

L'initié programmé balaye sur FireAMP/AMPÈRE pour des points finaux

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Avant de commencer](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[La stratégie est mise à jour, mais une tâche programmée n'est pas trouvée](#)

[La tâche est créée, mais ne s'exécute pas](#)

Introduction

Vous pouvez exécuter des balayages programmés sur FireAMP quotidien, hebdomadaire, ou mensuel selon vos conditions requises. Quand vous créez des balayages programmés, vous devez fournir les identifiants utilisateurs administratifs pour vos ordinateurs. Ce document adresse les autorisations exigées de l'utilisateur expliquent des balayages programmés réussis.

Conditions préalables

Conditions requises

- Access au tableau de bord de FireAMP
- Les qualifications pour un administrateur expliquent des PC de Windows
- FireAMP 3.x pour Windows XP ou plus tard - Balayages programmés
- FireAMP 4.x pour Windows XP ou plus tard - Balayages COI programmé de balayages et de point final

[Avant de commencer](#)

Quand vous ajoutez un balayage programmé dans une stratégie de FireAMP, elle augmente le numéro de série de stratégie. Les points finaux abaissent la nouvelle stratégie quand ils envoient la pulsation. Utilisant les qualifications fournies, FireAMP crée une tâche programmée dans Windows, et exécute plus tard la tâche. En raison de cette conception, nous devons nous assurer que le compte que nous les utilisons a les autorisations correctes.

Avant que nous configurions programmé, le balayage là sont deux conditions requises principales pour un compte utilisateur que vous prévoyez d'utiliser.

Remarque: Ces autorisations s'appliquent également pour des balayages COI de point final.

1. Le compte doit être un compte administrateur. Ceci pourrait être un administrateur local ou administrateur de domaine.
2. Le compte doit pouvoir **ouvrir une session en tant que lot**.

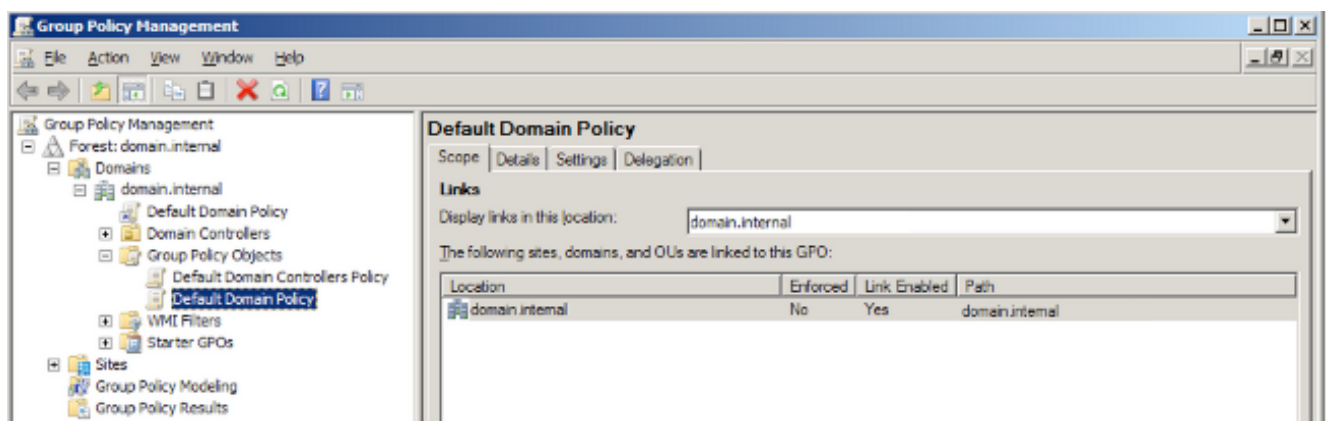
Le login comme autorisation en lots est configuré par l'intermédiaire de la stratégie de groupe. Si ceci n'est pas configuré pour votre domaine, alors les comptes administratifs par défaut devraient pouvoir ouvrir une session en tant que lot. S'il est configuré pour votre domaine, le compte doit appartenir à un groupe défini dans l'objet de stratégie de groupe (GPO).

Configuration

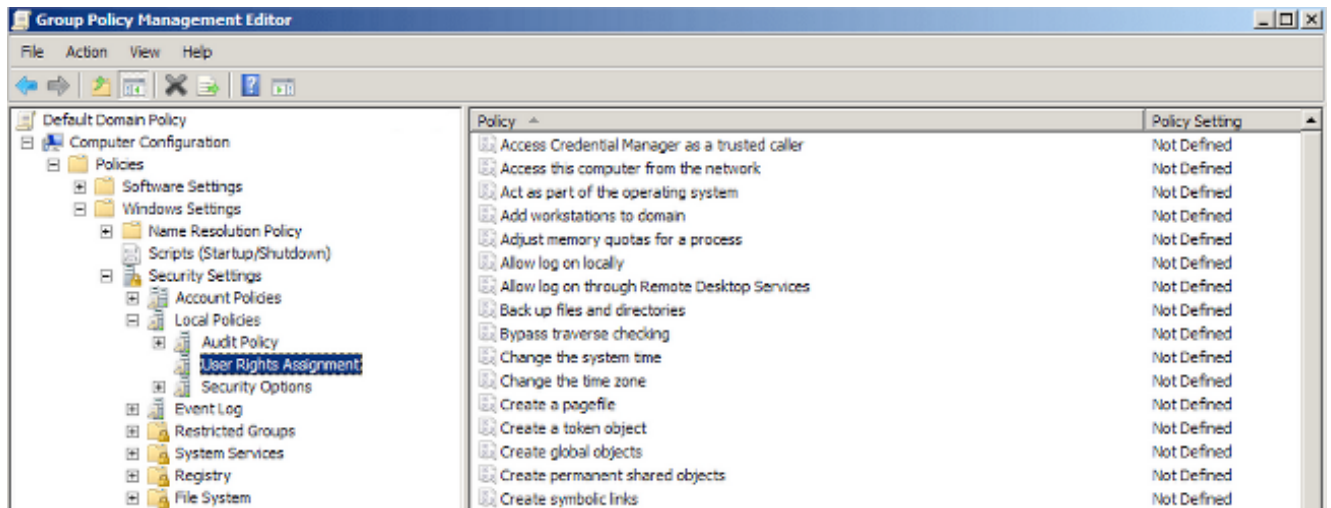
Les étapes suivantes appliquent à des Windows Server courants 2008 R2 de contrôleur de domaine :

