

A imagem ou clona um computador com o conector de FireAMP instalado

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Instalação provisória - Versões 4.1.4 e mais recente](#)

[A Cargo-instalação - Versões 4.1.4 e mais recente](#)

[Instalação provisória - As versões abaixam do que 4.1](#)

[A Cargo-instalação - As versões abaixam do que 4.1](#)

Introdução

Este documento descreve os processos para impedir computadores múltiplos para tentar globalmente o uso de mesmos - o identificador exclusivo (GUID), que impede objetos duplicados do computador para aparecer no painel da nuvem de FireAMP. Este processo permite que FireAMP trabalhe corretamente em uma máquina clonada.

Como um administrador de sistema, você pode querer incluir o conector de FireAMP em suas imagens mestras do PC Windows. FireAMP, contudo, exige que os sistemas podem excepcionalmente ser identificados. As etapas gerais para clonar uma máquina para Linux estão na parte inferior deste artigo.

Note: O primeiro grupo de instruções aplica-se à versão 4.1.4 ou mais recente de FireAMP. Mais você encontra as etapas originais para as máquinas que executam versões anterior.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

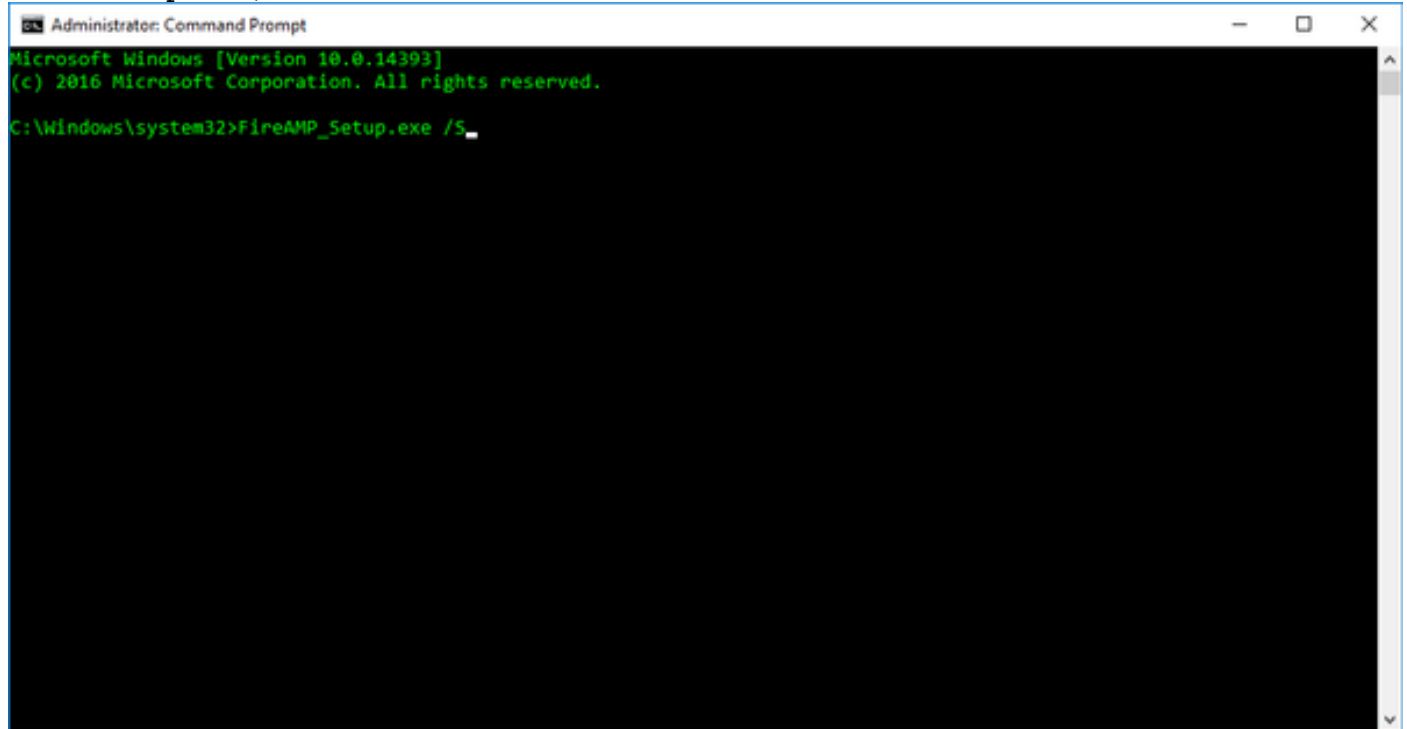
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Instalação provisória - Versões 4.1.4 e mais recente

Execute estas etapas para preparar um computador para a imagem latente:

Etapa 1. Instale FireAMP em sua imagem mestra.

