

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

Contenu

[Introduction](#)

[Copiez un ordinateur avec le connecteur de FireAMP installé](#)

[Méthode manuelle](#)

[Préinstallation](#)

[Post installation](#)

[Synchronisation d'identité](#)

Introduction

En tant qu'administrateur système, vous pouvez vouloir créer une image de votre disque ou copier votre disque dur, et le répliquez sur l'autre système physique ou virtuel. Il te permet pour économiser le temps et les ressources. Si les utilisateurs dans votre organisation exécutent un certain logiciel, vous pouvez vouloir l'inclure sur « l'image principale », de sorte que chaque système copié ait une copie de ce logiciel. Certains logiciels tels que FireAMP exige d'un système d'être seulement identifié. Ce document décrit les processus pour empêcher de plusieurs ordinateurs de tenter pour utiliser la même chose globalement - l'identifiant unique (GUID), qui peut empêcher les objets en double d'ordinateur d'apparaître dans le tableau de bord de nuage de FireAMP. Il permet à FireAMP pour travailler correctement sur un système copié.

Copiez un ordinateur avec le connecteur de FireAMP installé

Si vous voulez créer une image d'un disque ou copier un disque dur, il y a de deux vous approche peut prendre :

- Méthode manuelle
- Synchronisation d'identité

Méthode manuelle

Vous pouvez manuellement créer « une image principale » de votre ordinateur avec le connecteur de FireAMP installé. Il y a deux étapes principales à ce processus :

