制作镜像或克隆一台计算机用安装的FireAMP连接器

目录

简介

本文描述进程防止多台计算机尝试使用同样全局唯一标识符(GUID)，在FireAMP网云控制板防止重复的计算机对象出现。此进程在一被克隆的计算机允许FireAMP适当地运作。

作为系统管理员，您可以要包括在您重要的Windows PC镜像的FireAMP连接器。FireAMP，然而，要求系统可以独特识别。克隆的一计算机一般步骤Linux的在此条款的底部。

> **注意**：说明第一组适用于FireAMP版本4.1.4或以上。 进一步您查找机器运行更早版本的原始步骤。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

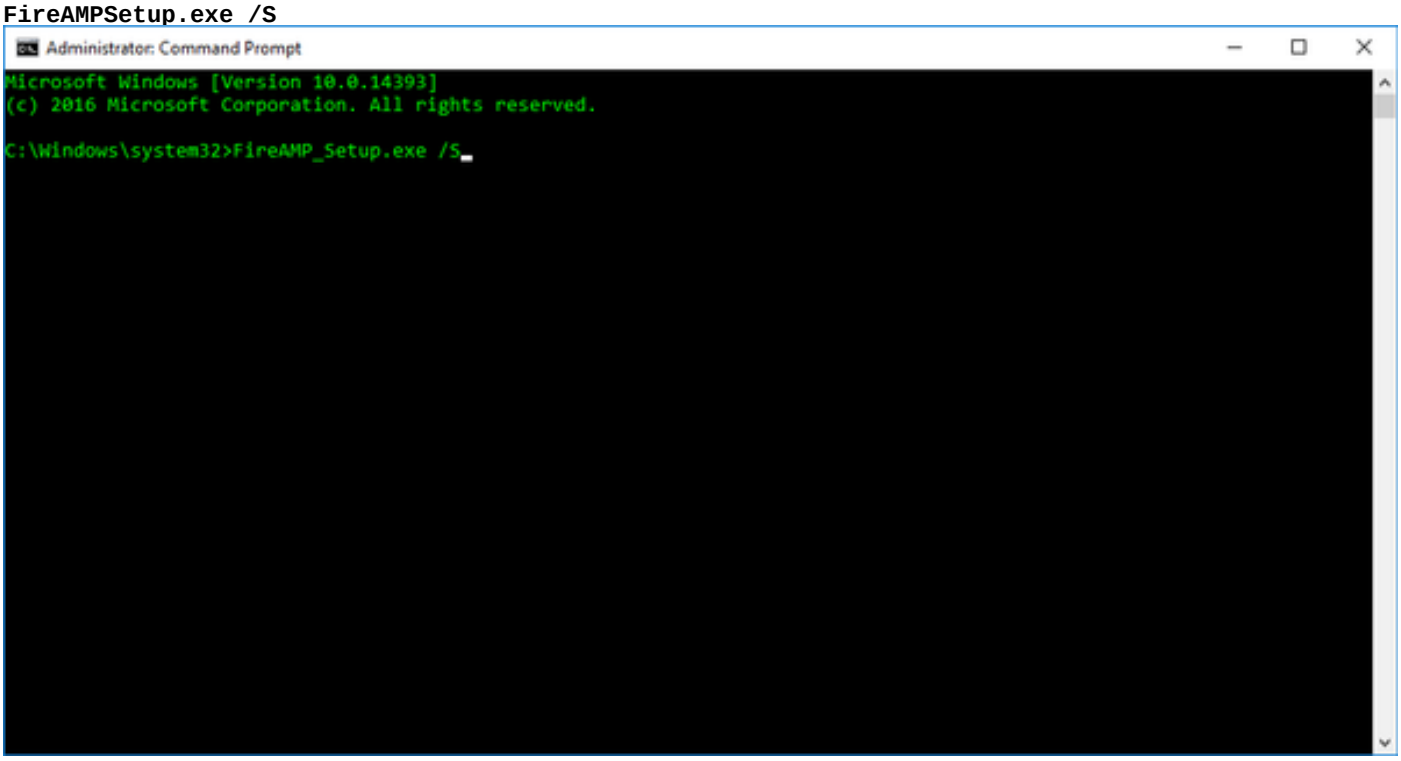
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

