L'image ou copient un ordinateur avec le connecteur de FireAMP installé

Contenu

Introduction

Ce document décrit les processus pour empêcher de plusieurs ordinateurs pour tenter l'utilisation de mêmes globalement - l'identifiant unique (GUID), qui empêche les objets en double d'ordinateur pour apparaître dans le tableau de bord de nuage de FireAMP. Ce processus permet à FireAMP pour fonctionner correctement sur un ordinateur copié.

En tant qu'administrateur système, vous pouvez vouloir inclure le connecteur de FireAMP sur vos images principales de PC Windows. FireAMP, cependant, exige que des systèmes peuvent être seulement identifiés. Les étapes générales pour copier un ordinateur pour le Linux est au bas de cet article.

> Remarque: Le premier ensemble d'instructions s'applique à la version 4.1.4 ou ultérieures de FireAMP. Plus loin vous trouvez les étapes d'origine pour des ordinateurs exécutant des versions antérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

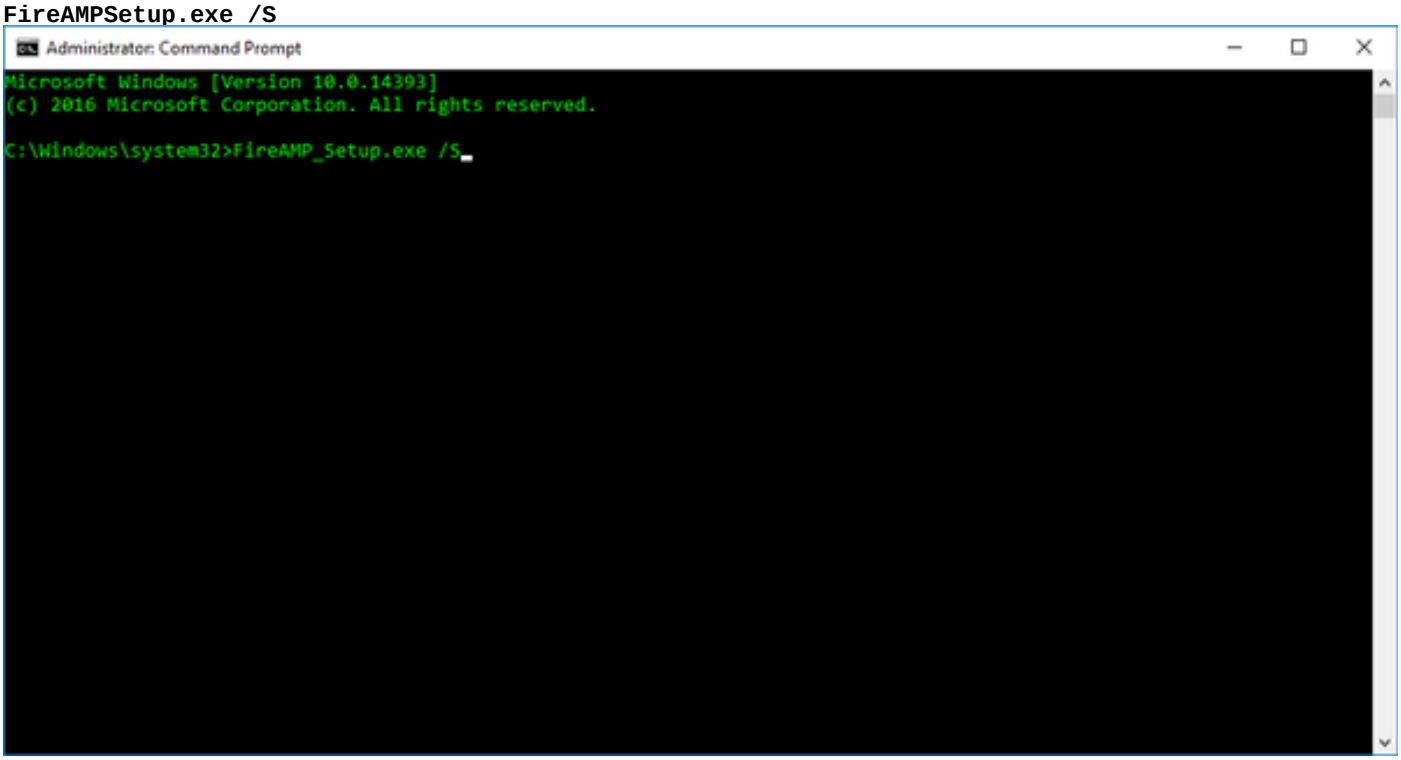
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Préinstallation - Versions 4.1.4 et ultérieures

Exécutez ces étapes pour préparer un ordinateur pour la représentation :

