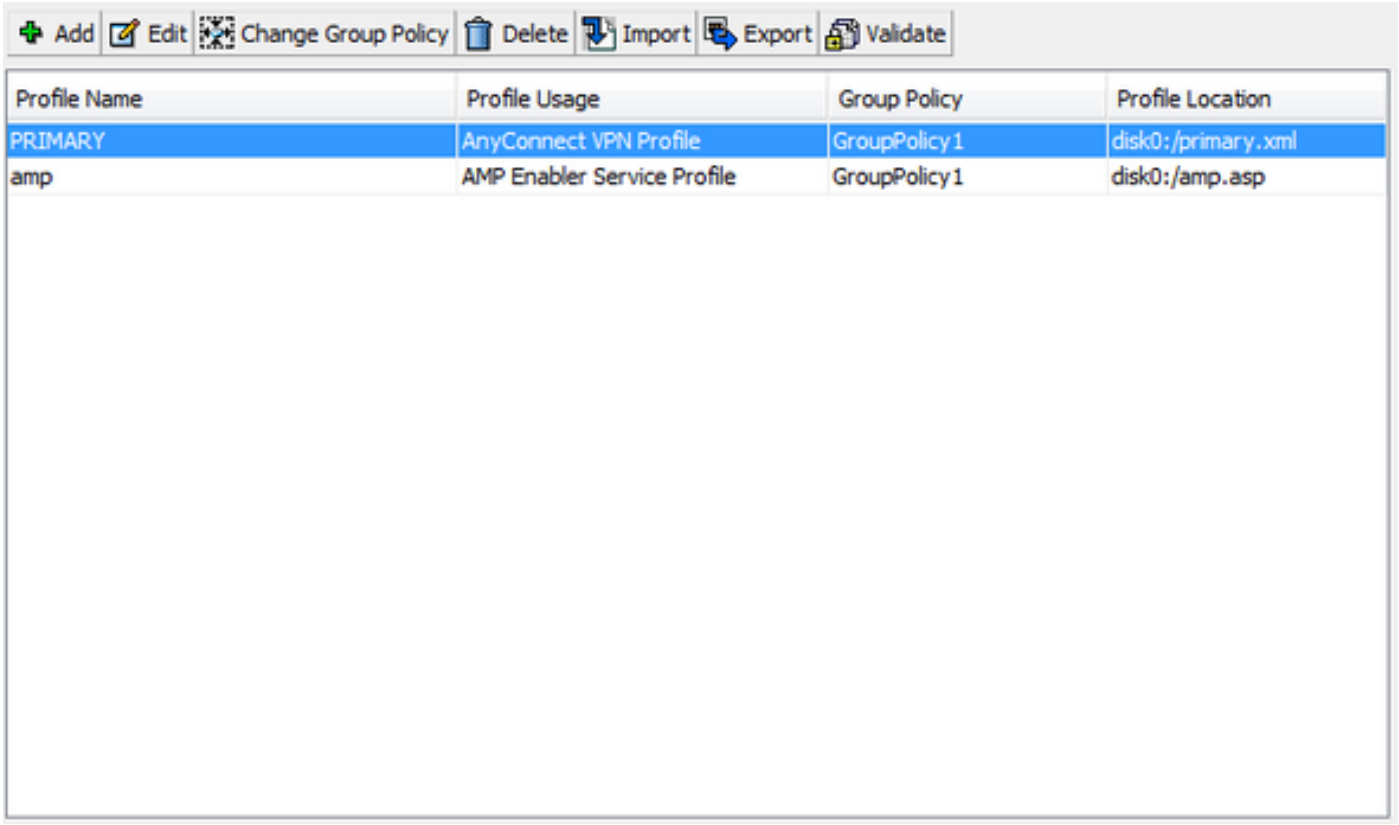
配置中涉及的步骤如下：

- 配置AnyConnect AMP启用程序客户端配置文件。
- 编辑AnyConnect VPN组策略并下载AMP启用程序服务配置文件。
- 登录AMP控制面板以获取连接器URL下载链接。
- 验证用户计算机上的安装。