装配前准备工作-版本4.1.4和以上

执行这些步骤准备制作镜像的一台计算机：

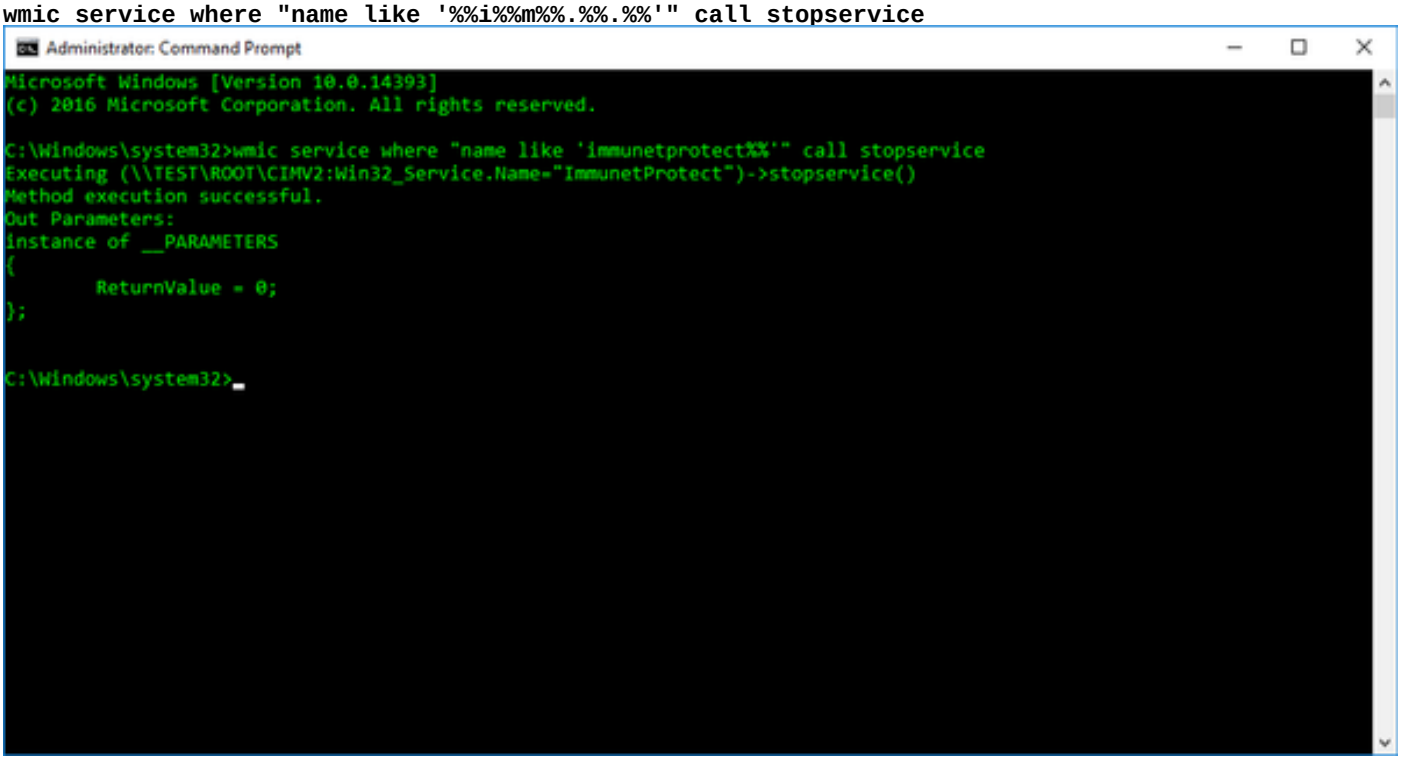
步骤1.在您的主图象的安装FireAMP。

```
FireAMPSetup.exe /S
```



步骤2.终止FireAMP服务。

```
wmic service where "name like '%%i%%m%%.%%.%%'" call stopservice
```



请使用以下命令是否安排连接器保护启用。密码将是可视在prompt命令。

```
4.2 and Lower: Not Available
4.3 to 5.0: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\sfc.exe" -k protectionpassword
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\sfc.exe" -k protectionpassword
```

