インストール済み FireAMP でコンピュータをイメージングまたはクローニングする

目次

概要

この資料は FireAMP クラウド ダッシュボードに現われるために重複したコンピュータ オブジェクトを防ぐ同じグローバルに固有の 識別子 (GUID) の使用を試みるために複数のコンピューターを防ぐようにプロセスを説明したものです。 このプロセスは FireAMP がクローンとして作られたマシンできちんと動作するようにします。

システム アドミニストレータとして、マスター Windows PC イメージの FireAMP コネクタを含みたいと思う場合もあります。 しかし FireAMP はシステムが識別することができることを必要とします。 Linux のためのマシンをクローンとして作るための一般的なステップはこの技術情報の下部のにあります。

> **注:** 最初に指示の設定 される FireAMP バージョン 4.1.4 または それ 以上に適用します。 更に以前のバージョンを実行するマシンのためのオリジナル ステップを見つけます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

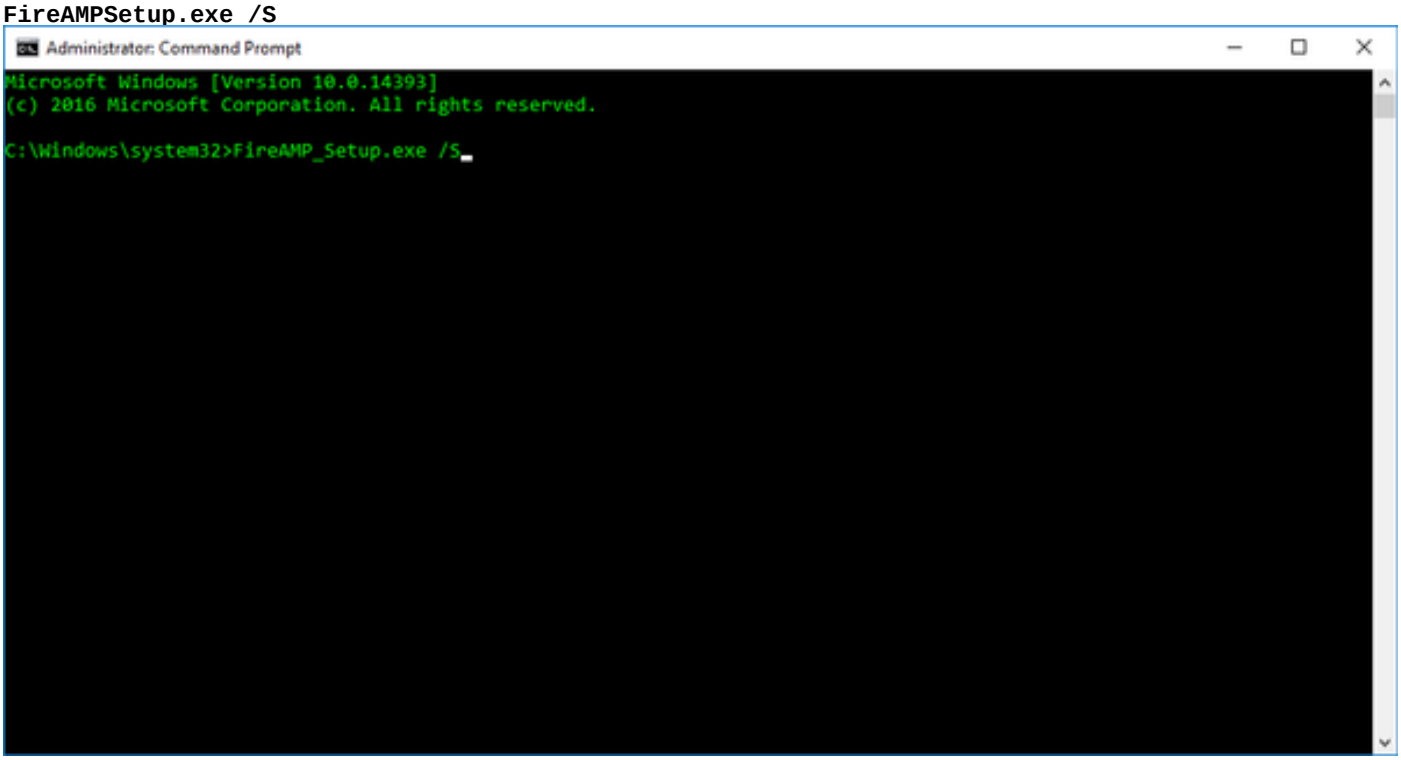
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

プレインストール-バージョン 4.1.4 および それ 以上

イメージングのコンピュータを準備をするためにこれらのステップを実行して下さい:

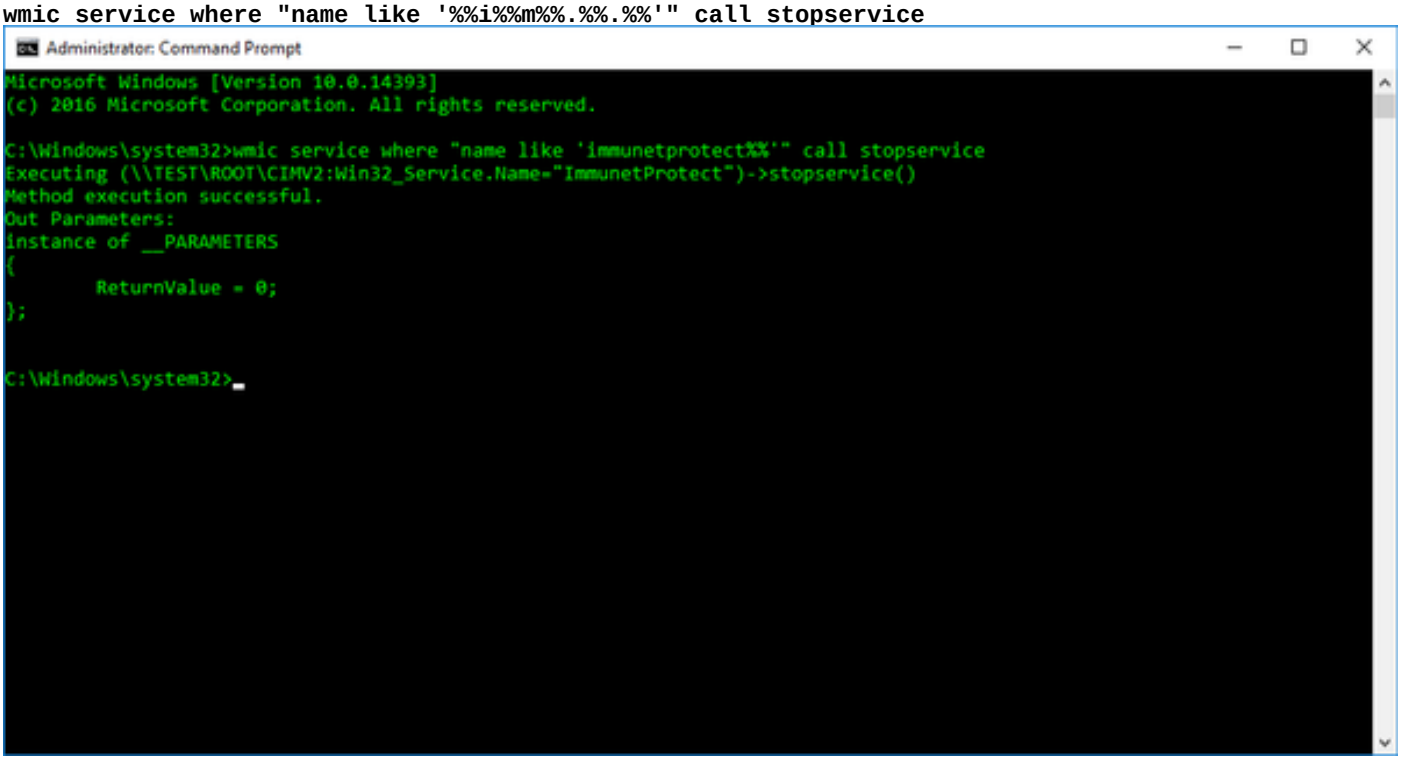
ステップ 1.マスター イメージで FireAMP をインストールして下さい。

```
FireAMPSetup.exe /S
```



ステップ 2. FireAMP サービスを停止して下さい。

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



コネクタ 保護を有効に してもらう場合次のコマンドを使用して下さい。 パスワードはコマンド プロンプトで目に見えます。

```
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
```