步骤 1：配置AnyConnect AMP启用程序客户端配置文件

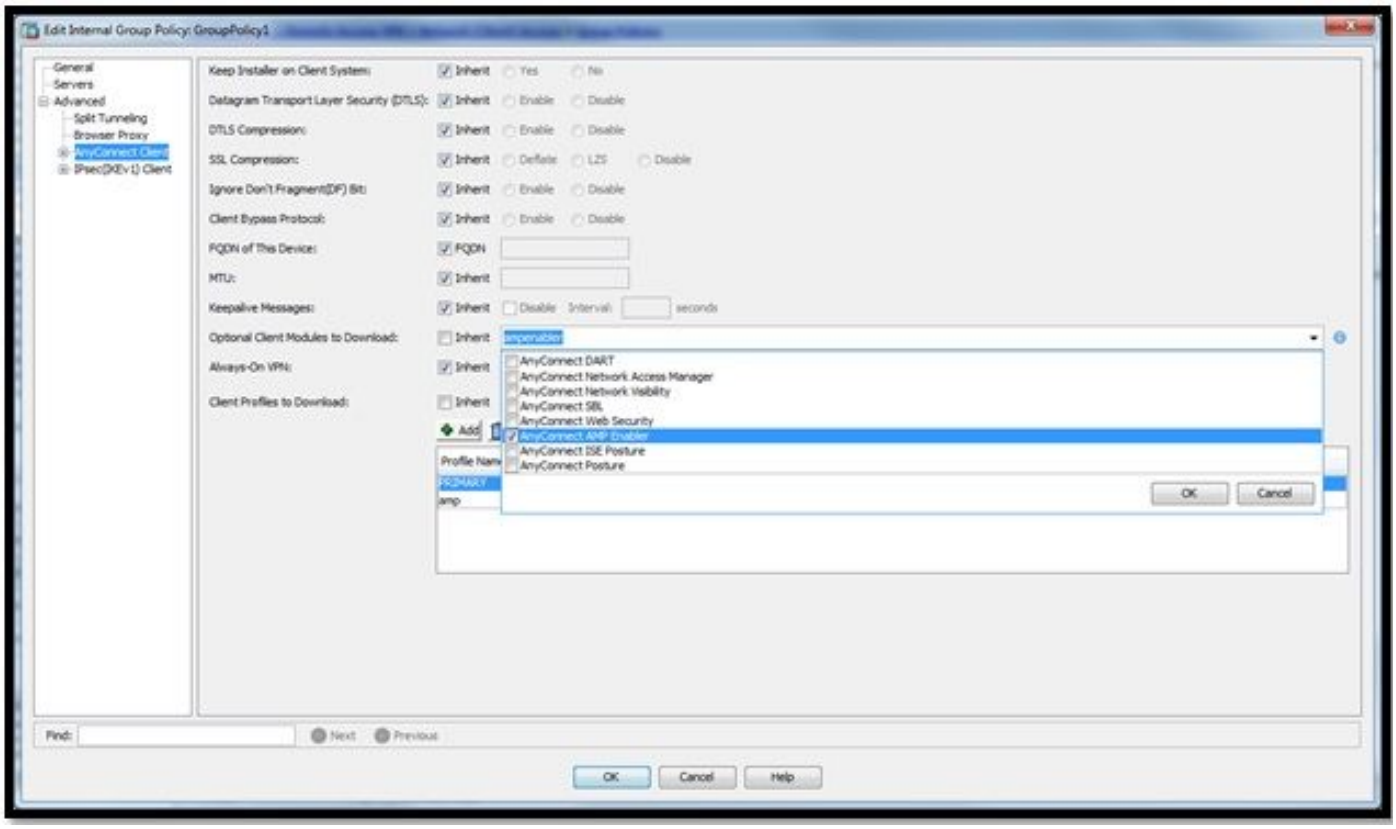
- 导航至**Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Client Profile**。
- 添加AMP启**用程序服务配置文件**。





步骤 2：编辑组策略以下载AnyConnect AMP启用程序

- 导航至Configuration > Remove Access VPN > Group Policies > Edit。
- 转至“高级”>“AnyConnect客户端”>“可选客户端模块”以下载。
- 选择AnyConnect AMP Enabler。



