Déploiement d'AMP de Cisco pour des points finaux avec la persistance d'identité

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Processus](#)
[Configurez](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

Introduction

Ce document décrit que comment la caractéristique de persistance d'identité sur Cisco a avancé la protection de malware (AMP) pour des points finaux permet un identifiant unique d'objet d'ordinateur universellement (UUID) à réutiliser quand un ordinateur ou un virtual machine (VM) est réimagé ou redéployé. Ceci empêche la création des objets en double d'ordinateur dans un tableau de bord, et met à jour des données contiguës pour ces objets d'ordinateur. Ceci aide également à mettre à jour les connecteurs de point final, à fournir la continuité des données, et à maintenir le compte de permis dans le contrôle.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du ce des thèmes :

- Access à l'AMP de Cisco pour le tableau de bord de points finaux
- Configurez la persistance d'identité avant que vous déployiez au commencement le connecteur
- La persistance d'identité est seulement prise en charge sur le système d'exploitation Windows (le SYSTÈME D'EXPLOITATION)

Note: La caractéristique de persistance d'identité doit être activée avec le centre d'assistance technique Cisco (TAC).

Composants utilisés

Les informations dans ce document sont basées sur l'AMP de Cisco pour le tableau de bord de points finaux.

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Processus

L'option de persistance d'identité utilise ces le processus quand c'est enable :

1. L'option de persistance d'identité est configurée dans une stratégie.
2. L'AMP pour l'installateur de points finaux est généré du tableau de bord et déployé sur un nouveau ordinateur ou VM.
3. Un nouvel objet d'ordinateur est créé avec un UUID et l'indicateur de persistance d'identité.

- Contrôle d'enregistrement

Quand les débuts de service de connecteur, le contrôle d'enregistrement de nuage est exécutés. Le contrôle d'enregistrement évalue les informations de l'ordinateur comme, de l'adresse Internet et de l'adresse MAC en cours. Il évalue également la configuration de persistance d'identité dans la stratégie contre le nuage afin de déterminer si un nouvel UUID doit être généré.

- Critères d'enregistrement

Un objet d'ordinateur a un indicateur masqué réglé qui correspond à la configuration de persistance d'identité utilisée. Cet indicateur, avec les seules informations (adresse Internet ou adresse MAC) est utilisé pour fournir l'UUID existant à n'importe quel ordinateur qui apparie les critères. Si un indicateur et les seules informations de l'ordinateur ne s'assortit avec aucun objet existant d'ordinateur, un nouveaux UUID et objet sont générés pour l'ordinateur.

> **Note**: Quand vous utilisez l'adresse Internet, le nom de domaine complet (FQDN) est utilisé. Si vous avez un ordinateur nommé **test** et des autres **test.domain.com** nommé par ordinateur, ils ne s'assortissent pas, et l'UUID n'est pas réutilisé.

- Ordinateurs mobiles

Le mouvement des ordinateurs entre les groupes avec différentes configurations de persistance d'identité crée des doublons. C'est dû à un indicateur masqué qui est associé avec chaque configuration de persistance d'identité. Quand les configurations ne s'assortissent pas, des doublons sont générés. Les deux groupes doivent faire appliquer la même stratégie quand ils travaillent avec **à travers des paramètres de la stratégie**. Si les configurations sont identiques mais les stratégies sont différentes, des doublons sont créés.

> **Note**: Si vous voulez copier ou image un ordinateur avec l'AMP de Cisco pour des points finaux installés, lisez ce document.

- Élection d'adresse MAC

Un ordinateur peut avoir des plusieurs adresses MAC, cependant, il n'est pas possible d'influencer manuellement le processus d'élection d'adresse MAC pendant l'enregistrement de connecteur. Vous devez utiliser les configurations d'adresse MAC seulement si vous pouvez garantir que vos ordinateurs a seulement une adresse MAC, autrement utilisez l'adresse Internet.