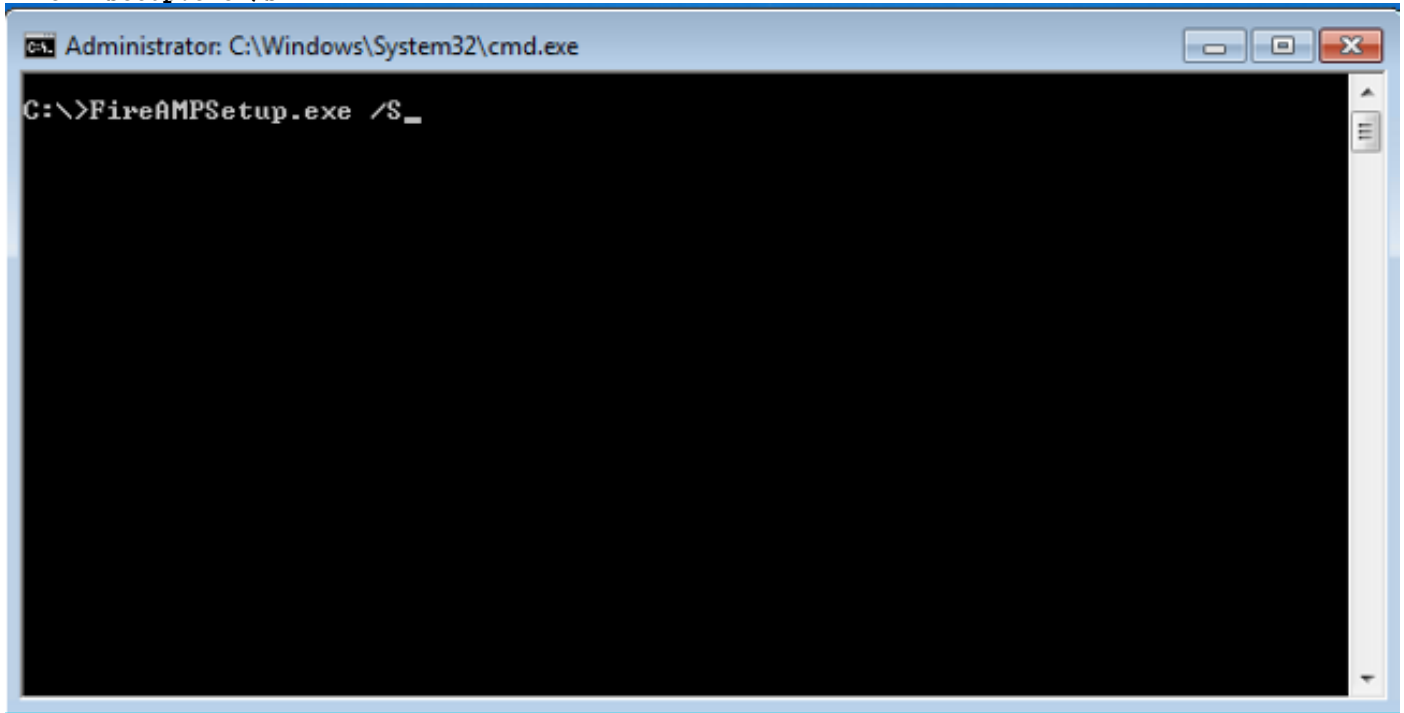
- Préinstallation
- Post installation

Préinstallation

Exécutez les étapes suivantes pour préparer un ordinateur pour la représentation :

1. Exécutez l'installateur d'installation de FireAMP.

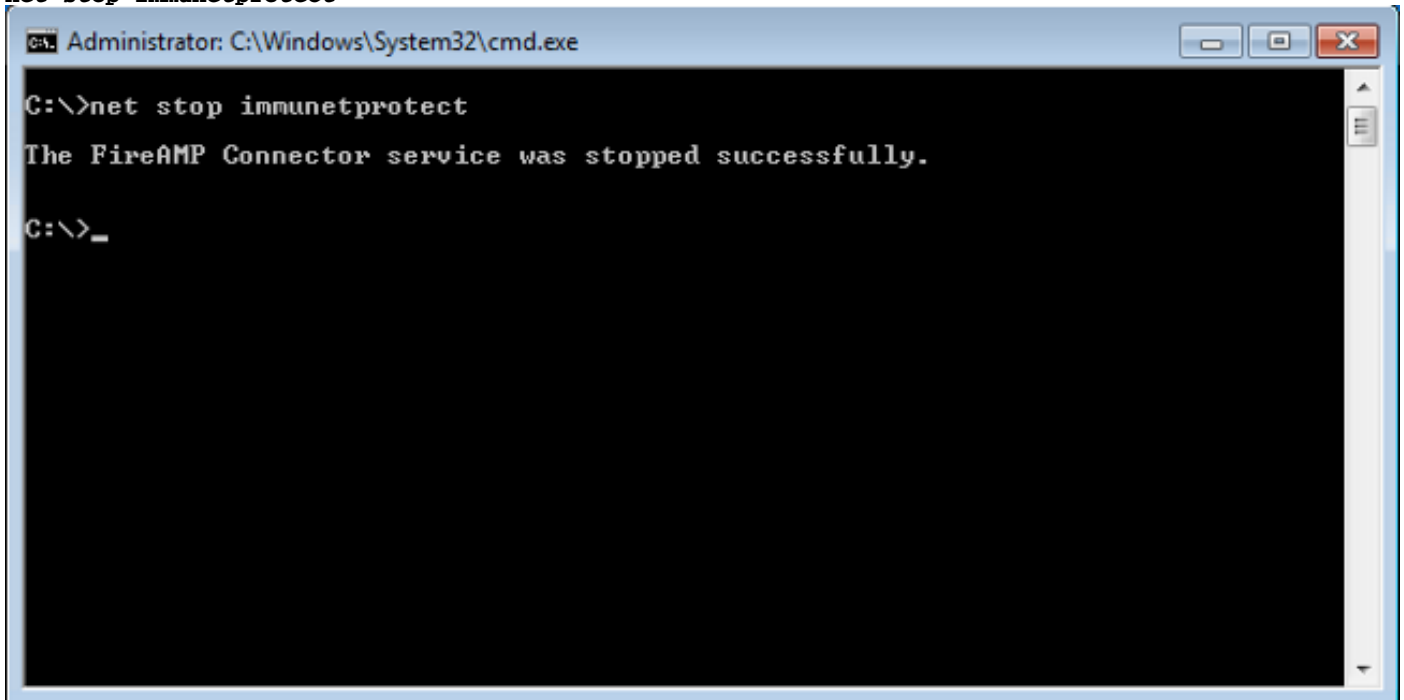
`FireAMPSetup.exe /S`



```
Administrator: C:\Windows\System32\cmd.exe
C:\>FireAMPSetup.exe /S_
```

2. Ouvrez une invite de commande en tant qu'administrateur et arrêtez le connecteur de FireAMP en exécutant la commande suivante :