步骤 3：下载FireAMP策略

注意：在继续之前，检查您的系统是否满足终端AMP Windows连接器的要求。

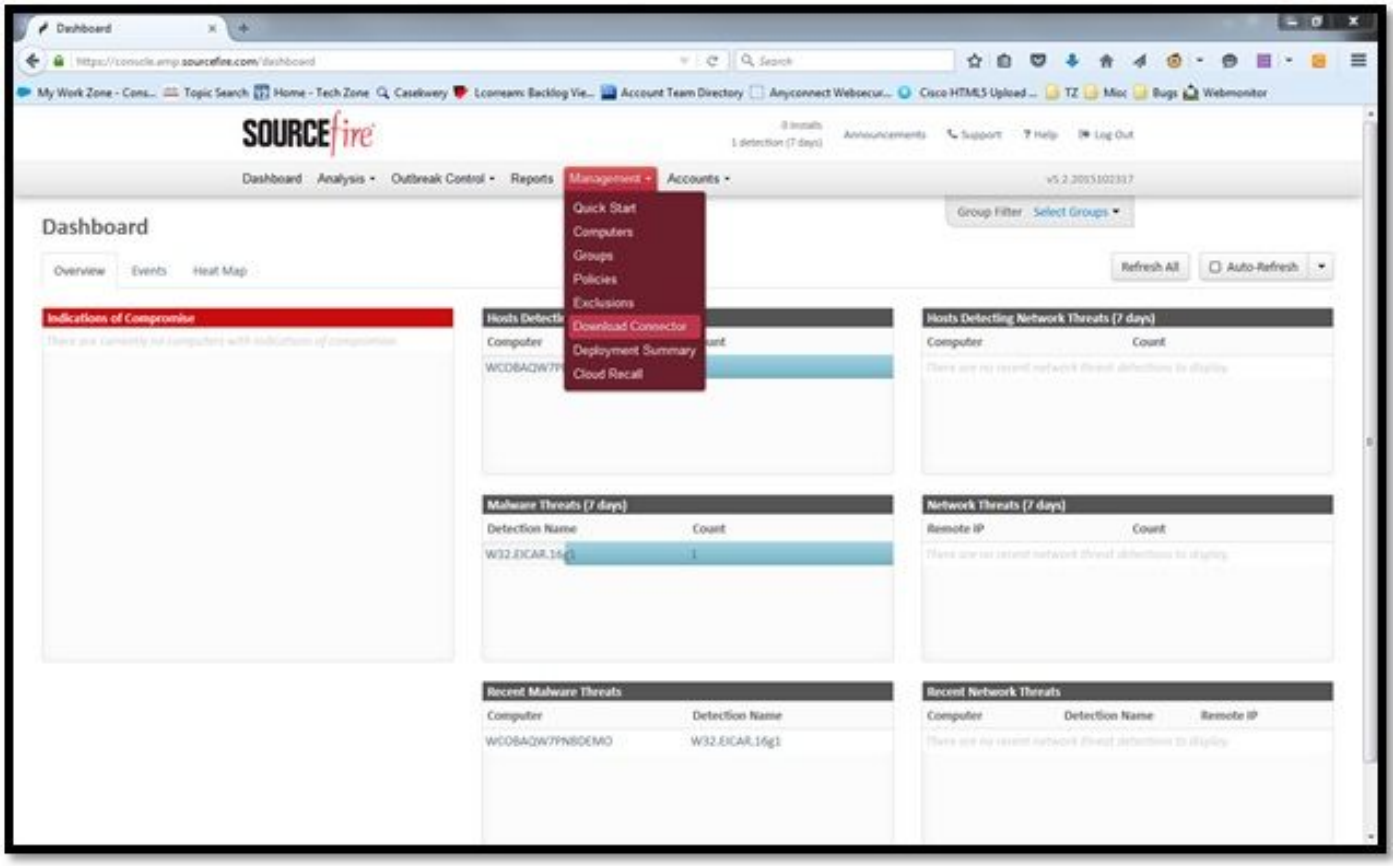
面向终端的AMP的系统要求Windows连接器

这些是基于Windows操作系统的FireAMP连接器的最低系统要求。FireAMP连接器支持这些操作系统的32位和64位版本。最新的AMP文档可在AMP部署中找到

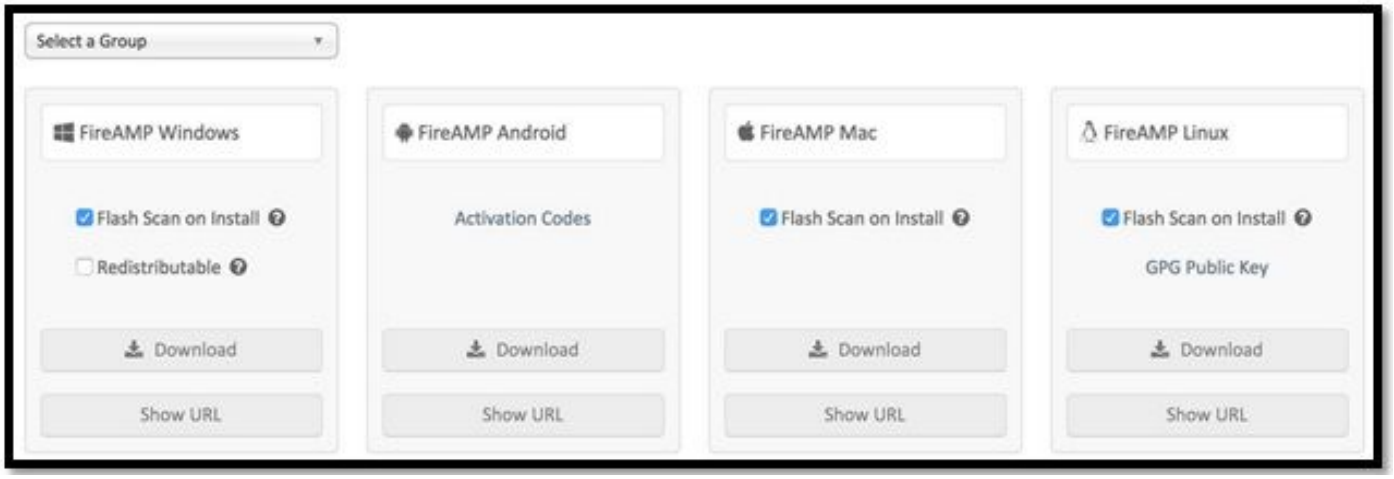
操作系统	处理器	内存	磁盘空间、仅云模式	磁盘空间
Microsoft Windows 7	1 GHz或更快的处理器	1 GB RAM	150 MB可用硬盘空间 — 仅云模式	1 GB可用硬盘空间 — TETRA
Microsoft Windows 8和8.1（需要FireAMP连接器5.1.3或更高版本）	1 GHz或更快的处理器	512 MB RAM	150 MB可用硬盘空间 — 仅云模式	1 GB可用硬盘空间 — TETRA
Microsoft Windows Server 2003	1 GHz或更快的处理器	512 MB RAM	150 MB可用硬盘空间 — 仅云模式	1 GB可用硬盘空间 — TETRA
Microsoft Windows Server 2008	2 GHz或更快的处理器	2 GB RAM	150 MB可用硬盘空间 — 仅云模式	1 GB可用硬盘空间 — TETRA
Microsoft Windows Server 2012（需要FireAMP连接器5.1.3或更高版本）	2 GHz或更快的处理器	2 GB RAM	150 MB可用硬盘空间 — 仅云模式	1 GB可用硬盘空间 — TETRA