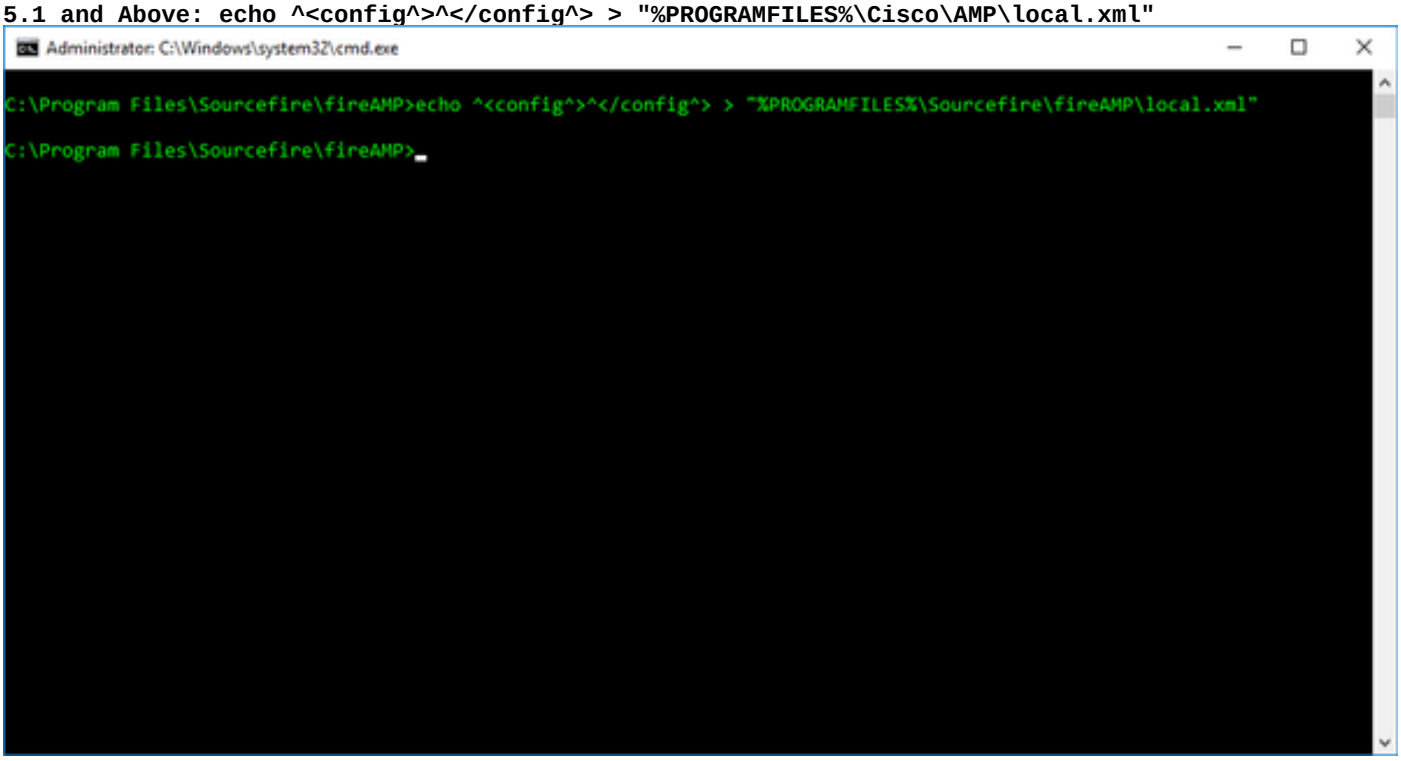
注意：如果FireAMP服务再开始，主图象重新生成**local.xml。您**需要重复这些步骤再中立化主图象。请务必包括这些步骤在您的主图象准备进程。

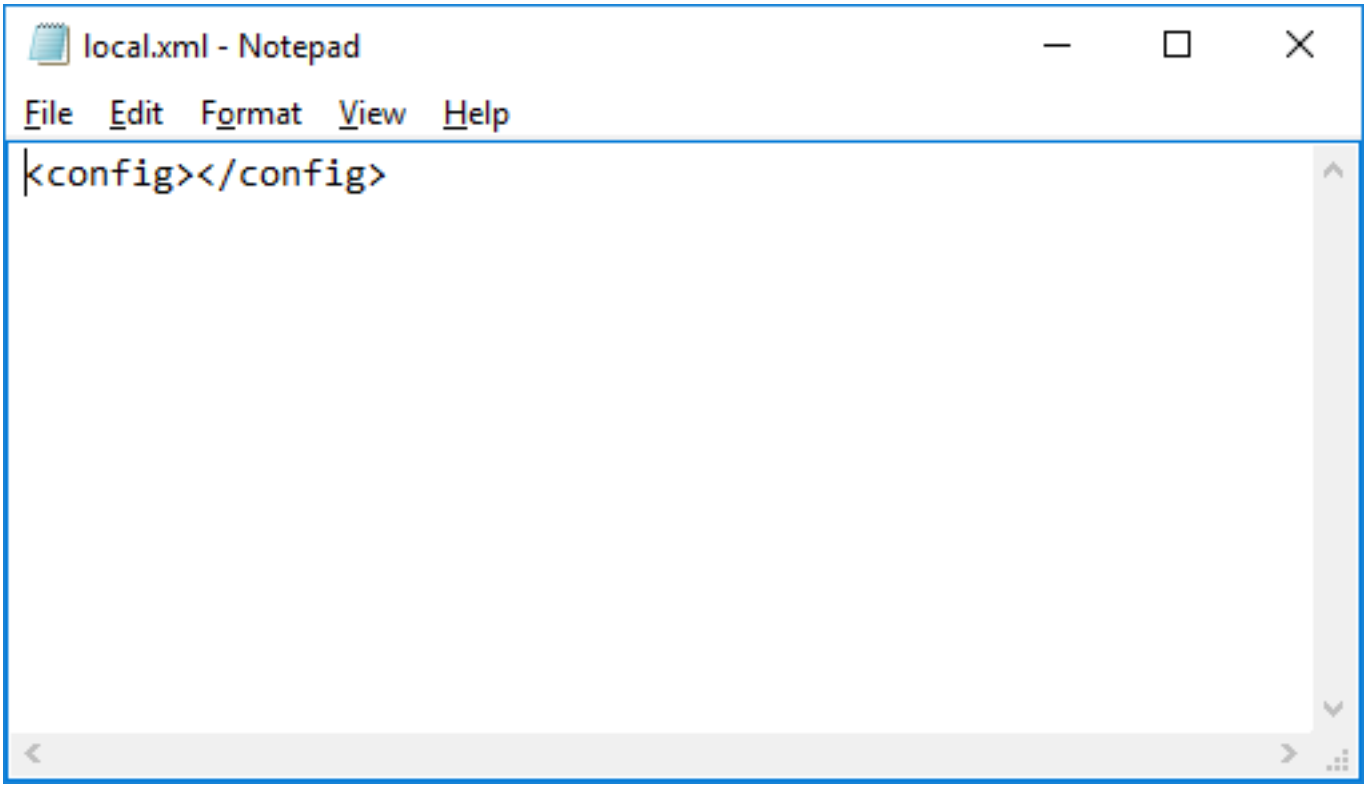
步骤3.删除**local.xml**

```
5.0 and Lower: del "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
5.1 and Above: del "%PROGRAMFILES%\Cisco\AMP\local.xml"
```