`net stop immunetprotect`

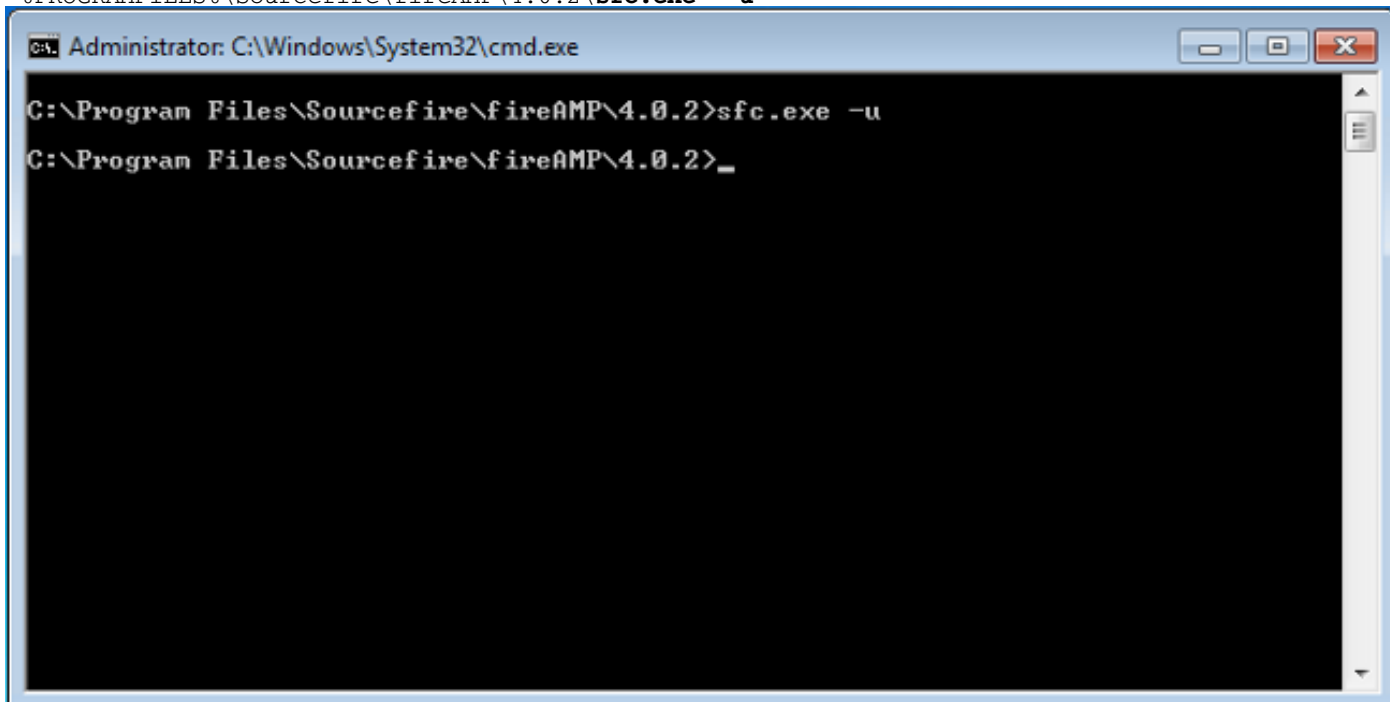


```
Administrator: C:\Windows\System32\cmd.exe
C:\>net stop immunetprotect
The FireAMP Connector service was stopped successfully.
C:\>_
```

3. Déterminez l'emplacement du produit de fireAMP. Le par défaut est `%PROGRAMFILES% \ Sourcefire \ fireAMP`

4. Désinstallez le service de connecteur de FireAMP du panneau de configuration en exécutant `sfc.exe - u` du répertoire de version.