- Groupe par défaut

La persistance d'identité doit également être configurée pour la stratégie appliquée à votre groupe par défaut. Au cas où une stratégie ou un groupe serait supprimée avec un ordinateur actif, l'ordinateur est placé dans le groupe par défaut quand un contrôle d'enregistrement est exécuté la fois prochaine. Si la persistance d'identité n'est pas configurée pour le groupe par défaut, alors l'objet de doublon est généré.

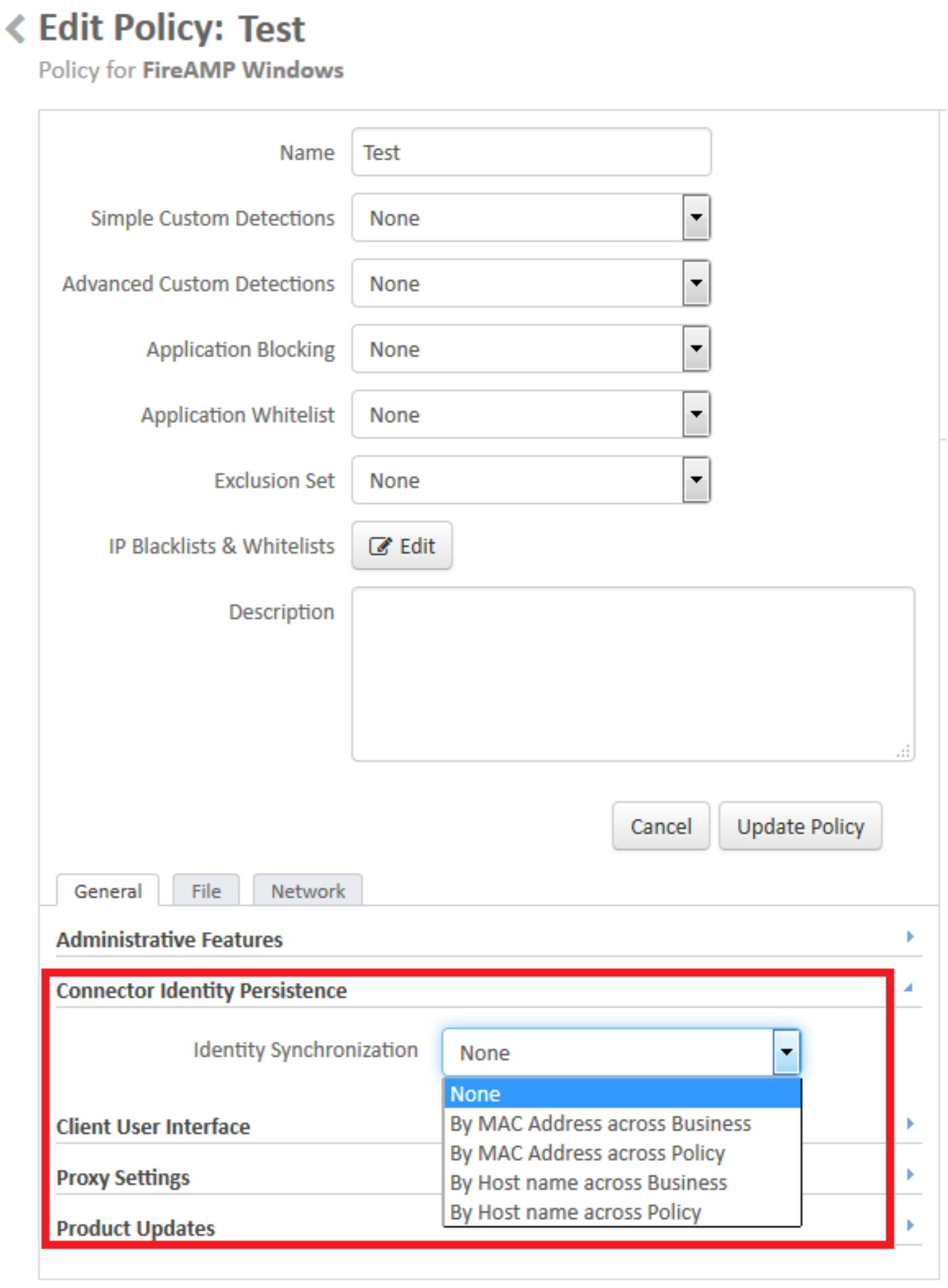
> **Note**: Dans certains cas, une VM copiée pourrait être placée au groupe par défaut plutôt que le groupe qu'il a été copié de. Si ceci se produit, entrez la VM dans le groupe correct dans la console de FireAMP.