FireAMPSetup.exe /S

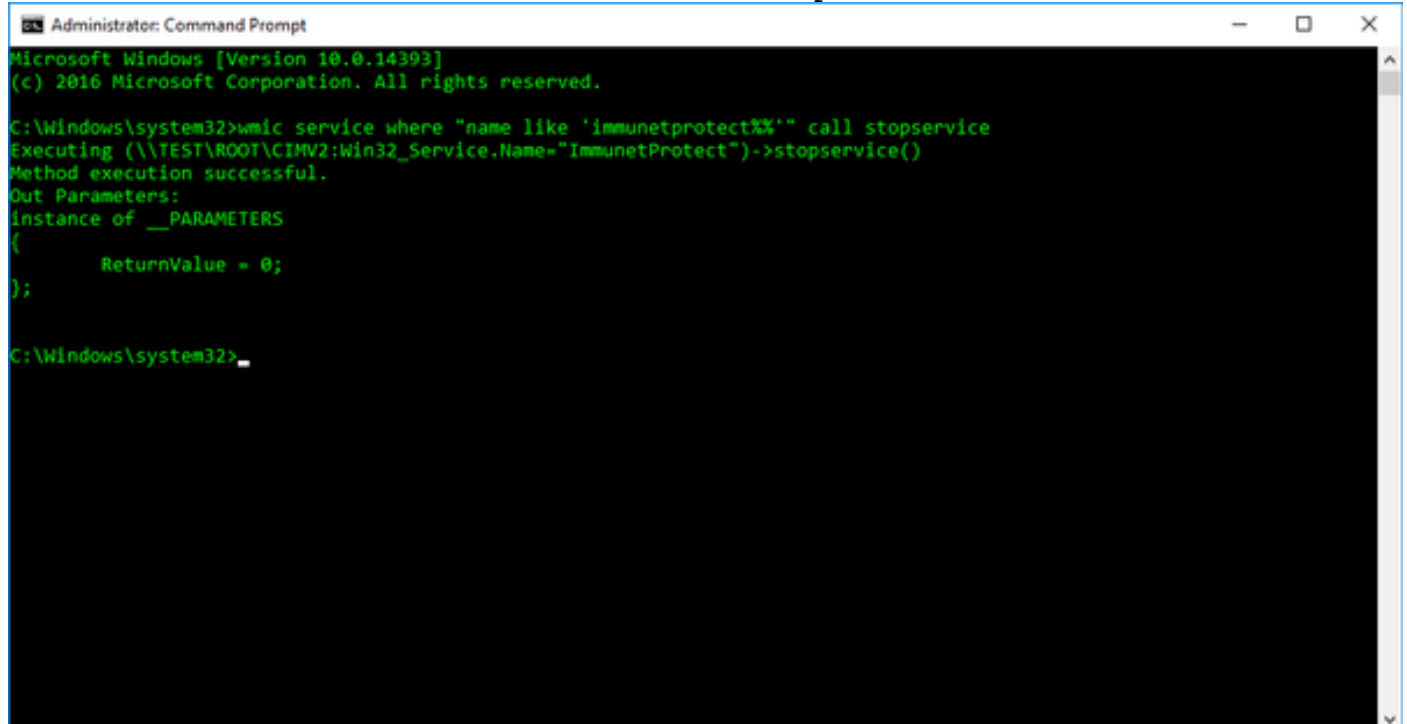


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>FireAMP_Setup.exe /S_
```

Etapa 2. Pare o serviço de FireAMP.

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic service where "name like 'immunetprotect%'" call stopservice
Executing (\\TEST\ROOT\CIMV2:Win32_Service.Name="ImmunetProtect")->stopservice()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};

C:\Windows\system32>_
```

Use o comando seguinte se você tem a proteção do conector permitida. A senha será visível no comando prompt.

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

Note: Se o serviço de FireAMP é começado outra vez, a imagem mestra regenera **local.xml**. **Você** precisa de repetir estas etapas para neutralizar outra vez a imagem mestra. Seja certo incluir estas etapas em seu processo da preparação da imagem mestra.