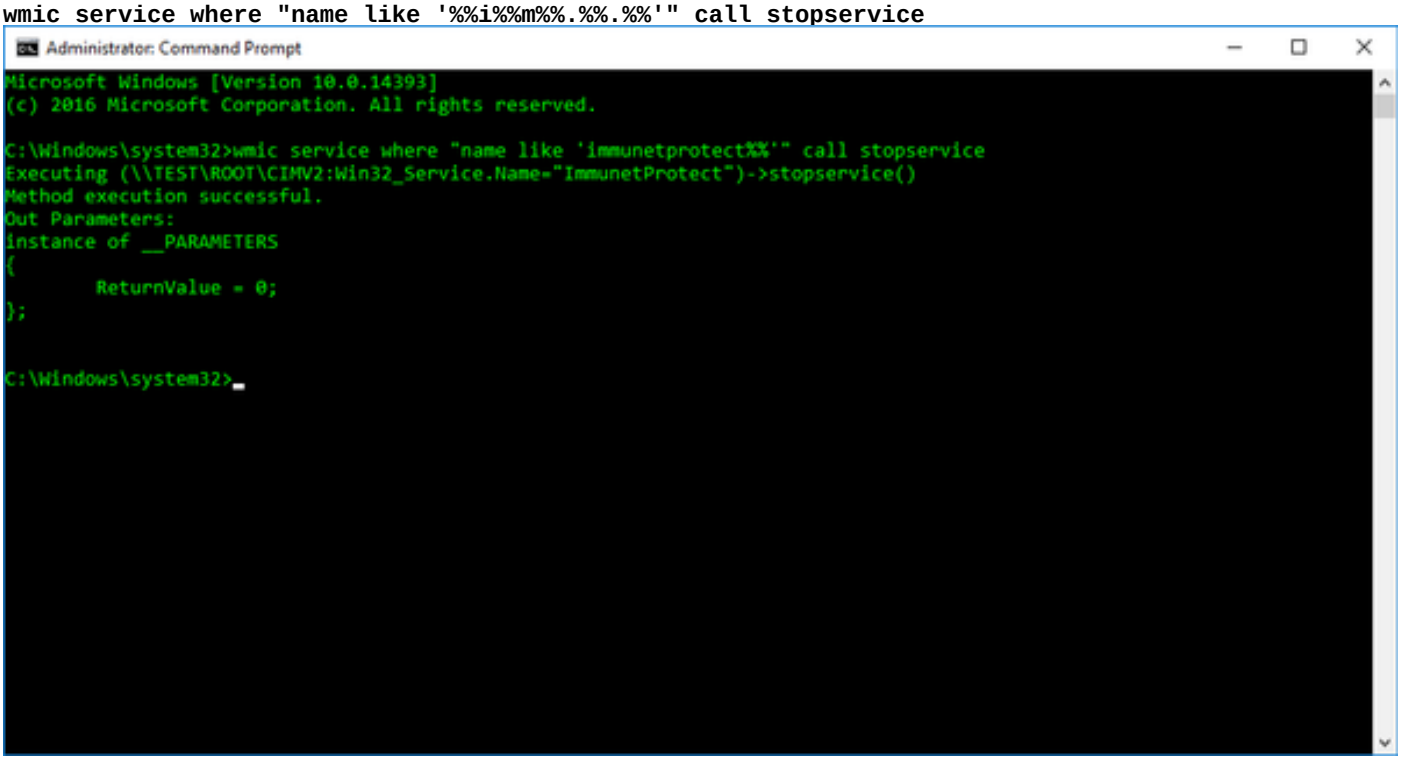
Étape 1. Installez FireAMP sur votre image principale.

```
FireAMPSetup.exe /S
```



Étape 2. Arrêtez le service de FireAMP.

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



Utilisez la commande suivante si vous faites activer la protection de connecteur. Le mot de passe sera visible dans l'invite de commande.

```
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
```