最常见的是将AMP安装程序放在企业Web服务器上。

要下载连接器，请导航至**Management > Download Connector**。然后选择类型，并**下载** FireAMP(Windows、Android、Mac、Linux)。



“下载连接器”(Download Connector)页面允许您下载每种FireAMP连接器的安装包。此软件包可以放置在网络共享中，也可以通过管理软件分发。



选择用户列表组

- **仅审核**：根据对每个文件计算的SHA-256监控系统。此“仅审核”模式不会隔离恶意软件，而是将事件作为警报发送。
- **保护**：使用隔离恶意文件保护模式。监控文件复制和移动。
- **分类**：这用于已受感染/受感染的计算机。
- **服务器**：用于Windows服务器的安装套件，其中连接器安装时不使用Tetra引擎和DFC驱动程序。此组由其名称为非域控制器服务器设计。
- **域控制器**:此组的默认策略设置为审核模式，与在服务器组中一样。关联此组中的所有Active Directory服务器，这意味着连接器将在Windows域控制器上运行。

AMP具有称为TETRA的功能，即完全防病毒引擎。此选项是每个策略的可选选项。

功能

- **安装时的Flash Scan:**扫描进程在安装期间运行。执行速度相对较快，建议只运行一次。
- **可再发行：**您应下载一个包，其中包含32位和64位安装程序。启动程序(可用，但此选项未勾选并下载安装程序文件（一旦执行）)。

注意：您可以创建自己的组并为其配置关联策略。其目的是将所有（例如Active Directory服务器）放置到一个组中，其中策略处于审核模式。
引导程序和可再分发安装程序还都包含用作AMP连接器配置文件的policy.xml文件。

步骤 4：下载网络安全客户端配置文件

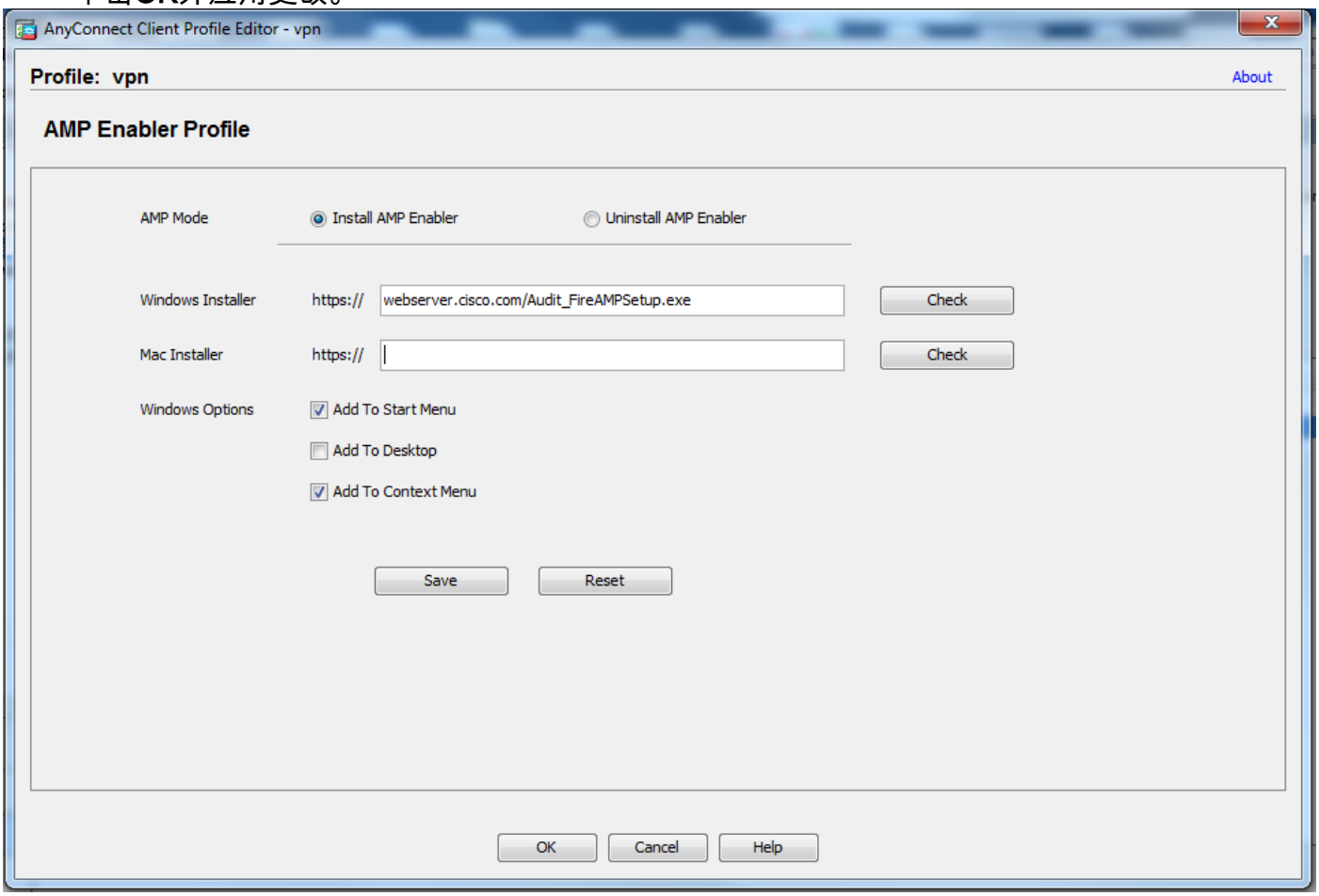
指定公司Web服务器或与AMP安装程序的网络共享。这在公司中最常用，以节省带宽并将受信任的安装程序放置在集中位置。