Etapa 3. Supressão **local.xml**.

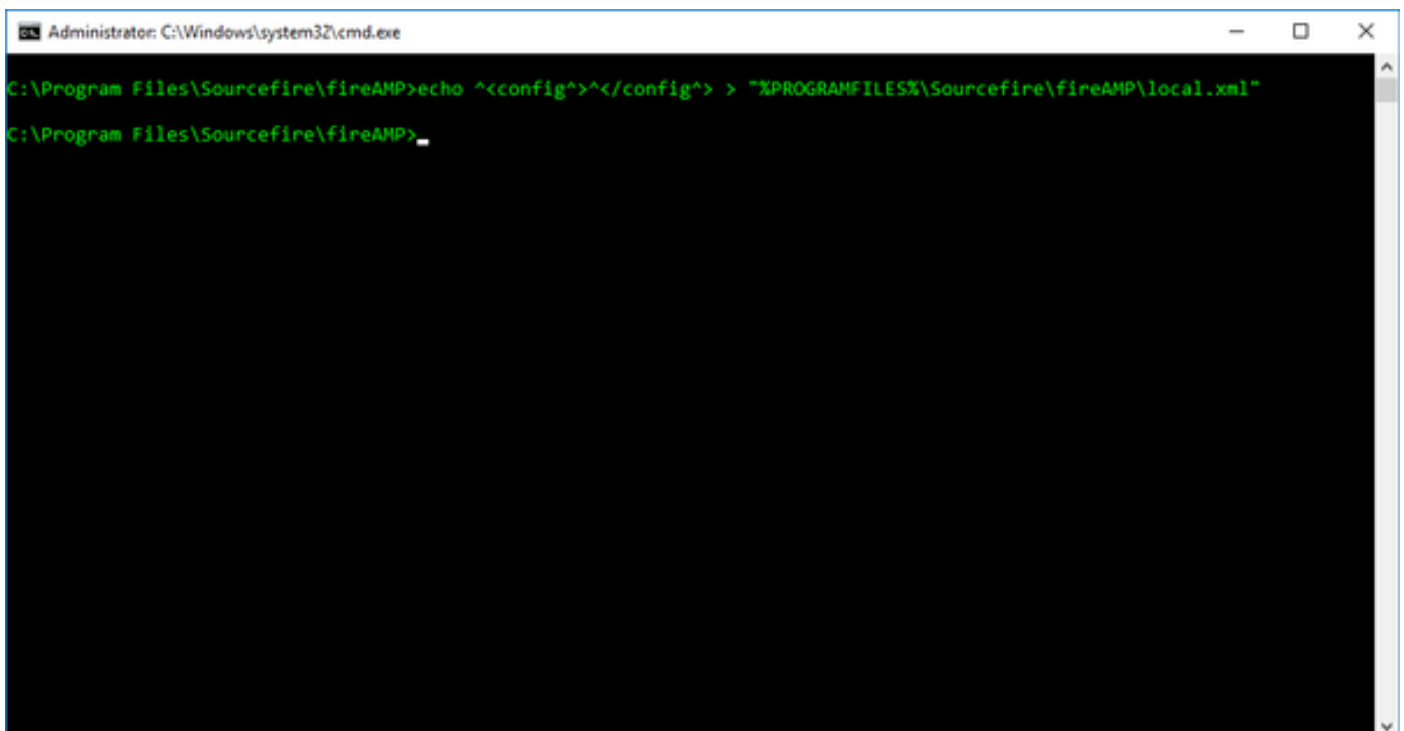
5.0 and Lower: del "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"

5.1 and Above: del "%PROGRAMFILES%\Cisco\AMP\local.xml"