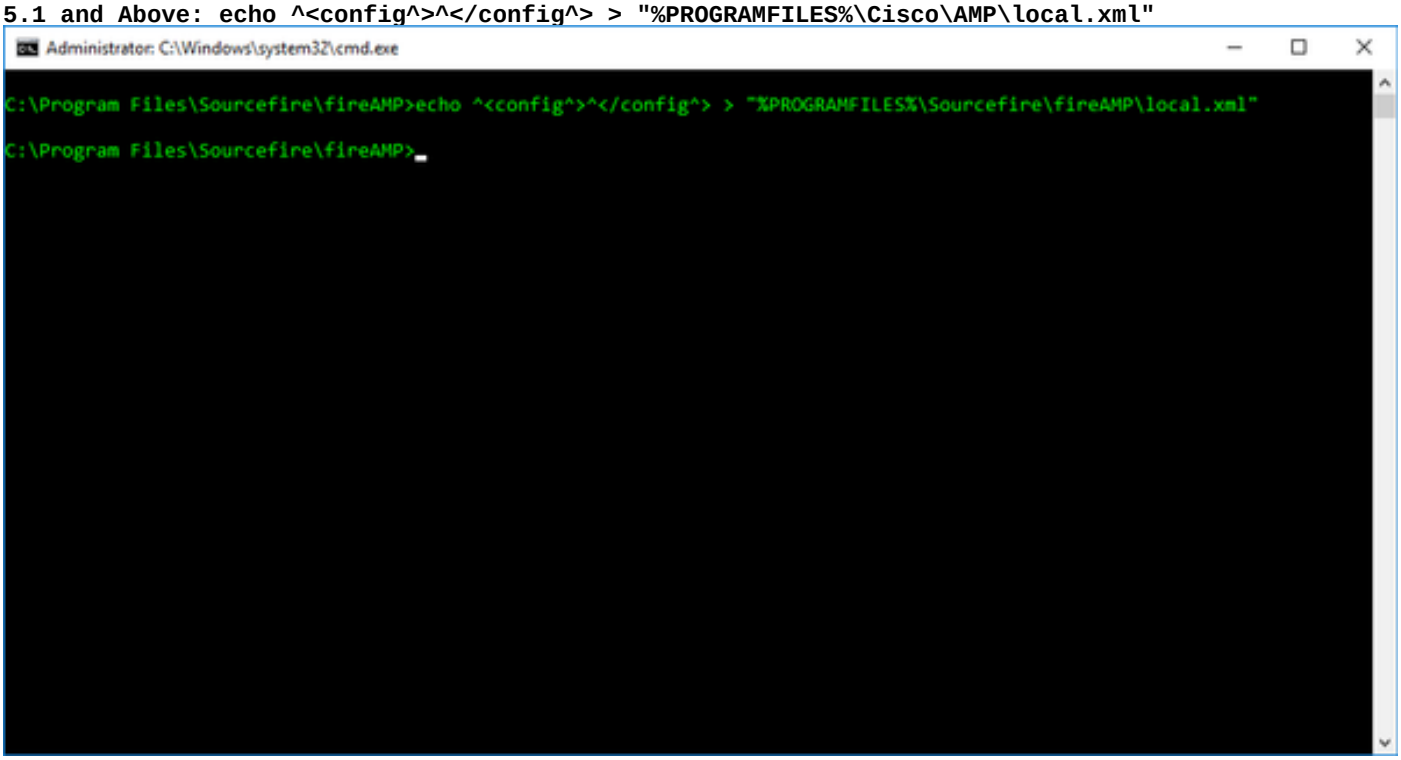
注: FireAMP サービスが再度開始する場合、マスター イメージは local.xml を再生します。マスター イメージを再度中和するためにこれらのステップを繰り返す必要があります。 マスター イメージ準備プロセスにこれらのステップを含めることを忘れないでいて下さい。