请确保终端上可以访问HTTPS链接，且没有任何证书错误，并且根证书已安装在计算机存储中。

返回之前在ASA上创建的AMP配置文件（步骤1）并编辑AMP启**用程序配置文件**:

1. 对于AMP模式，单击“Install AMP Enabler(安**装AMP启用程**序)”单选按钮。
2. 在**Windows Installer**字段中，添加Web服务器的IP和FireAMP的文件。
3. Windows选项是可选的。

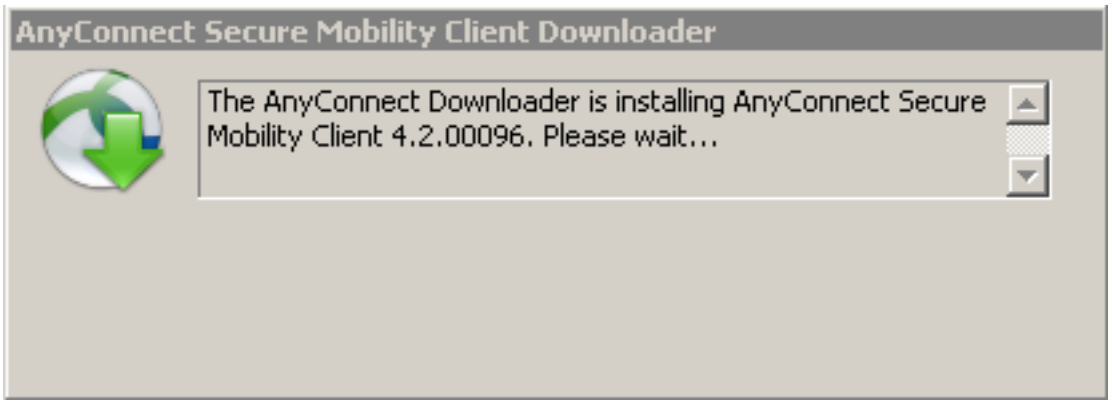
单击**OK**并应用更改。



步骤 5：使用AnyConnect连接并验证模块的安装

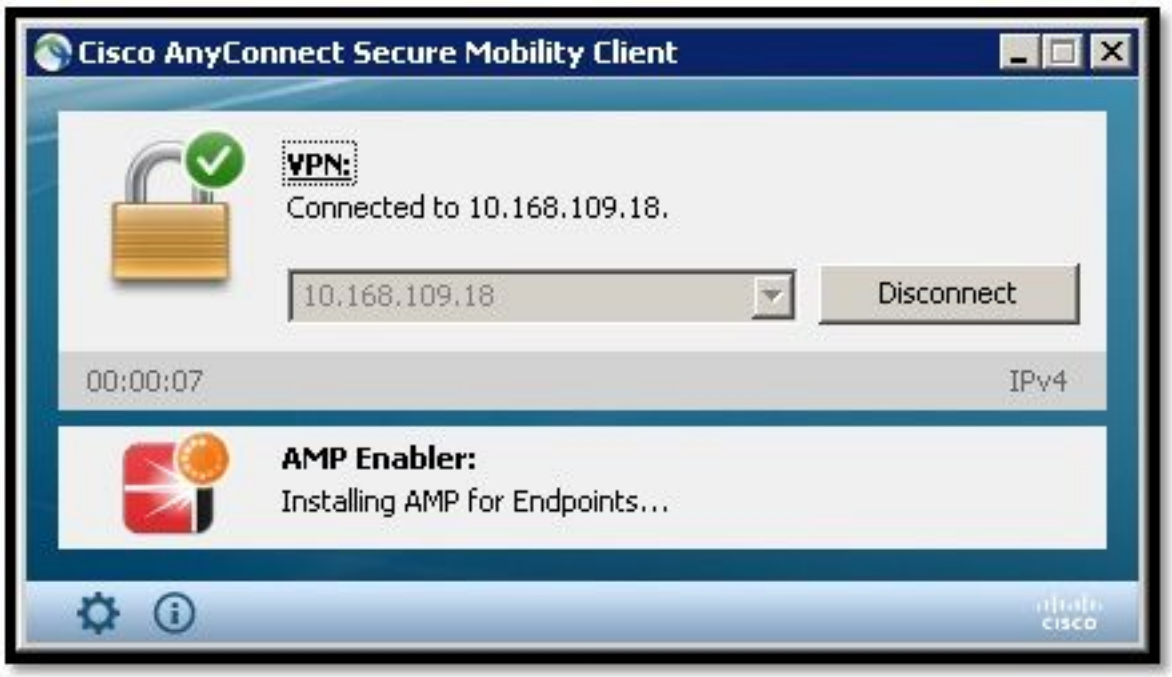
当AnyConnect VPN用户连接时，ASA通过VPN推送AnyConnect AMP启用程序模块。对于已登录的用户，建议注销，然后重新登录以启用功能。

```
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%
```