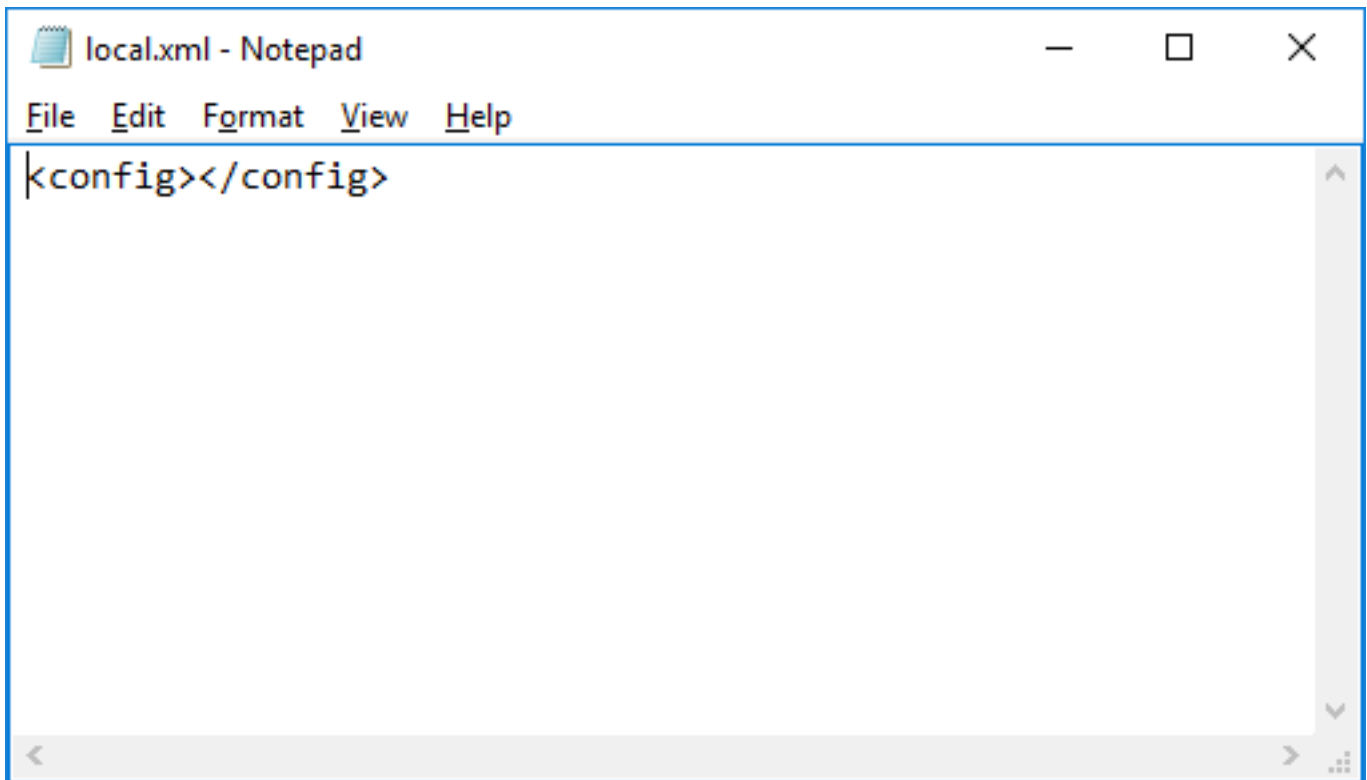
Etapa 4. Crie um arquivo vazio **local.xml**.

5.0 and Lower: echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"

5.1 and Above: echo ^<config^>^</config^> > "%PROGRAMFILES%\Cisco\AMP\local.xml"



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The prompt is at "C:\Program Files\Sourcefire\fireAMP>". The user has entered the command: `echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"`. The command has been executed, and the prompt is now at "C:\Program Files\Sourcefire\fireAMP>".



A Cargo-instalação - Versões 4.1.4 e mais recente

FireAMP 4.1.4 e mais alto gerencie automaticamente um registration novo e um identificador exclusivo universal (UUID) quando o serviço do conector detecta um **arquivo** vazio **local.xml**. Não mais etapa precisa de ser executada na máquina própria.

Note: Espera-se que as máquinas que se registram com um **arquivo** vazio **local.xml** é colocado no grupo padrão das suas organizações. Você deve decidir se você quer mover manualmente estas máquinas ou mudar seu grupo padrão para ser o grupo desejado para aquelas máquinas.

Neste momento o cliente de FireAMP deve ser em serviço. Você pode usar a interface do utilizador para verificar a Conectividade e que o serviço está sendo executado. Se sua interface do utilizador não é ajustada para começar, pode manualmente ser começada com estes comando. Seja certo atualizar atualmente o número de versão para sua versão instalada.

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



Instalação provisória - As versões abaixo do que 4.1

Execute estas etapas para preparar um computador para a imagem latente:

Etapa 1. Instale FireAMP em sua imagem mestra.