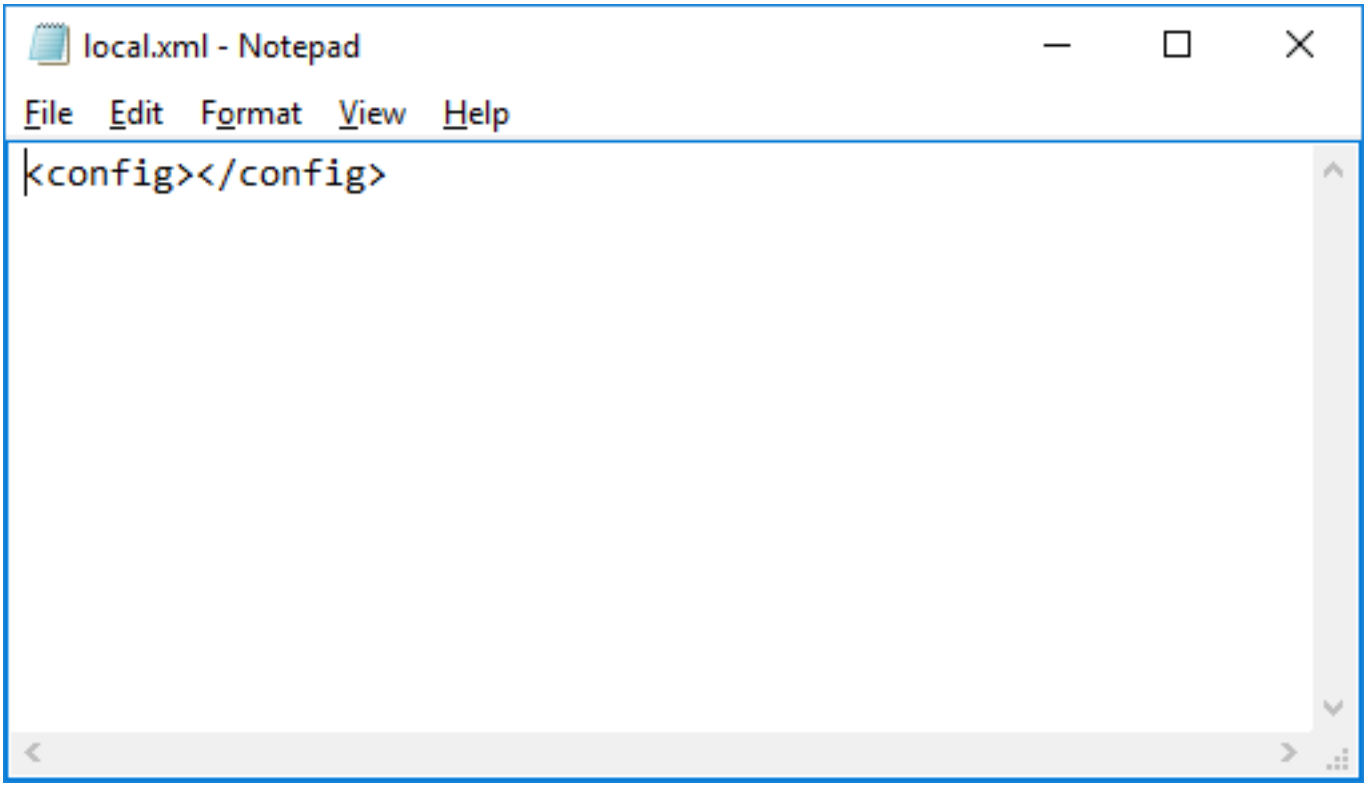
ステップ 3.削除 **local.xml**

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

ステップ 4.ブランク **local.xml** 作成して下さい。

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





インストール後-バージョン 4.1.4 および それ 以上

コネクタ サービスがブランク `local.xml` 検出するとき FireAMP 4.1.4 はおよびより高い自動的に新しい regisration およびユニバーサル固有の識別番号（UUID）を生成します。 これ以上のステップはマシン自体で実行される必要がありません。