步骤 6：启动VPN连接安装AMP启用程序和AMP连接器

按下连接以启动VPN的按钮后，它将下载新的下载程序模块。这将具有AMP启用程序，并从您之前指定的几个步骤的URL路径下载AMP软件包。




```
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]
```

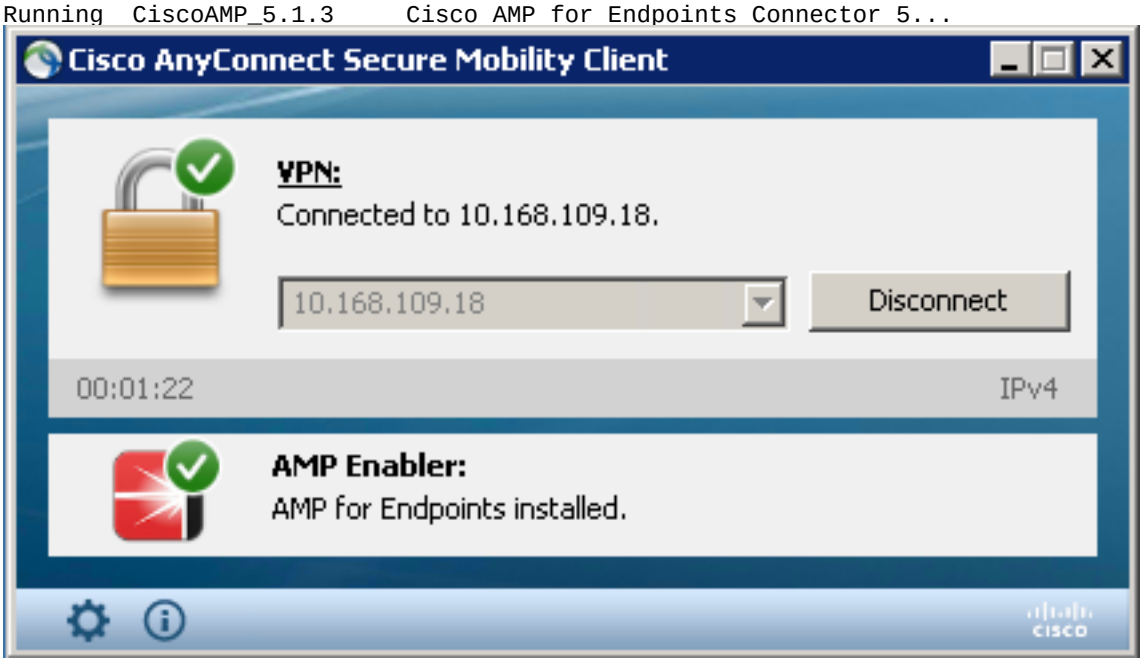
步骤 7：检查AnyConnect并验证是否已安装所有设备

连接VPN并安装Web服务器配置后，检查AnyConnect并验证所有安装都是否正确。

在services.msc中，您可以找到名为CiscoAMP_5.1.3的新服务。在Powershell命令中，我们看到：