步骤4.创建空白**local.xml**。

```
5.0 and Lower: echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
5.1 and Above: echo ^<config^>^</config^> > "%PROGRAMFILES%\Cisco\AMP\local.xml"
```





安装后-版本4.1.4和以上

FireAMP 4.1.4和更加高自动地生成一个新的regisration和通用唯一标识符(UUID)，当连接器服务检

测空白`local.xml`。没有其他步骤在计算机不需要被执行。

> **注意**：预计向空白`local.xml`被放置到您的组织的默认组的机器。您必须决定您是否要手工移动这些机器或更改您的默认组是那些机器的希望的组。

这时FireAMP客户端应该是正在运行的。您能使用用户界面验证连接，并且服务运行的那。如果您的用户界面没有设置开始，可以手工开始与这些命令。请务必当前更新您的安装的版本的版本号。

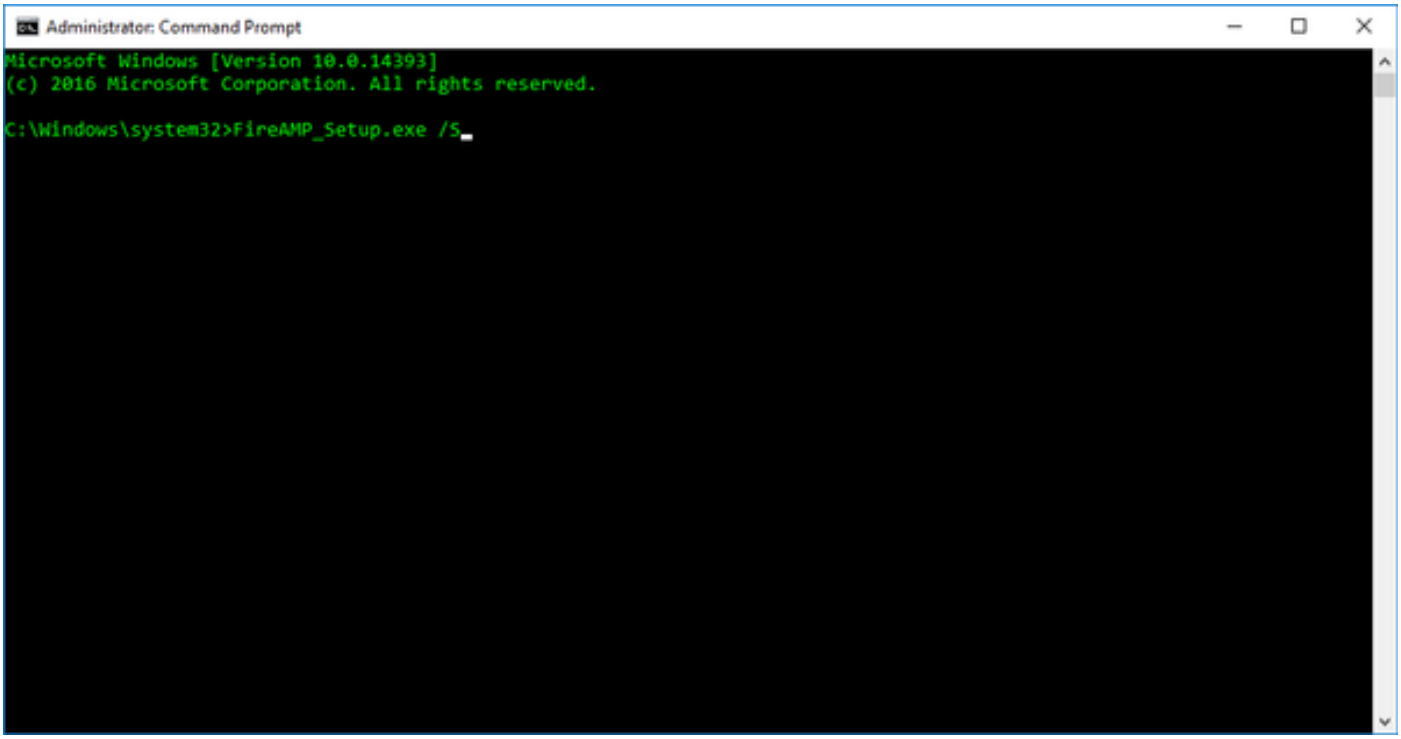
```
5.0 and Lower: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\iptray.exe" -f
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\iptray.exe" -f
```