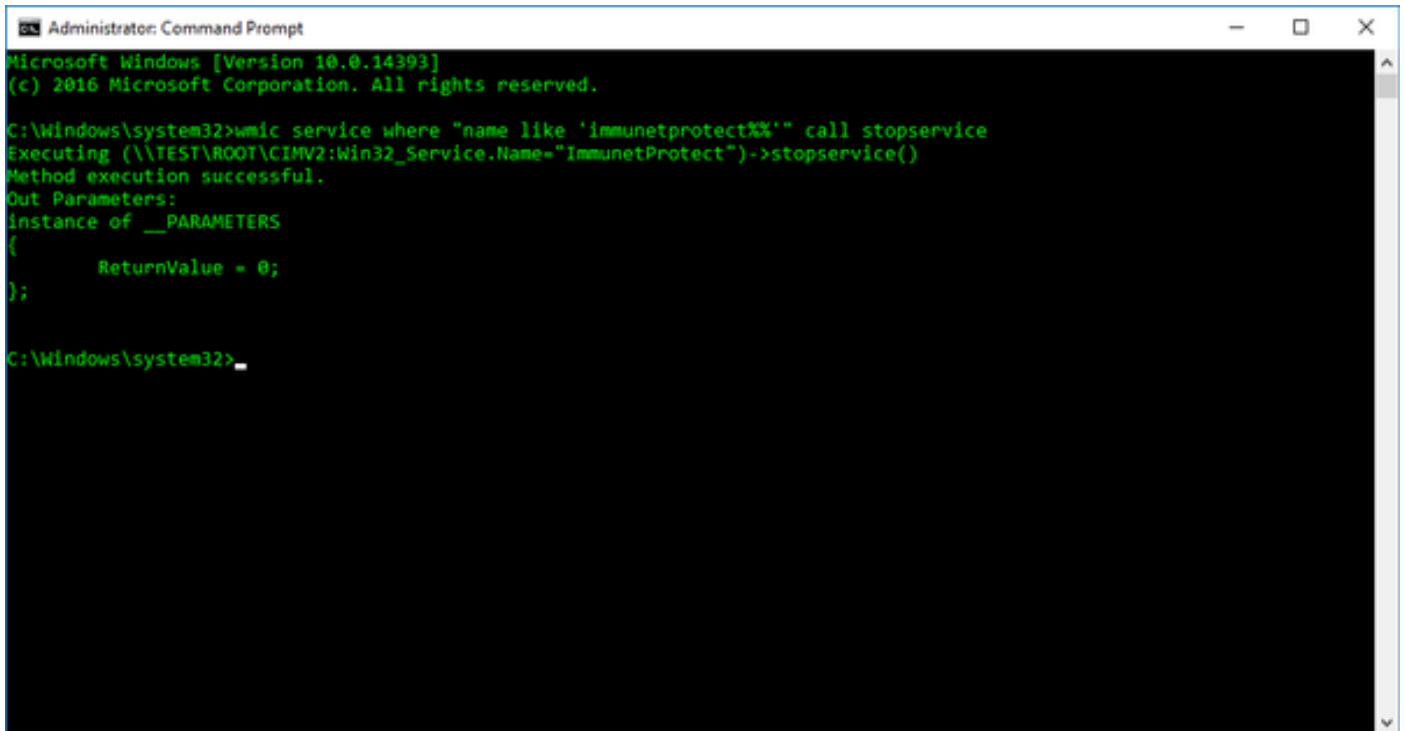
```
FireAMPSetup.exe /S
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Windows\system32>FireAMP_Setup.exe /S_
```

Etapa 2. Pare o serviço de FireAMP.

Note: Se você usa uma senha da proteção do conector, esta precisa de ser feita da

interface do utilizador.