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

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



AMP安装程序将新驱动程序添加到Windows操作系统。您可以使用driverquery命令列出驱动程序。

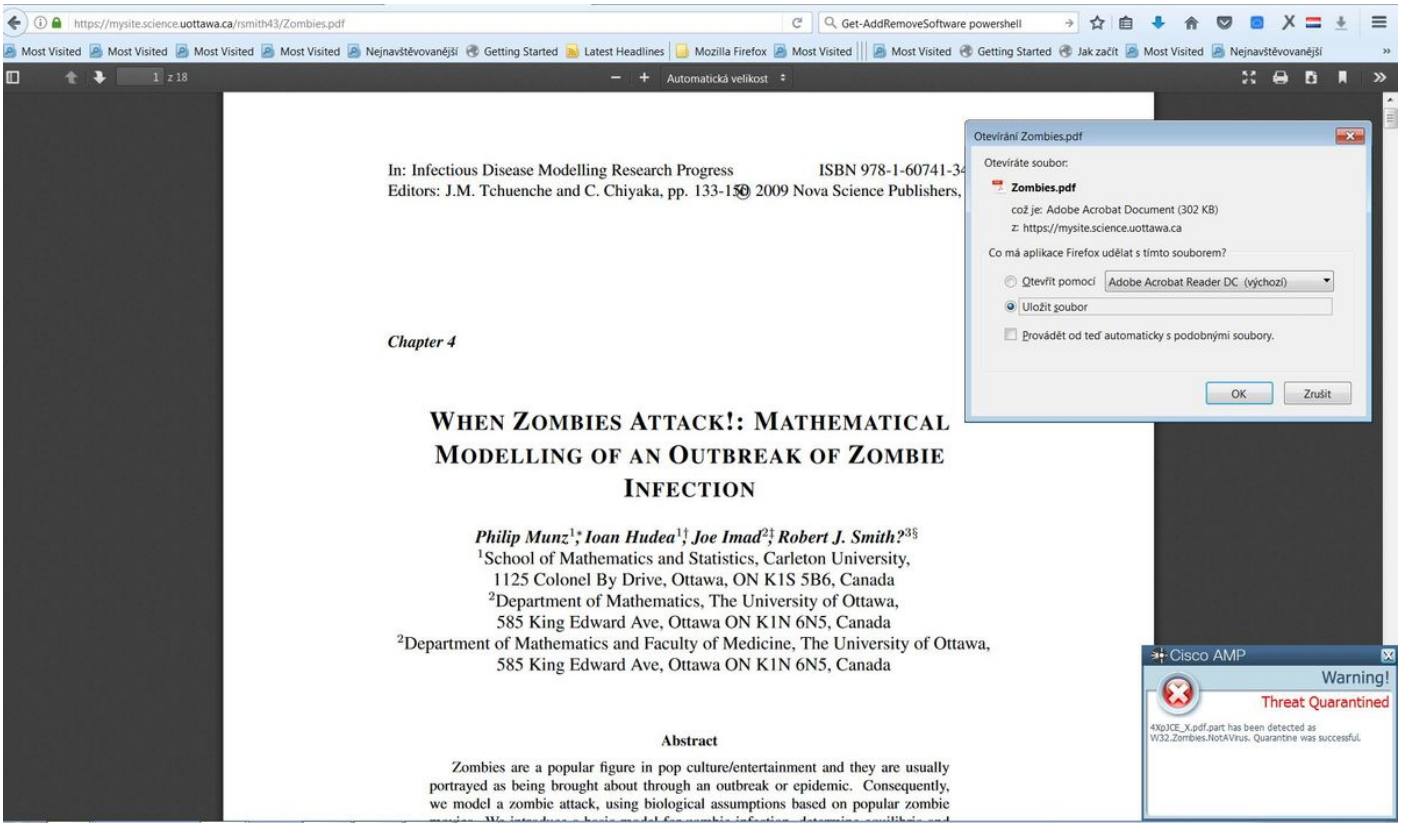
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

步骤 8::使用僵尸PDF文件中包含的Eicar字符串进行测试

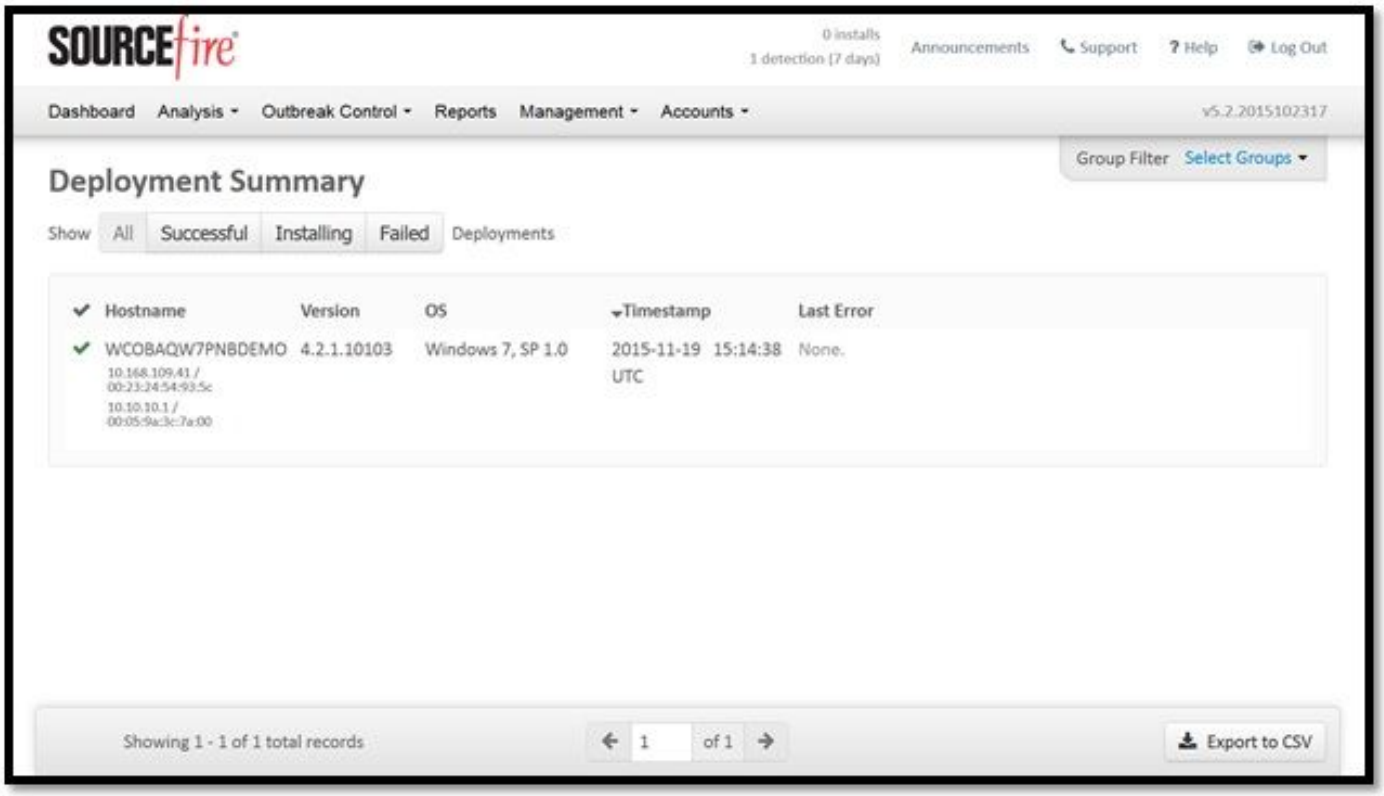
使用测试计算机中僵尸PDF文件中包含的Eicar字符串进行测试，以验证恶意文件是否被隔离。