装配前准备工作-版本比4.1降低

执行这些步骤准备制作镜像的一台计算机：

步骤1.在您的主图象的安装FireAMP。

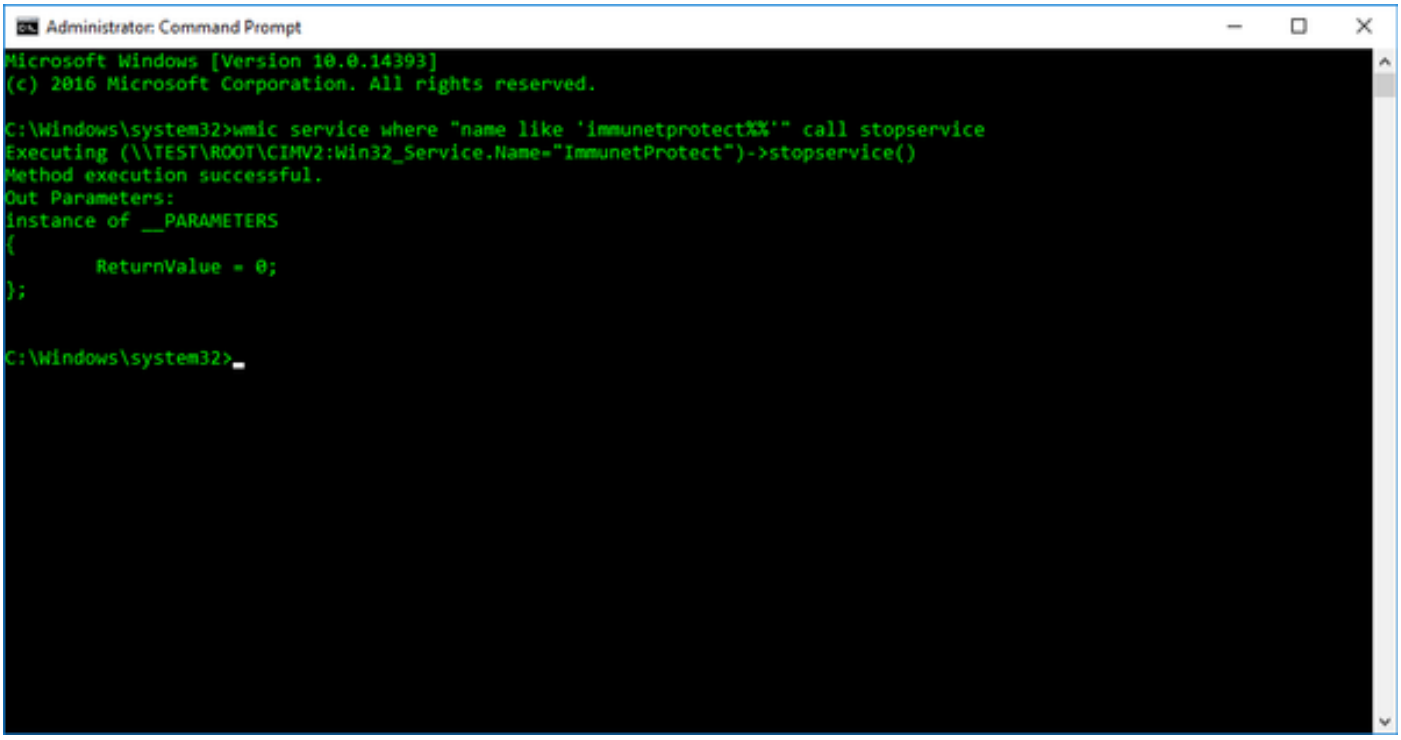
```
FireAMPSetup.exe /S
```



步骤2.终止FireAMP服务。

注意：如果使用一个连接器保护密码，这需要从用户界面执行。

```
wmic service where "name like '%%i%%m%%.%%.%%'" call stopservice
```