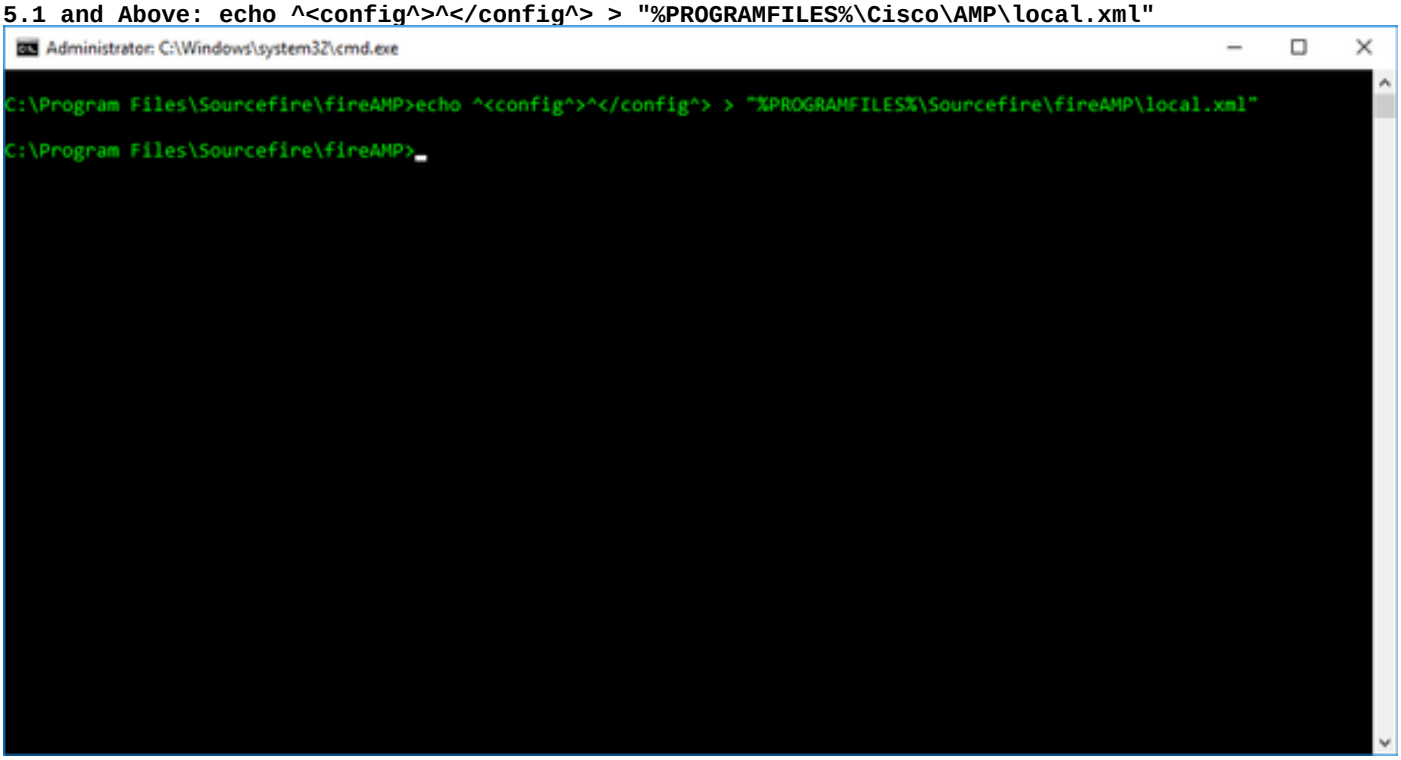
> Remarque: Si le service de FireAMP est commencé de nouveau, l'image principale régénère local.xml. Vous devez répéter ces étapes pour neutraliser l'image principale de nouveau. Soyez sûr d'inclure ces étapes dans votre procédé de préparation d'image principale.