僵尸.pdf包含Eicar字符串

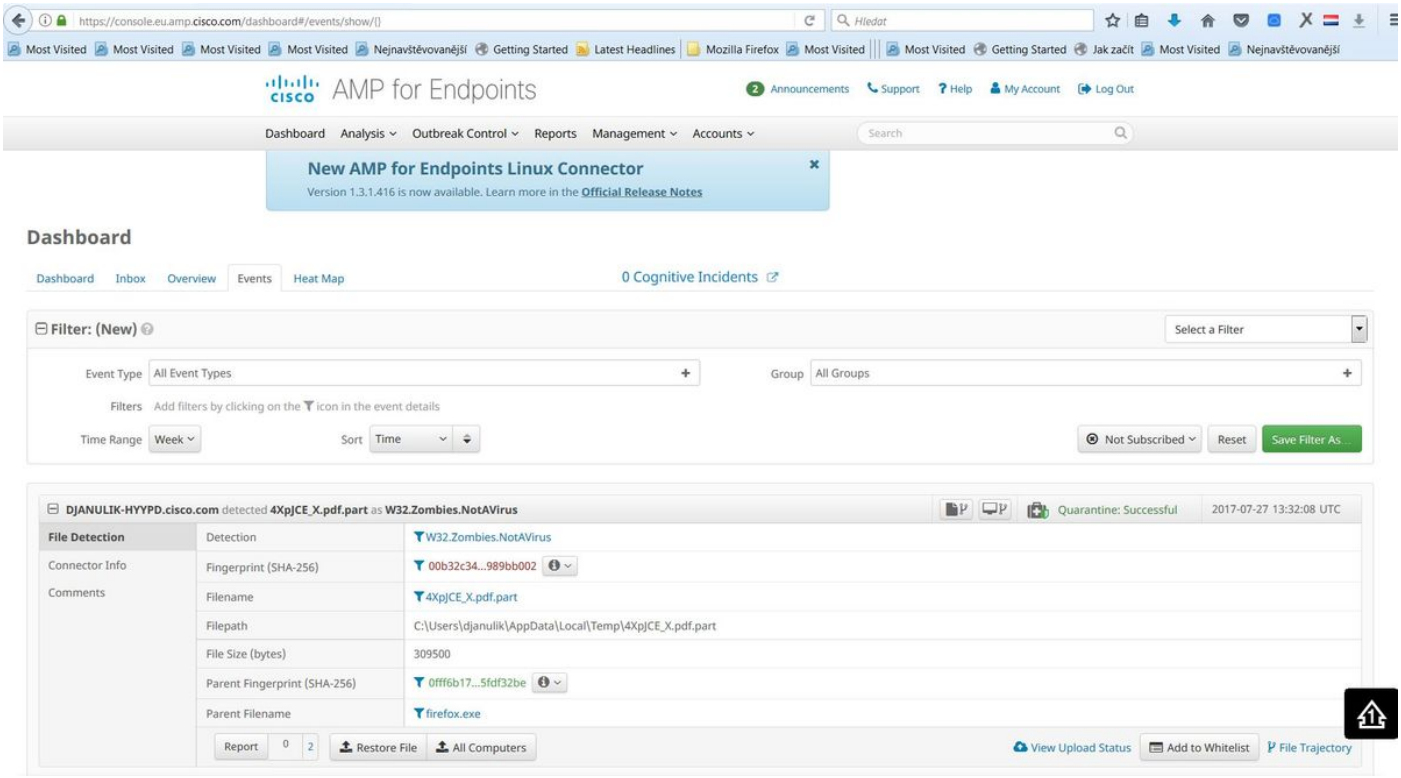
步骤 9：部署摘要

此页显示成功和失败的FireAMP连接器安装列表以及当前正在安装的连接器。可以转到管理**>部署摘要**。



步骤 10：线程检测验证

僵尸.pdf触发隔离事件，发送到AMP控制面板。



隔离事件

其他信息

要获得AMP帐户，您可以注册ATS大学。这为您概述了实验室中的AMP功能。

相关信息

- 配置AMP启用程序
- 技术支持和文档 - Cisco Systems