Configurez

Suivez les étapes ici afin de déployer le connecteur avec la persistance d'identité :

Étape 1. Appliquez-vous la persistance désirée d'identité plaçant à vos stratégies :

- Naviguez vers la **Gestion > les stratégies**
- Sélectionnez la stratégie désirée. Cliquez sur Edit
- Naviguez vers l'**onglet Général**. Il est sélectionné, par défaut
- Sélectionnez la **persistance d'identité de connecteur**. **La synchronisation d'identité** chutent apparaît vers le bas suivant les indications de l'image.



Note: L'activation d'une caractéristique après que l'installation des points finaux puisse causer les objets en double d'être générée pour chaque ordinateur.

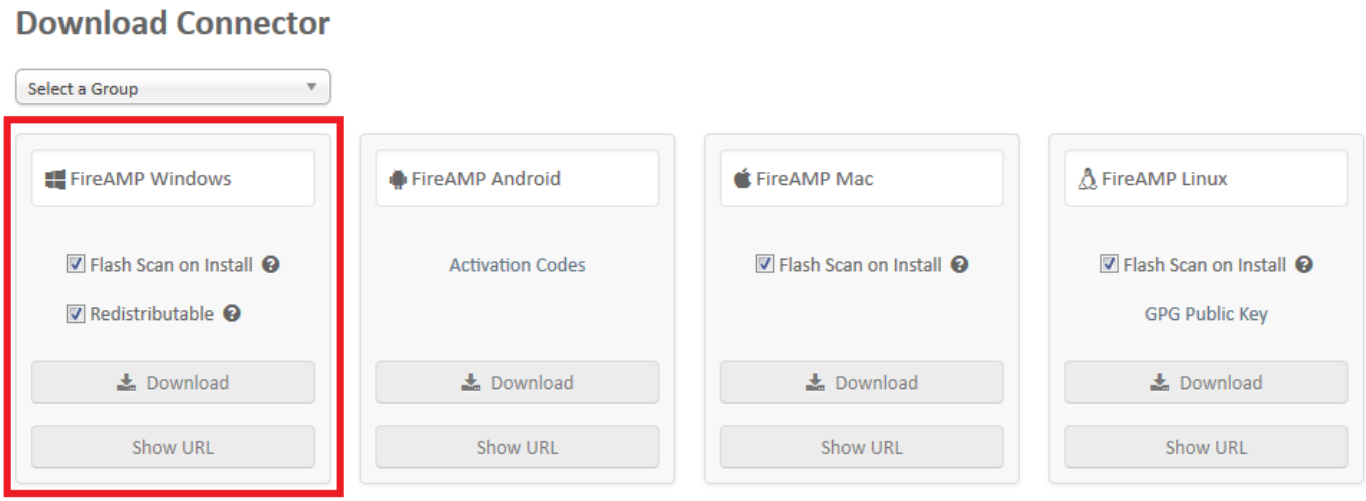
Sélectionnez une option de **synchronisation d'identité** qui est le meilleur pour votre environnement. Ces options sont disponibles :