步骤3.确定fireAMP产品的位置。默认是

```
%PROGRAMFILES%\Sourcefire\fireAMP
```

步骤4.通过运行`sfc.exe`卸载从控制面板的FireAMP连接器服务-版本文件夹的`u`。请务必当前更新命令用您的安装的版本编号。

```
“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -u
```

第五步：如果要重新使用现有计算机对象，您必须备份现有**local.xml**。在此目录local.xmlis ：

```
%PROGRAMFILES%\Sourcefire\fireAMP\
```

> **注意**：这对单个重新镜像是理想的，但是可能不是实用的为一对多的想象实践，因为存储唯一信息，例如单个的计算机的GUID。

第六步：在您备份**local.xml**如果不需要重新使用在您的控制板的计算机对象，删除local.xml

```
del local.xml
```

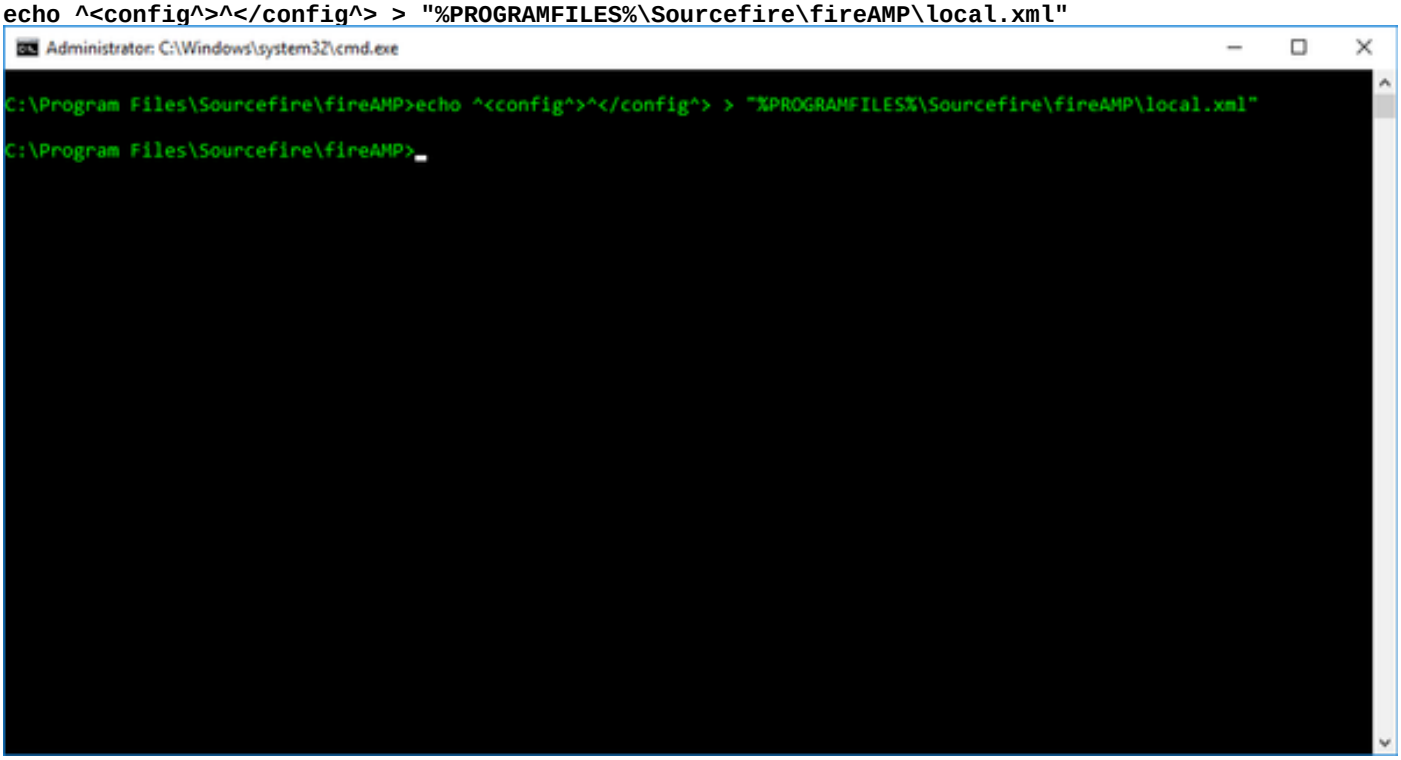
安装后-版本比4.1降低

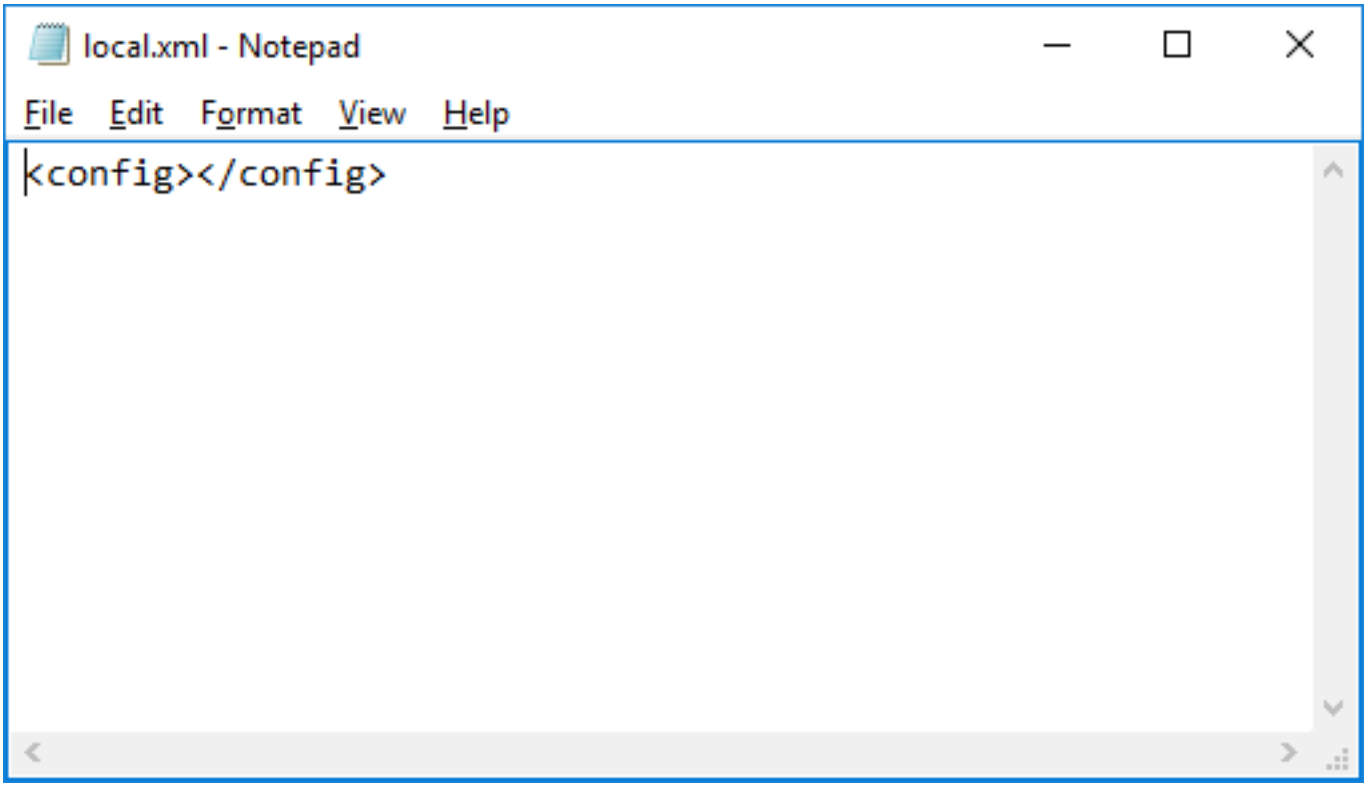
在部署您的镜像以后执行这些步骤：

> **注意**：如果开始FireAMP服务用通用的**local.xml**，创建一个新的计算机对象。如果有原始local.xmlfile您能每台计算机恢复他们安排对象被重新使用。

步骤1.，如果在重新映像之前，返回了它请恢复**local.xml**对此目录此时。如果不恢复local.xmlfile您必须仍然创建一通用的一个连接器的能正确地注册。

```
echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
```





步骤2.通过运行**SFC**注册有服务的连接器-从版本文件夹的**r**。此步骤完成计算机的**local.xml**。请务必当前更新下面的命令用您的安装的版本编号。