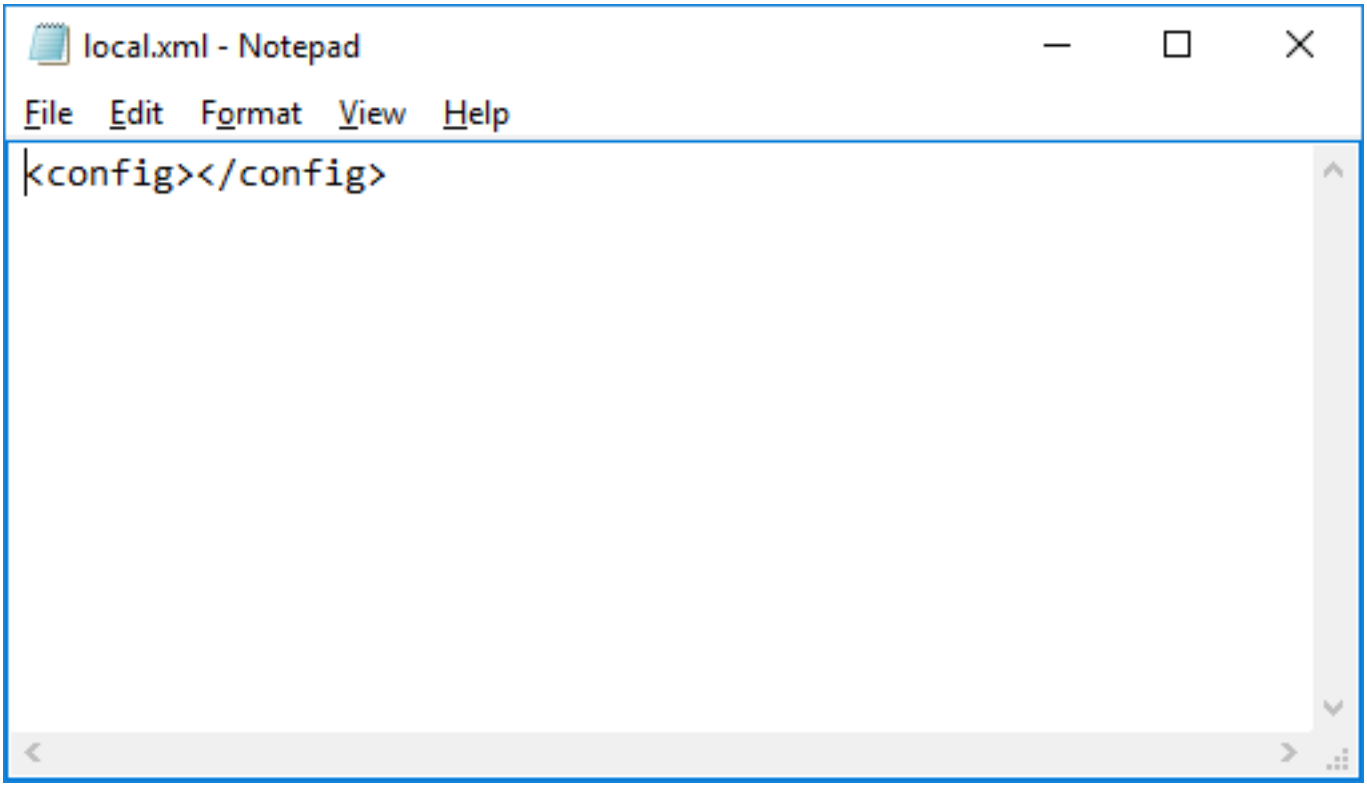
Étape 3. Effacement **`local.xml.`**

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

Étape 4. Créez un **`fichier du`** blanc **`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"
```





POST-installation - Versions 4.1.4 et ultérieures

FireAMP 4.1.4 et plus élevé génère automatiquement un nouvel identifiant unique de regisration et d'universel (UUID) quand le service de connecteur détecte un **fichier du** blanc **local.xml**. Plus d'étapes n'ont besoin d'être exécutées sur l'ordinateur lui-même.

> Remarque: On le prévoit que les ordinateurs qui s'inscrivent à un **fichier du** blanc **local.xml** est placé dans le groupe par défaut de vos organismes. Vous devez décider si vous voulez déplacer ces ordinateurs manuellement ou changer votre groupe par défaut pour être le groupe désiré pour ces ordinateurs.