> **注:** 組織のデフォルト グループに置かれるブランク `local.xml` と登録するマシンことが期待されます。 これらのマシンを手動で移動するか、またはそれらのマシンのための望ましいグループであるためにデフォルト グループを変更したいと思うかどうか決定して下さい。

この時点で FireAMP クライアントは作動中であるはずです。 サービスが実行されていること接続を確認するのにユーザインターフェイスを使用。 ユーザインターフェイスが開始するために設定 されない場合これらのコマンドで手動で開始することができます。 現在アップデートすることをインストール済み バージョンのためのバージョン番号を忘れないでいて下さい。

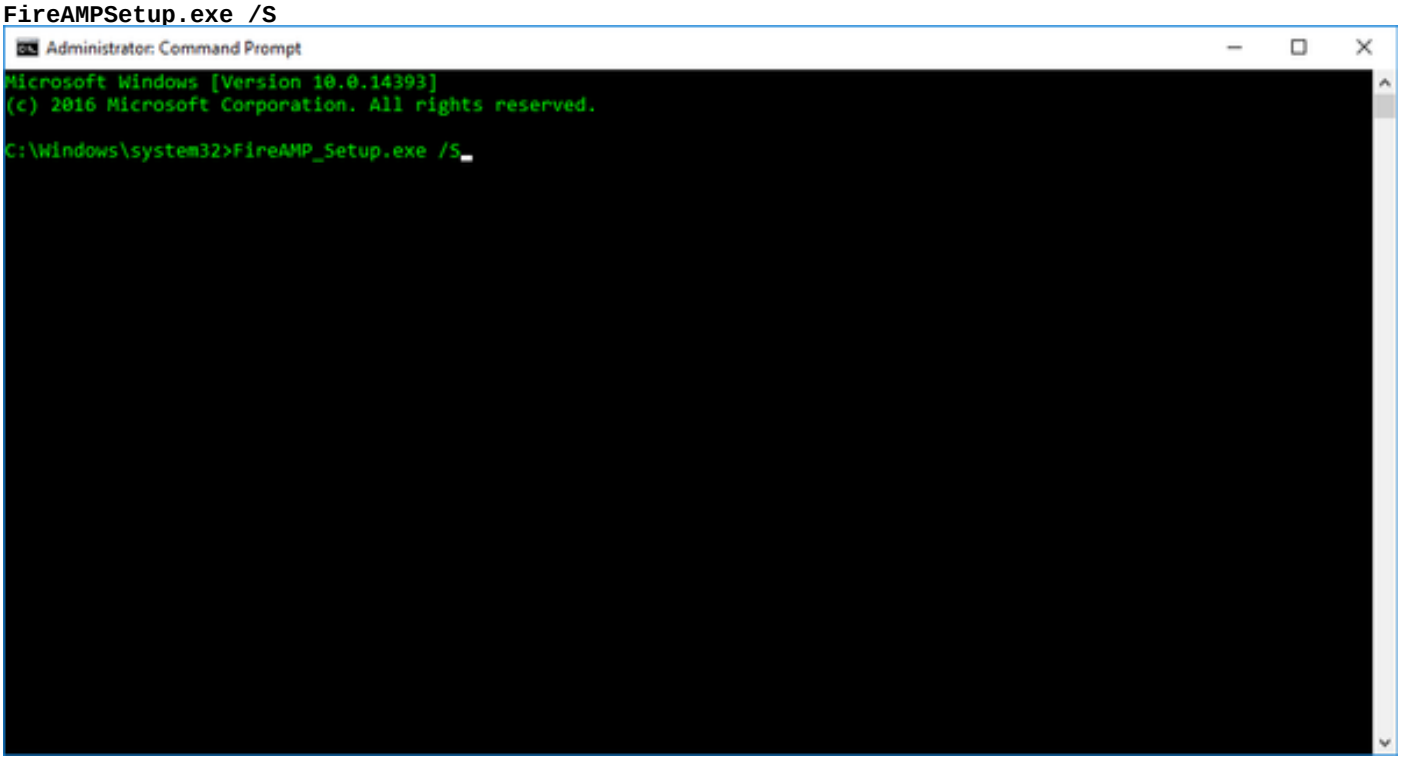
```
5.0 and Lower: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\iptray.exe" -f
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\iptray.exe" -f
```