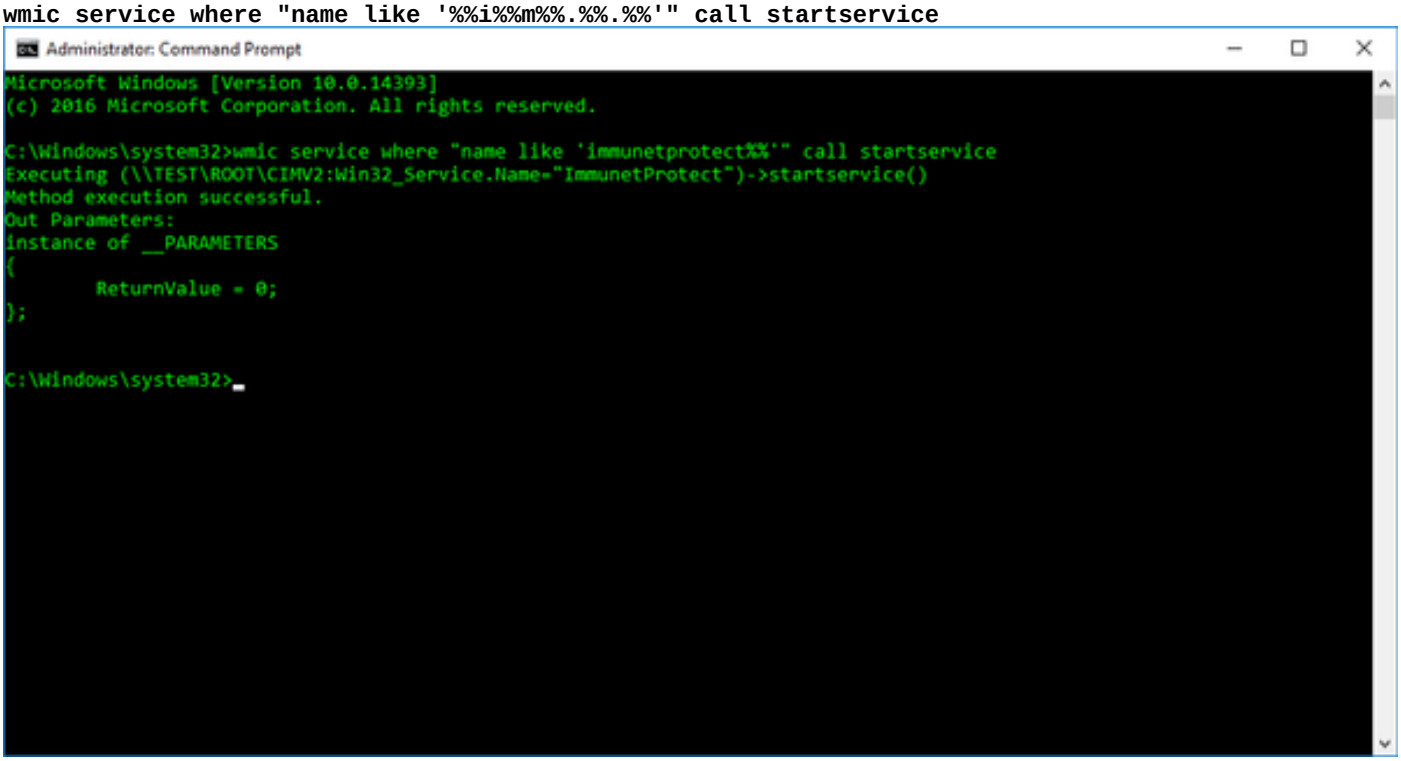
“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -r

安装连接器对服务控制面板通过运行**sfc.exe** -版本文件夹的**i**。

“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -i

通过运行命令启动连接器：

wmic service where "name like '%%i%%m%%.%%.%%'" call startservice



注意：预计这样手工注册的机器被放置到您的组织的默认组。您必须决定您是否要手工移动这些机器或更改您的默认组是那些机器的希望的组。

这时FireAMP客户端应该是正在运行的。您能使用用户界面验证连接，并且服务运行的那。如果您的用户界面没有设置开始，可以用下面的命令手工开始。请务必当前更新您的安装的版本号。

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\iptray.exe" -f
```

Linux

克隆的一计算机一般步骤Linux的和有一新的标识类似于Windows。这是步骤和命令：

在您的主图象的安装安培

```
$ (sudo) yum install filename.rpm
```

终止安培服务

```
$ (sudo) initctl stop cisco-amp
```

删除local.xml

```
$ (sudo) rm /opt/cisco/amp/etc/local.xml
```

当一不同的计算机启动与被克隆的镜像，安培服务将自动地开始并且生成一新的标识。它在一组中一定是唯一在所有通信的连接器间网云[whether public， or private]的。