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic service where "name like 'immunetprotect%'> call stopservice
Executing (\\TEST\ROOT\CIMV2:Win32_Service.Name="ImmunetProtect")->stopservice()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
(
    ReturnValue = 0;
);

C:\Windows\system32>
```

Etapa 3. Determine o lugar do produto do fireAMP. O padrão é

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

Etapa 4. Desinstale o serviço do conector de FireAMP do Control Panel executando `sfc.exe -u` do dobrador da versão. Seja certo atualizar atualmente o comando com seu número de versão instalada.

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

Etapa 5. Se você quer reutilizar o objeto existente do computador, você deve backup o **arquivo** existente `local.xml`. O `local.xml`is **encontrado** neste diretório:

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

Note: Isto é ideal para a nova imagem individual mas não pode ser prático para um-à-muitas práticas da imagem latente como armazena a informação exclusiva, tal como o GUID de um único computador.

Etapa 6. Depois que você suporta `local.xml` ou se você não precisa de reutilizar o objeto do computador em seu painel, a supressão `local.xml`, **segundo as indicações** da imagem:

```
del local.xml
```

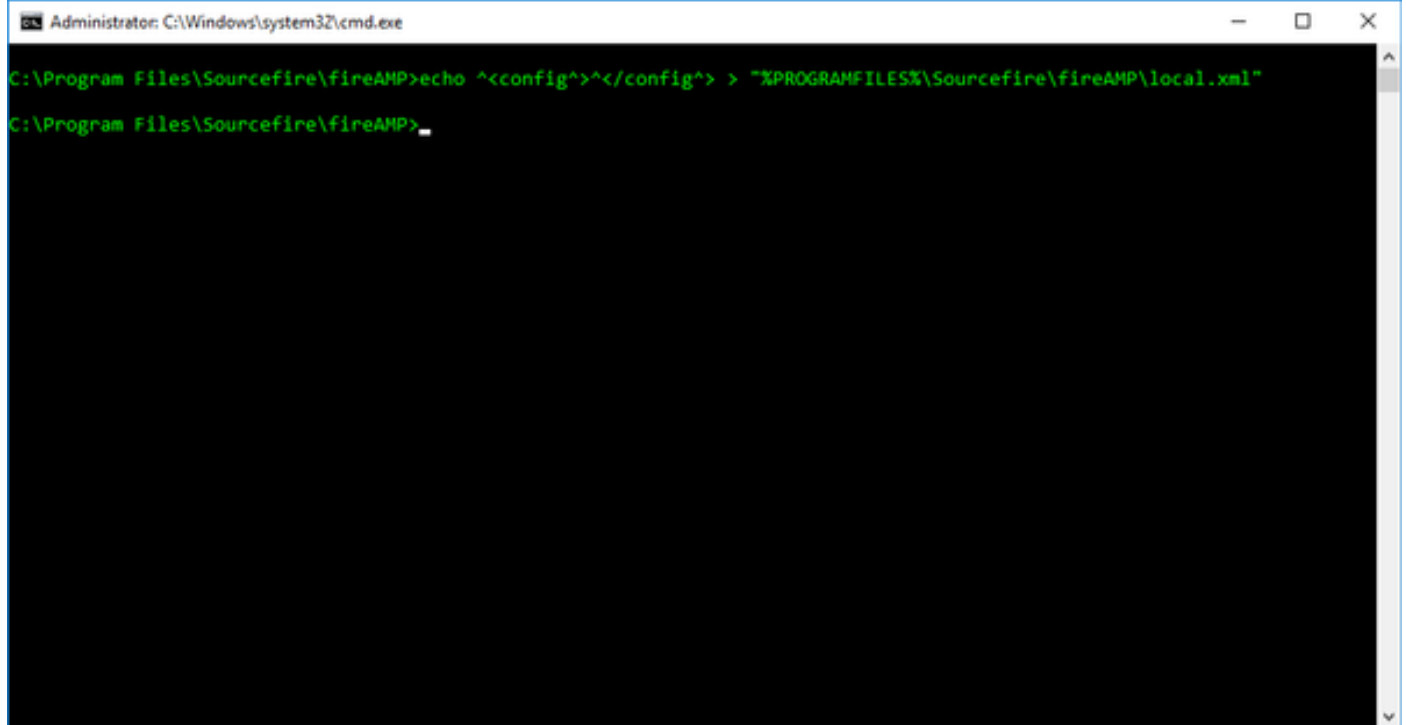
A Cargo-instalação - As versões abaixo do que 4.1

Execute estas etapas após ter distribuído sua imagem:

Note: Se você começa o serviço de FireAMP com o **arquivo** genérico `local.xml`, cria um objeto novo do computador. Se você tem o `local.xmlfile` original, você pode restaurá-lo pelo computador para ter o objeto reutilizado.

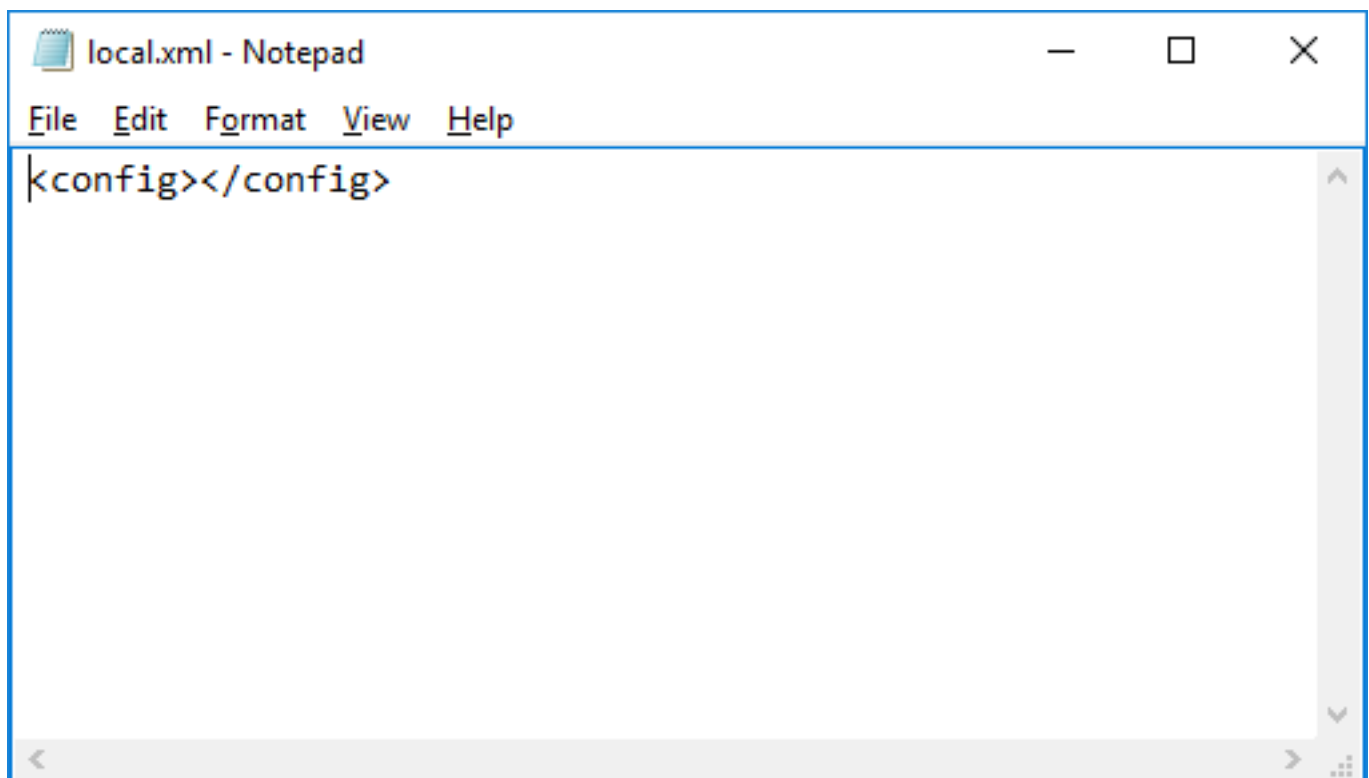
Etapa 1. Restaure o **arquivo** `local.xml` a este diretório neste tempo se você o suportou acima antes de reimaging. Se você não restaura um `local.xmlfile`, você deve ainda criar genérico para que o conector registre-se corretamente.

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



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command prompt displays the following text:

```
C:\Program Files\Sourcefire\fireAMP>echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"  
C:\Program Files\Sourcefire\fireAMP>_
```



The screenshot shows a Notepad window titled "local.xml - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The text area contains the following XML code:

```
<config></config>
```

Etapa 2. Registrar o conector com o serviço executando o `sfc -r` do dobrador da versão. Esta etapa termina o `arquivo local.xml` para um computador. Seja certo atualizar atualmente os comandos abaixo com seu número de versão instalada.

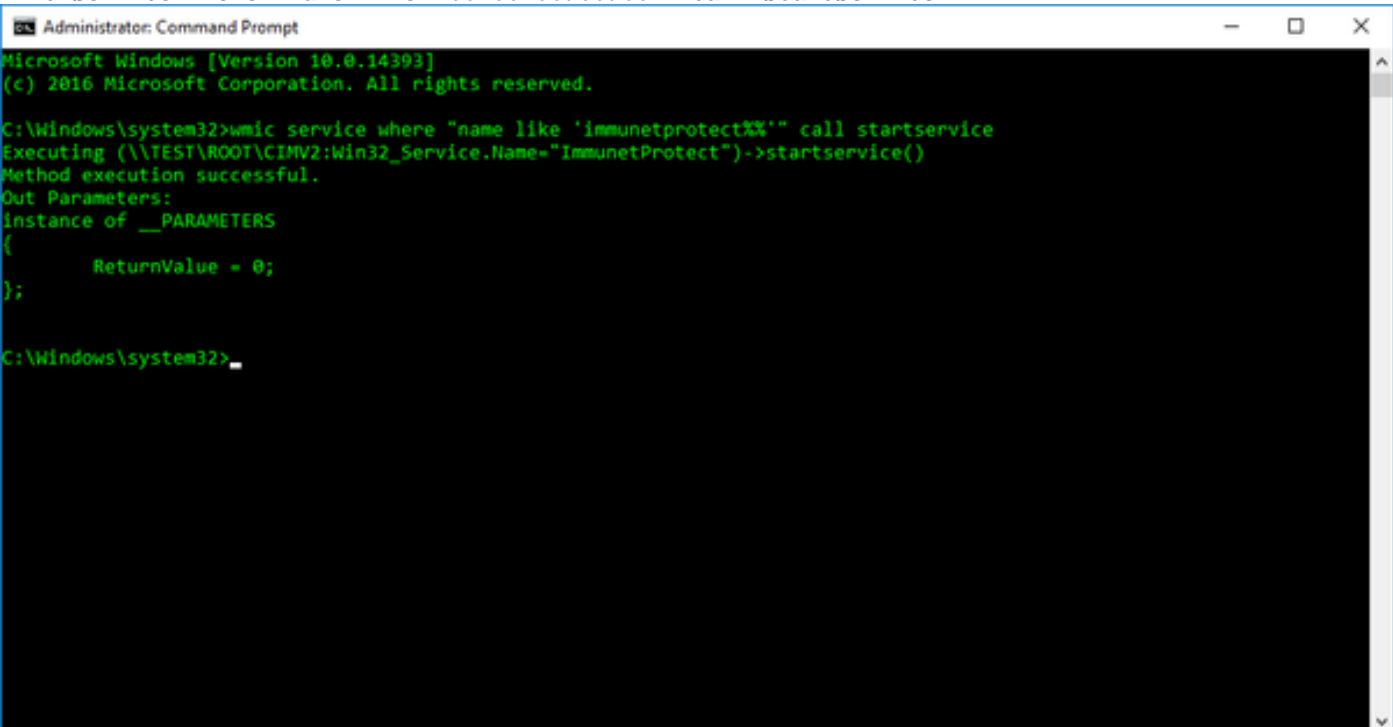
```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe" -r
```

Instale o conector ao Control Panel dos serviços executando `sfc.exe -i` do dobrador da versão.

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe" -i
```

Ligue o conector executando o comando:

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic service where "name like 'immnetprotect%'" call startservice
Executing (\\TEST\ROOT\CIMV2:Win32_Service.Name="ImmnetProtect")->startservice()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};

C:\Windows\system32>
```

Note: Espera-se que as máquinas que são registradas manualmente desta maneira estão colocadas no grupo padrão das suas organizações. Você deve decidir se você quer mover manualmente estas máquinas ou mudar seu grupo padrão para ser o grupo desejado para aquelas máquinas.

Neste momento o cliente de FireAMP deve ser em serviço. Você pode usar a interface do utilizador para verificar a Conectividade e que o serviço está sendo executado. Se sua interface do utilizador não é ajustada para começar, pode manualmente ser começada com o comando abaixo. Seja certo atualizar atualmente o número de versão para sua versão instalada.

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




Linux

As etapas gerais para clonar uma máquina para Linux e têm uma identidade nova são similares a Windows. Estão aqui as etapas e os comandos:

Instale o AMP em sua imagem mestra

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

Pare o serviço AMP

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

Suprima de local.xml

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

Quando as botas diferentes de uma máquina acima com a imagem clonada, o serviço AMP começarão automaticamente acima e gerarão uma identidade nova. Deve ser original através de todos os conectores de comunicação em um grupo no [whether public, or private] da nuvem.