En ce moment le client de FireAMP devrait être en service. Vous pouvez employer l'interface utilisateur pour vérifier la Connectivité et cela que le service exécute. Si votre interface utilisateur n'est pas placée pour commencer, elle peut être manuellement commencée par ces derniers commande. Soyez sûr de mettre à jour le numéro de version pour votre version actuellement installée.

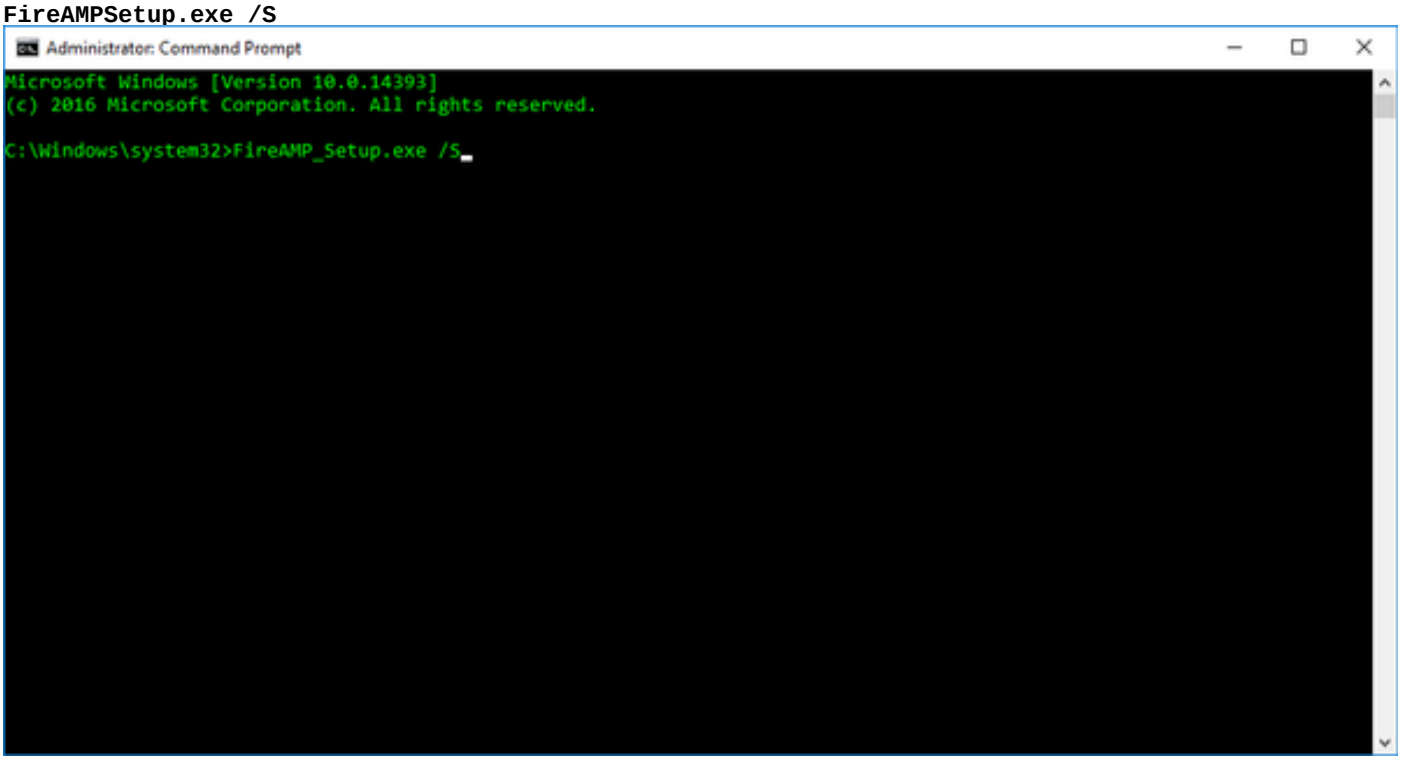
```
5.0 and Lower: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\iptray.exe" -f
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\iptray.exe" -f
```

Préinstallation - Les versions diminuent que 4.1

Exécutez ces étapes pour préparer un ordinateur pour la représentation :

Étape 1. Installez FireAMP sur votre image principale.

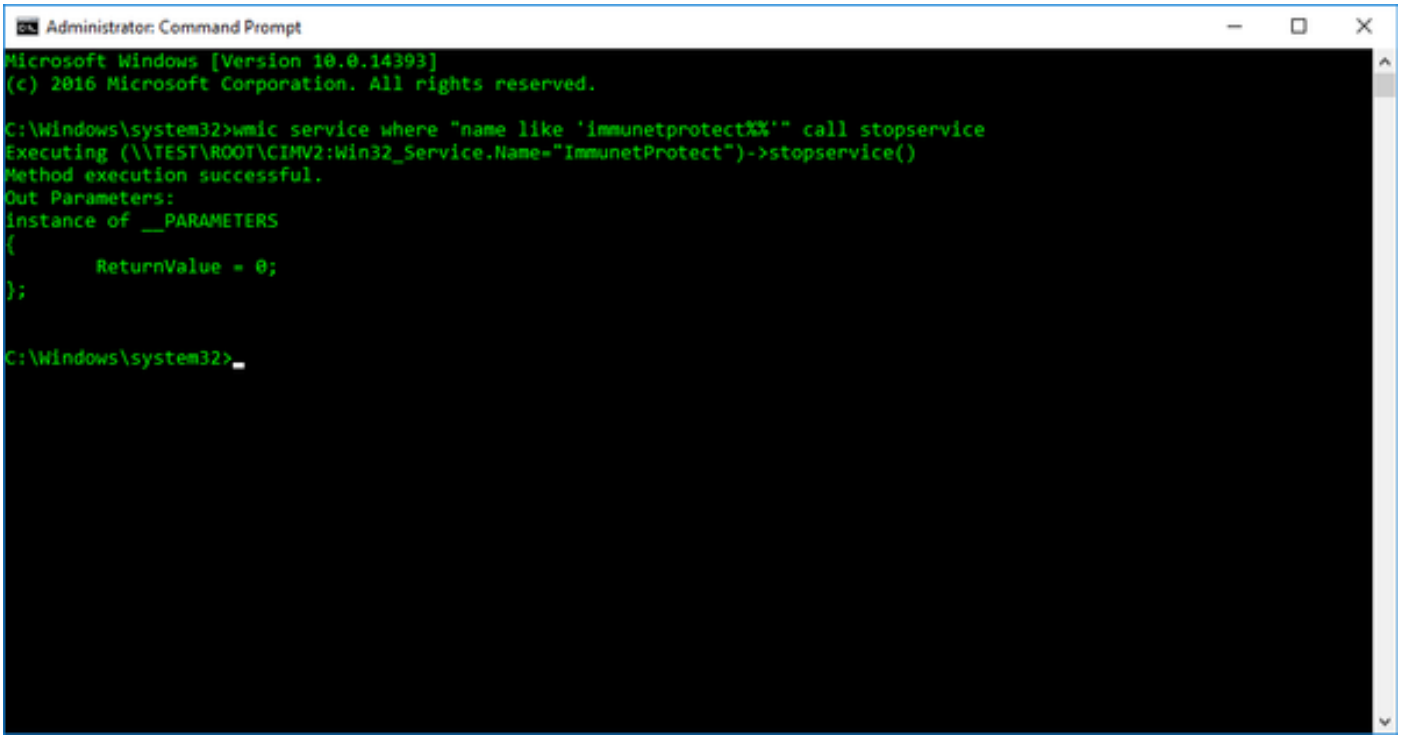
```
FireAMPSetup.exe /S
```



Étape 2. Arrêtez le service de FireAMP.

> Remarque: Si vous utilisez un mot de passe de protection de connecteur, ceci doit être fait de l'interface utilisateur.

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



Étape 3. Déterminez l'emplacement du produit de fireAMP. Le par défaut est

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

Étape 4. Désinstallez le service de connecteur de FireAMP du panneau de configuration en exécutant **sfc.exe - u du** répertoire de version. Soyez sûr de mettre à jour la commande avec votre numéro de version actuellement installé.

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

Étape 5. Si vous voulez réutiliser l'objet existant d'ordinateur, vous devez sauvegarde le **fichier** existant **local.xml**. Le local.xmlis **trouvé** dans ce répertoire :

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

> Remarque: C'est idéal pour la personne réimagent mais peuvent ne pas être pratique pour un-à-beaucoup de pratiques en matière de représentation car il stocke les seules informations, telles que GUID d'un ordinateur unique.

Étape 6. Après que vous sauvegardiez **local.xml ou** si vous n'avez pas besoin de réutiliser l'objet d'ordinateur dans votre tableau de bord, l'effacement local.xml**, suivant les indications de l'**image :