インストール前-バージョンは 4.1 より下がります

イメージングのコンピュータを準備をするためにこれらのステップを実行して下さい:

ステップ 1.マスター イメージで FireAMP をインストールして下さい。

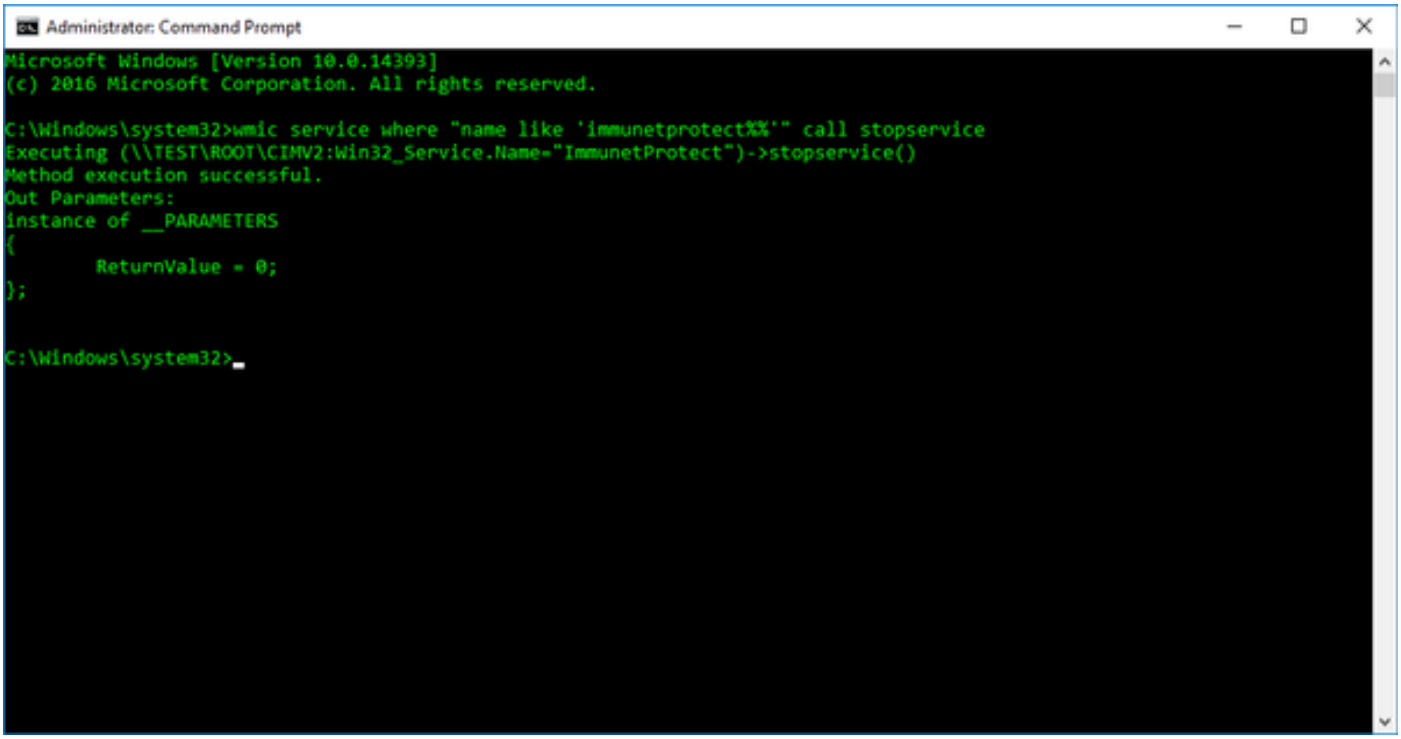
```
FireAMPSetup.exe /S
```



ステップ 2. FireAMP サービスを停止して下さい。

> **注:** コネクタ 保護 パスワードを使用する場合、これはユーザインターフェイスからされる必要があります。

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



ステップ 3. fireAMP 製品の位置を判別して下さい。 デフォルトはあります

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

ステップ 4. **sfc.exe** 実行によってコントロール パネルからの FireAMP コネクタ サービスを-バージョン フォルダ **u** アンインストールして下さい。 現在アップデートすることをインストール済み バージョン数とのコマンドを忘れないでいて下さい。

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

ステップ 5 既存のコンピュータ オブジェクトを再使用したいと思う場合既存の **local.xml** バックアップして下さい。 このディレクトリで local.xmlis:

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

> **注:** これはユーザーにとって理想的イメージ変更しましたりそれとして一対多イメージング推奨事項のために実用的ではないかもしれません保存します単一のコンピューターの GUID のような固有の情報を、ですが。

ステップ 6 **local.xml** バックアップした後ダッシュボードのコンピュータ オブジェクトを、削除 local.xml再使用する必要はなければ:

```
del local.xml
```