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.0.2\sfc.exe" -u
```



```
Administrator: C:\Windows\System32\cmd.exe
C:\Program Files\Sourcefire\fireAMP\4.0.2>sfc.exe -u
C:\Program Files\Sourcefire\fireAMP\4.0.2>_
```

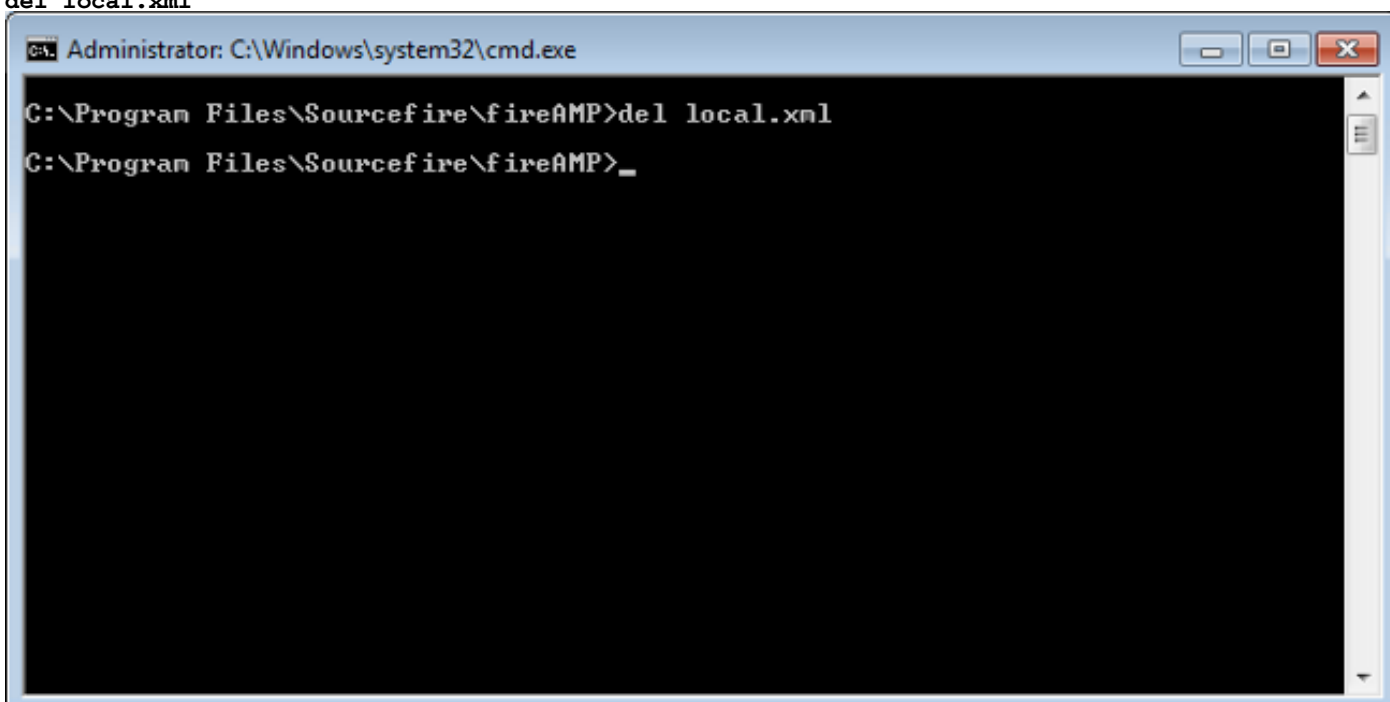
5. Si vous voulez réutiliser l'objet existant d'ordinateur, vous devez sauvegarde le fichier existant `local.xml`. Le `local.xml` est trouvé dans le répertoire suivant :

```
%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.

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, supprimez `local.xml`.

```
del local.xml
```



```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files\Sourcefire\fireAMP>del local.xml
C:\Program Files\Sourcefire\fireAMP>_
```