- Aucun : La caractéristique n'est pas activée. Le connecteur UUIDs ne sont pas synchronisés avec le nouveau connecteur n'installe sous aucune circonstance. Chaque nouvelle installation génère un nouvel objet d'ordinateur.
- Par l'adresse MAC à travers l'entreprise : Les nouveaux connecteurs recherchent le connecteur le plus récent qui a la même adresse MAC afin de synchroniser à travers toutes les stratégies dans l'entreprise qui ont la synchronisation d'identité réglée à une valeur autre qu'aucun. Une fois sélectionné, un objet d'ordinateur est créé et signalé pour synchroniser avec n'importe quel ordinateur qui utilise cette adresse MAC à travers le compte entier.
- Par l'adresse MAC à travers la stratégie : Les nouveaux connecteurs recherchent le connecteur le plus récent qui a la même adresse MAC afin de synchroniser avec dans la même stratégie. Une fois sélectionné, un objet d'ordinateur est créé et signalé pour synchroniser avec n'importe quel ordinateur qui utilise cette adresse MAC et est assigné enregistré contre la stratégie spécifique.
- Par nom d'hôte à travers l'entreprise : Les nouveaux connecteurs recherchent le connecteur le plus récent qui a la même adresse Internet afin de synchroniser avec à travers toutes les stratégies dans l'entreprise qui ont la synchronisation d'identité réglée à une valeur autre qu'aucun. Une fois sélectionné, un objet d'ordinateur est créé et signalé pour synchroniser avec n'importe quel ordinateur qui utilise cette adresse Internet à travers le compte entier. **Note**: Si vous choisissez d'utiliser la persistance d'identité, Cisco recommande que vous utilisiez **par nom d'hôte à travers l'entreprise**. Un ordinateur a une adresse Internet, mais peut avoir plus d'une adresse MAC. La configuration à travers votre entreprise peut réduire la complexité de la configuration pendant qu'elle rend les objets globalement disponibles plutôt que par stratégie.
- Par nom d'hôte à travers la stratégie : Les nouveaux connecteurs recherchent le connecteur le plus récent qui a la même adresse Internet afin de synchroniser avec dans la même stratégie. Une fois sélectionné, un objet d'ordinateur est créé et signalé pour synchroniser à n'importe quel ordinateur qui utilise cette adresse Internet et enregistré à la stratégie spécifique.

Étape 2. Téléchargez le module d'installation du tableau de bord de nuage suivant les indications de l'image :

- Naviguez vers le **connecteur de Gestion > de téléchargement**
- Sélectionnez le nom de groupe désiré, et les options
- Cliquez sur Download
- Utilisez le **redistribuable** pour le logiciel de déploiement de tiers, ou les installations hors ligne

Note: Cisco ne prend en charge pas la création des modules ou de l'installation qui utilise le logiciel de déploiement de tiers.



Étape 3. Déployez le connecteur vers les ordinateurs dans votre organisation.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier si les travaux de persistance d'identité, suivent ces étapes :

1. Installez le connecteur afin de générer un objet d'ordinateur qui est signalé pour la synchronisation d'identité.
2. Après que l'objet ait été créé, notez le **<uuid>** à partir du local.xml classer dans le répertoire d'installation C:\Program Files\Sourcefire\fireAMP\local.xml**. Vous** devez voir une ligne semblable à ceci :
   `<uuid>1234567890-abcd-efgh-ijkl-mnopqrst</uuid>`
3. Après, désinstallez le connecteur. Choisissez **non** d'avoir tous les fichiers retirés du chemin d'installation.
4. Redémarrez le PC et réinstallez l'AMP pour des points finaux avec le même module que plus tôt.
5. Vérifiez le **fichier local.xml** de nouveau selon les mesures initiales et assurez-vous qu'il apparie l'UUID de l'original local.xmlfile**.**

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Assurez-vous que les modules d'installation et les configurations de persistance d'identité sont cohérents.
- Si vous activez le POST-déploiement de persistance d'identité, et employez un module plus ancien afin d'installer le connecteur sans persistance d'identité activée, le connecteur génère des doublons pendant qu'ils s'enregistrent, et met à jour les stratégies avec des configurations actuelles.
- Si vos ordinateurs semblent partager un UUID, assurez-vous qu'ils ne partagent pas les seules informations, telles que des adresses MAC dans les environnements virtualisés.

Informations connexes

- Points finaux avancés de protection de malware
- Support et documentation techniques - Cisco Systems