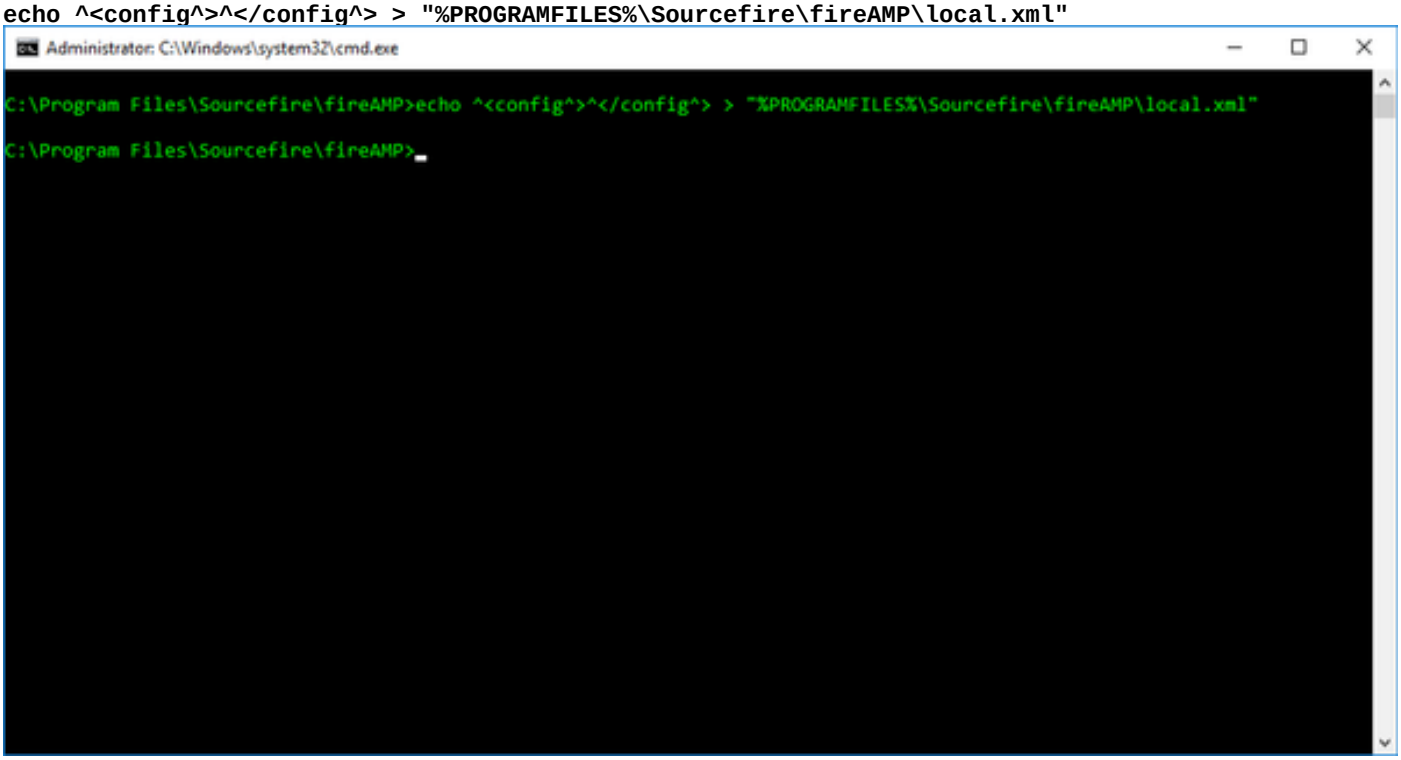
インストール後-バージョンは 4.1 より下がります

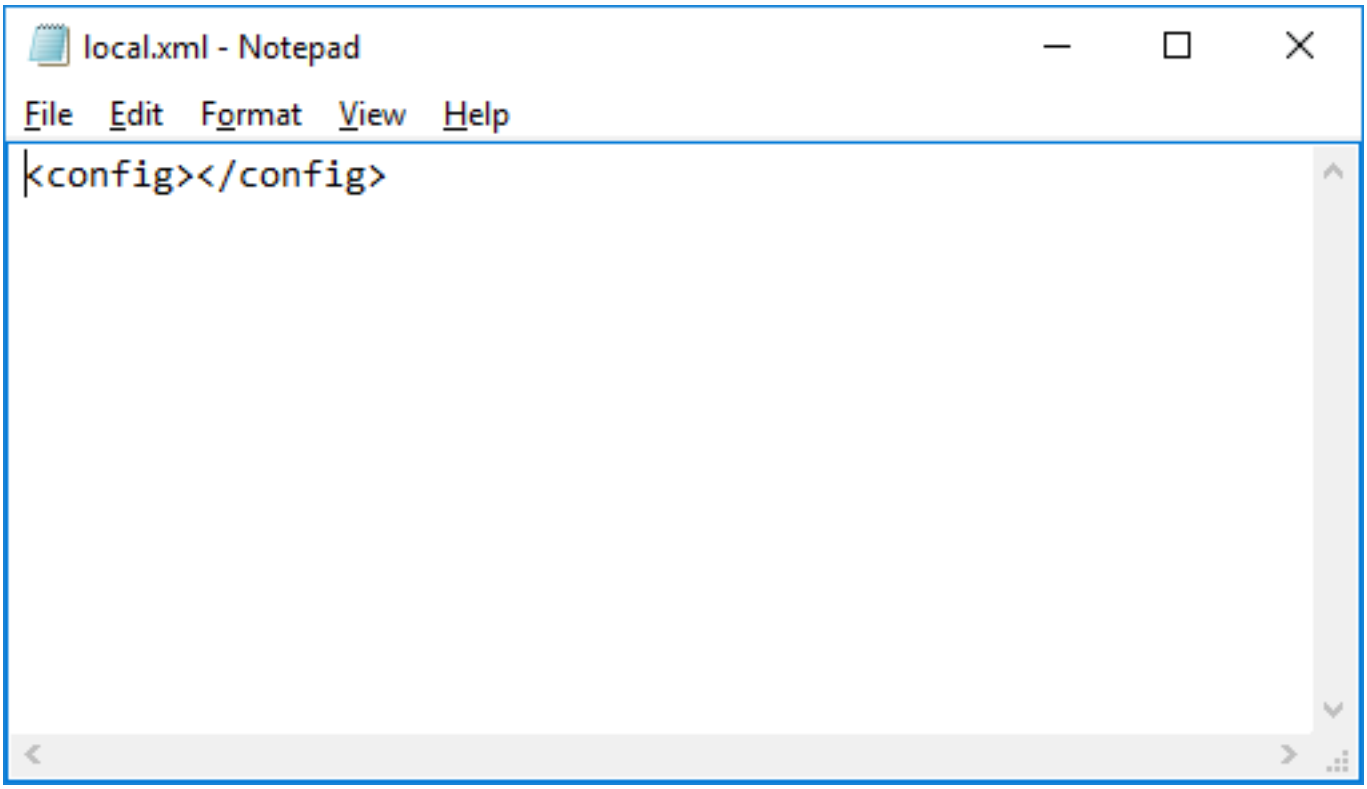
イメージを展開した後これらのステップを実行して下さい:

> **注:** ジェネリック **local.xml** の FireAMP サービスを開始する場合、新しいコンピュータ オブジェクトを作成します。 オリジナル local.xmlfile がある場合コンピュータ 1 台あたりにオブジェクトがあるために再使用されるそれらを復元することができます。

ステップ 1.イメージ変更する前にそれを支持した場合現時点でこのディレクトリに **local.xml** 復元する。 local.xmlfile を復元する場合まだ正しく登録するためにコネクタ用の一般的 な 1 つを作成して下さい。

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





ステップ 2. **SFC** 実行によってサービスのコネクタを-バージョン フォルダからの **r** 登録して下さい。 このステップはコンピュータのための **local.xml** 完了します。 現在アップデートすることをインストール済み バージョン数との下記のコマンドを忘れないでいて下さい。