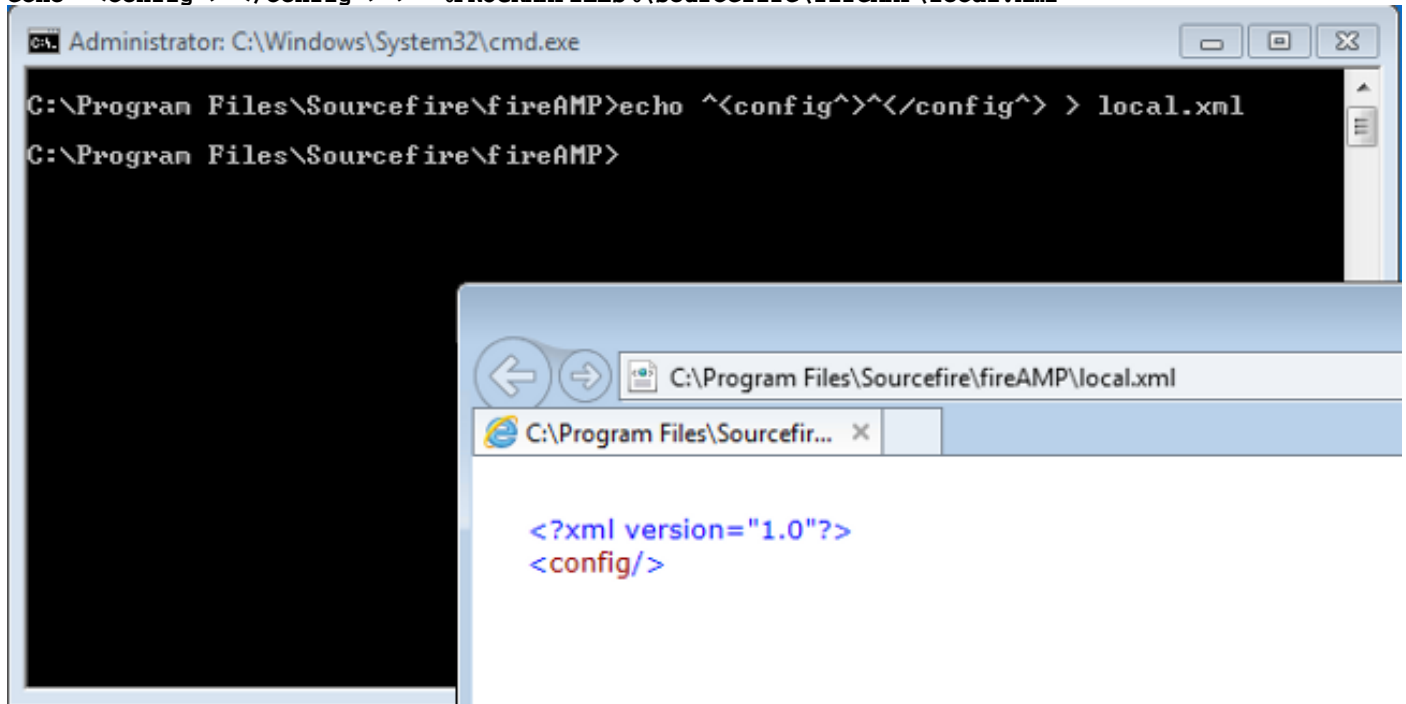
Post installation

Exécutez les étapes suivantes 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.

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`, nous devons encore créer générique pour que le connecteur s'enregistre correctement.

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



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.

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.0.2\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\4.0.2\sfc.exe" -i
```

Commencez le connecteur par exécuter la commande :