```
del local.xml
```

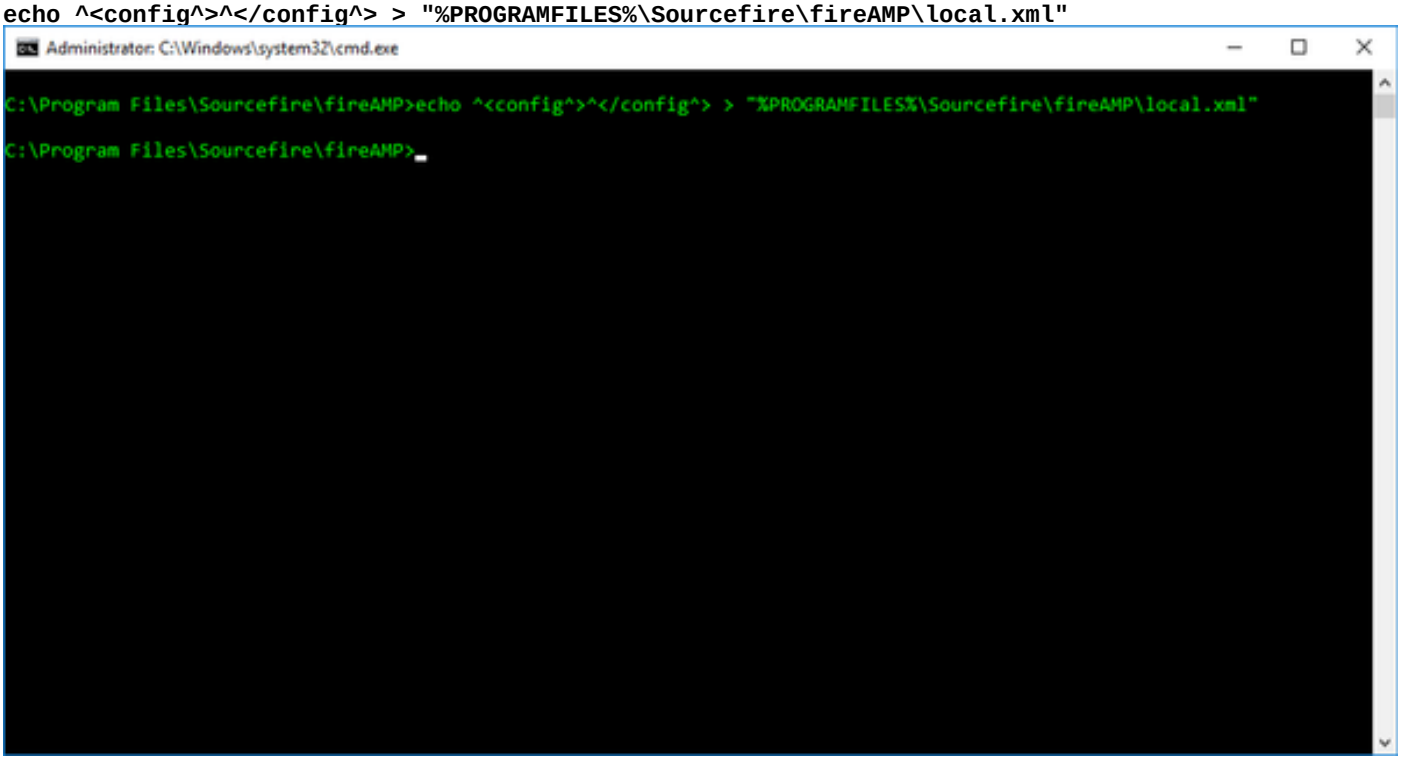
Post installation - Les versions diminuent que 4.1

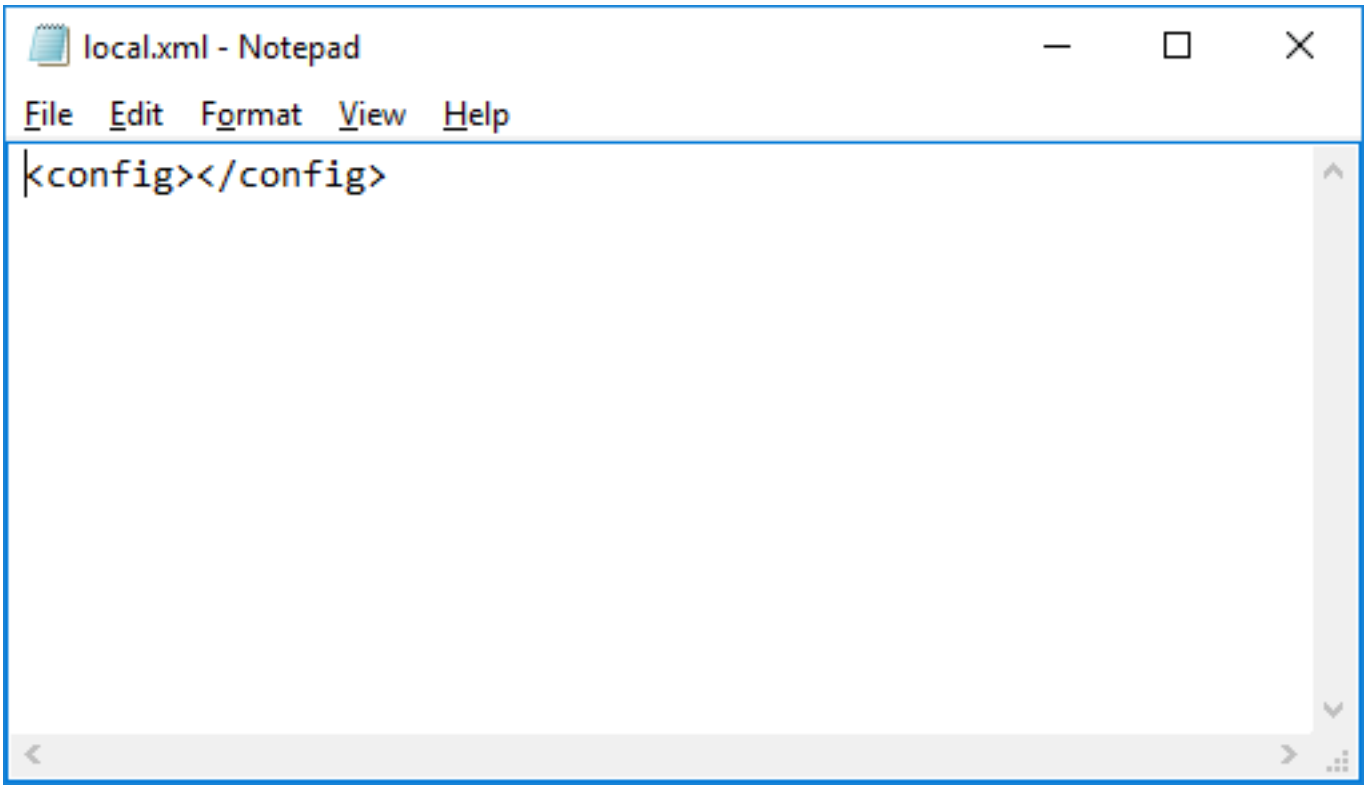
Exécutez ces étapes après avoir déployé votre image :

> Remarque: Si vous commencez le service de FireAMP avec le **fichier** générique **local.xml**, il crée un nouvel objet d'ordinateur. Si vous avez l'original local.xmlfile**,** vous pouvez les restaurer par ordinateur pour faire réutiliser l'objet.

Étape 1. Restaurez le **`fichier local.xml`** sur ce répertoire à ce moment si vous le souteniez avant de réimager. Si vous ne restaurez pas un local.xmlfile, vous devez encore créer générique pour que le connecteur s'enregistre correctement.

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





Étape 2. Enregistrez le connecteur avec le service par le **`sfc d'`**exécution **`- r du`** répertoire de version. Cette étape remplit le **`fichier local.xml`** pour un ordinateur. Soyez sûr de mettre à jour les commandes ci-dessous avec votre numéro de version actuellement installé.

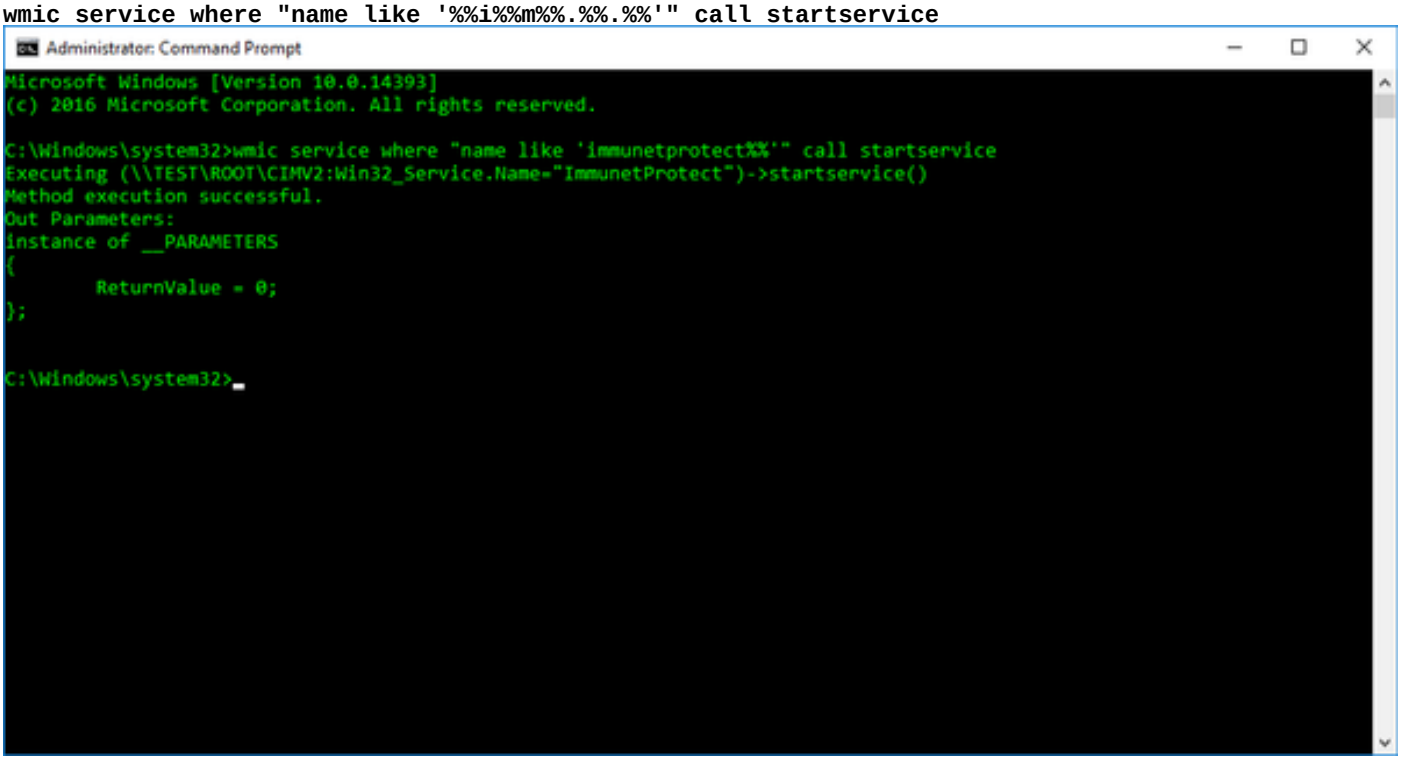
```
“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -r
```

Installez le connecteur sur le panneau de configuration de services en exécutant **`sfc.exe - I du`** répertoire de version.

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

Commencez le connecteur par exécuter la commande :

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



> Remarque: On s'attend à ce que les ordinateurs qui sont manuellement enregistrés de cette façon soient placés dans le groupe par défaut de vos organismes. Vous devez décider si vous voulez déplacer ces ordinateurs manuellement ou changer votre groupe par défaut pour être le groupe désiré pour ces ordinateurs.

En ce moment le client de FireAMP devrait être en service. Vous pouvez employer l'interface utilisateur pour vérifier la Connectivité et cela que le service exécute. Si votre interface utilisateur n'est pas placée pour commencer, elle peut être manuellement commencée par la commande ci-dessous. Soyez sûr de mettre à jour le numéro de version pour votre version actuellement installée.

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

Linux

Les étapes générales pour copier un ordinateur pour le Linux et ont une nouvelle identité est semblable à Windows. Voici les étapes et les commandes :

Installez l'AMPÈRE sur votre image principale

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

Arrêtez le service d'AMPÈRE

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

Effacement local.xml

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

Quand un ordinateur différent initialise avec l'image copiée, le service d'AMPÈRE commencera automatiquement et génèrera une nouvelle identité. Il doit être seul à travers tous les connecteurs de communication dans un groupe dans le nuage [si public, ou privé].