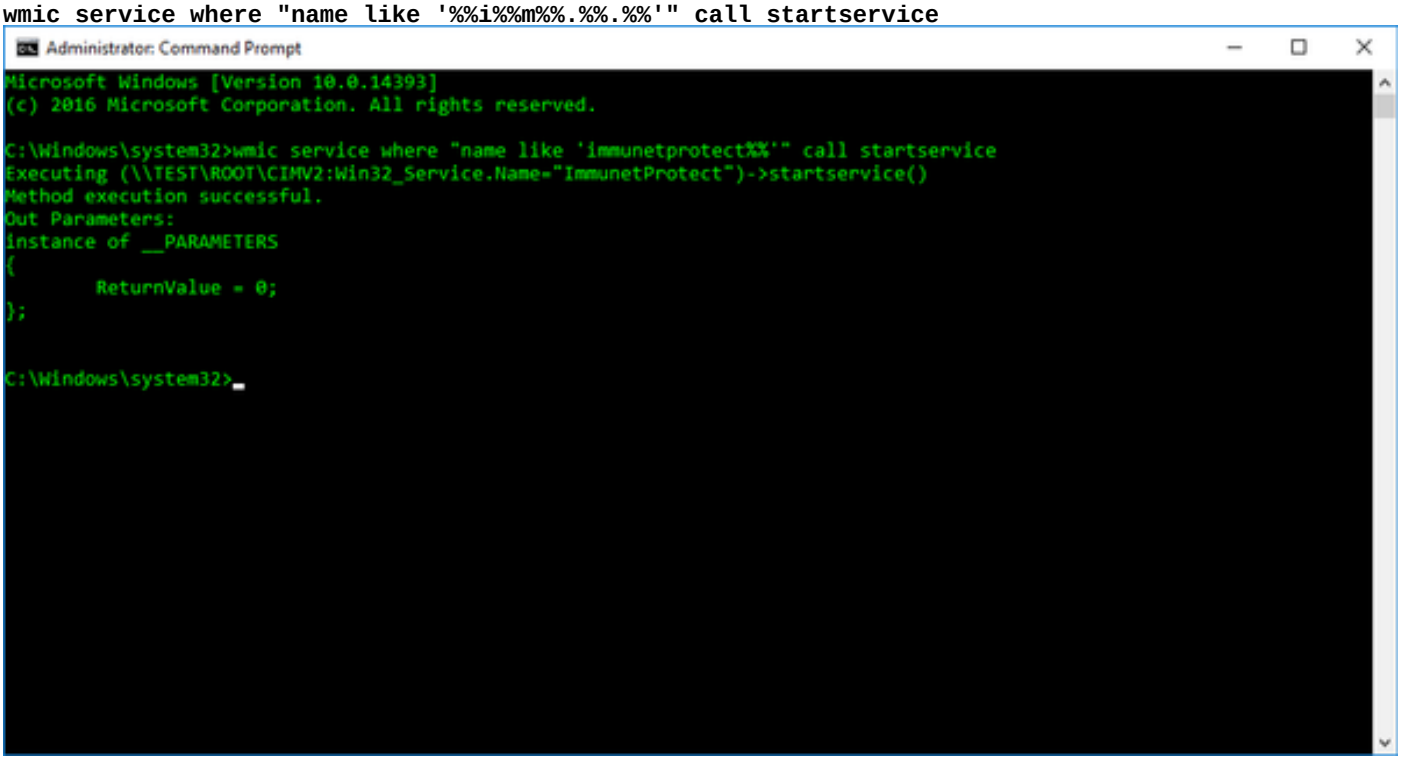
```
“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -r
```

sfc.exe 実行によってサービス コントロール コントロール· パネルにコネクタを-バージョン フォルダ **i** インストールして下さい。

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

コマンドの実行からコネクタを開始して下さい:

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



> **注:** 手動でこのように登録されているマシンが組織のデフォルト グループに置かれることが期待されます。 これらのマシンを手動で移動するか、またはそれらのマシンのための望ましいグループであるためにデフォルト グループを変更したいと思うかどうか決定して下さい。

この時点で FireAMP クライアントは作動中であるはずです。 サービスが実行されていること接続を確認するのにユーザインターフェイスを使用。 ユーザインターフェイスが開始するために設定 されない場合下記のコマンドで手動で開始することができます。 現在アップデートすることをインストール済み バージョンのためのバージョン番号を忘れないでいて下さい。

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

Linux

Linux のためのマシンをクローンとして作るための一般的なステップに新しい識別がです Windows に類似したあり。 ステップおよびコマンドはここにあります:

マスター イメージで AMP をインストールして下さい

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

AMP サービスを停止して下さい

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

local.xml を削除して下さい

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

異なるコンピューターがクローンとして作られたイメージと起動する場合、AMP サービスは自動的に開始し、新しい識別を生成します。 それはクラウドのグループのすべての通信コネクタを渡ってユニークである必要があります[かどうかパブリック、か private]。