```
net start immunetprotect
```

```
Administrator: C:\Windows\System32\cmd.exe
C:\Program Files\Sourcefire\fireAMP\4.0.2>sfc.exe -r
C:\Program Files\Sourcefire\fireAMP\4.0.2>sfc.exe -i
C:\Program Files\Sourcefire\fireAMP\4.0.2>net start immunetprotect
The FireAMP Connector service was started successfully.
C:\Program Files\Sourcefire\fireAMP\4.0.2>_
```

En ce moment le client de FireAMP devrait être en service. Vous pouvez employer l'interface utilisateur d'utilisateur web pour vérifier la Connectivité et cela que le service exécute.



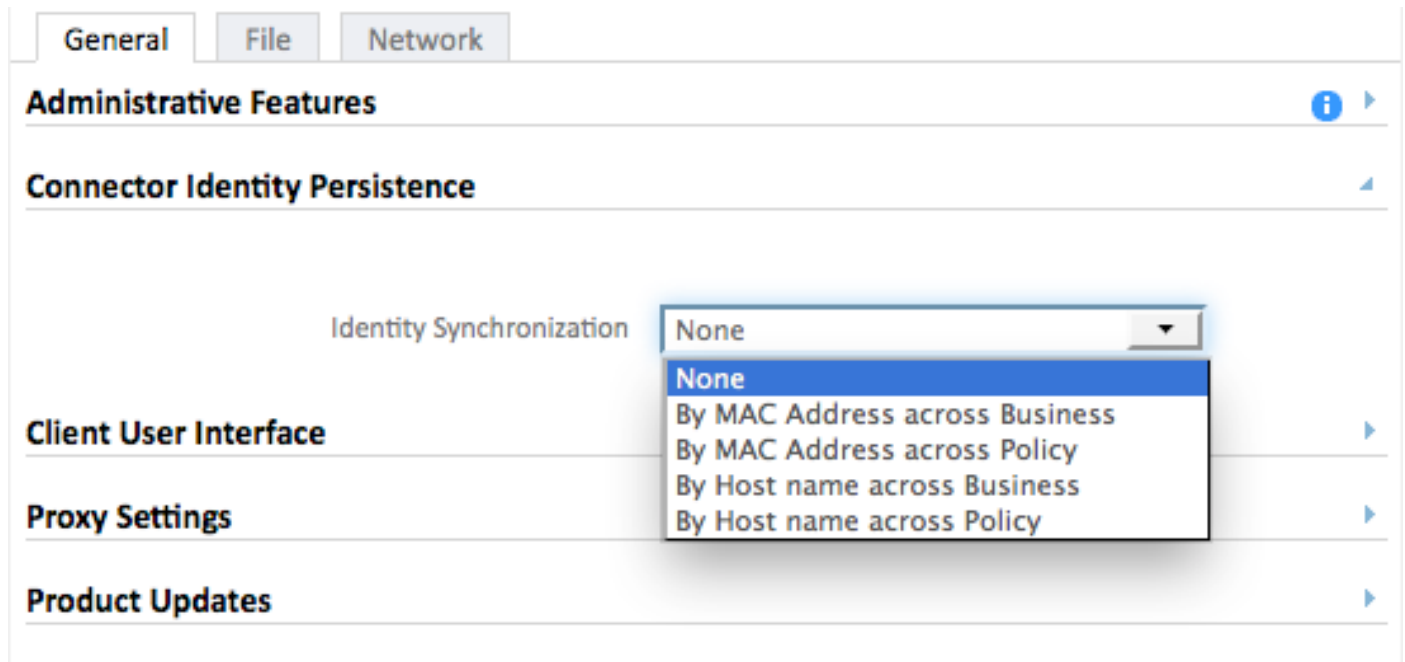
Synchronisation d'identité

La synchronisation d'identité te permet pour mettre à jour les environnements virtuels d'une procédure de connexion cohérente d'événement ou quand des ordinateurs sont réimagés. Vous pouvez lier un connecteur à une adresse MAC ou le nom d'hôte de sorte qu'un nouveau journal d'événements ne soit pas créé chaque fois une nouvelle session virtuelle soit commencé ou un ordinateur est réimagé. Vous pouvez choisir d'appliquer cette configuration avec la finesse à

travers différentes stratégies, ou à travers votre organisation entière.

Remarque: Dans certains cas un virtual machine copié peut être placé au groupe par défaut plutôt que le groupe qu'il a été copié de. Si ceci se produit, entrez le virtual machine dans le groupe correct dans la console de FireAMP.

Afin d'activer la synchronisation d'identité, vous devez configurer une stratégie que vous voulez appliquer à vos ordinateurs.



La synchronisation d'identité fonctionne bien dans un environnement de travaux pratiques parce que vous pouvez tester et contrôler des aspects de l'environnement. Cependant, il a plusieurs limites :

- La synchronisation d'identité fonctionne seulement par le proxy avec des versions 4.1.x et ultérieures d'agent.
- La synchronisation d'identité synchronise par une adresse MAC simple. Cela signifie, si vous avez un ordinateur portable avec une carte de câble et Sans fil, vous pourrait obtenir deux identités dans le nuage.
- La synchronisation d'identité synchronise par le nom de domaine complet. Cela signifie, si vous avez un serveur DHCP donnant le suffixe de domaine que votre identité peut ne pas changer.
- La synchronisation d'identité doit être configurée dans votre stratégie sur l'initiale installent. Si vous activez la synchronisation d'identité POST-installez, alors vous pouvez finir par avec des doublons.