Attention : Il est de votre responsabilité d'assurer la configuration correcte de stratégie de groupe sur les Windows Server. Cisco n'est pas responsable d'aucune question provoquée par des configurations incorrectes de stratégie de groupe.

1. Allez au **début** > aux **outils d'administration** > à la **Gestion de stratégie de groupe**.
2. Développez la **forêt** > les **domaines** > le *Your_Domain_Name* > les **objets de stratégie de groupe**.



3. Cliquez avec le bouton droit sur la stratégie que vous souhaitez modifier et choisir « **éditez** ».
4. Naviguez vers la **configuration de l'ordinateur** > les **stratégies** > les **paramètres de windows** > les **paramètres de sécurité** > **affectation locale de stratégies** > de **droits des utilisateurs**.



5. Double-cliquer sur le **login comme traitement par lots**.

6. Choisi **ajoutez l'utilisateur ou le groupez**.

7. Le clic **parcourent**, puis écrivent le nom désiré d'utilisateur ou de groupe.

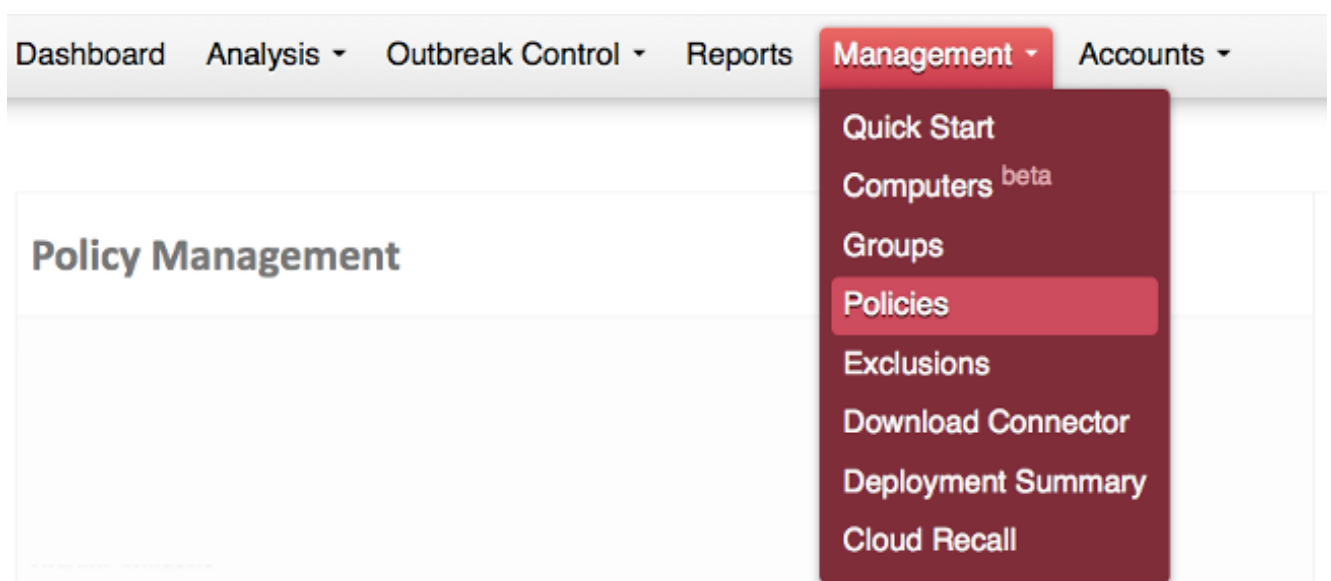
8. **Nom de contrôle de clic** pour le faire valider.

9. Cliquez sur en fonction **CORRECT** jusqu'à ce que vous reveniez à l'**éditeur de Gestion de stratégie de groupe**.

Appliquez-vous la stratégie de groupe à votre domaine ou la groupez s'il n'est pas déjà appliqué. Maintenant que nous avons configuré le compte utilisateur, nous configurerons le balayage dans le tableau de bord de FireAMP.

1. Procédure de connexion au tableau de bord de FireAMP.

2. Naviguez vers la **Gestion > les stratégies**.



3. Éditez la stratégie désirée.

4. Naviguez vers l'onglet de **fichier** > des **balayages programmés**. Écrivez un nom d'utilisateur et mot de passe.

General File Network

Modes i ▶

Offline Engine - TETRA i ▶

Cache Settings ▶

Engines i ▶

ETHOS i ▶

Cloud Policy ▶

Scheduled Scans ▶

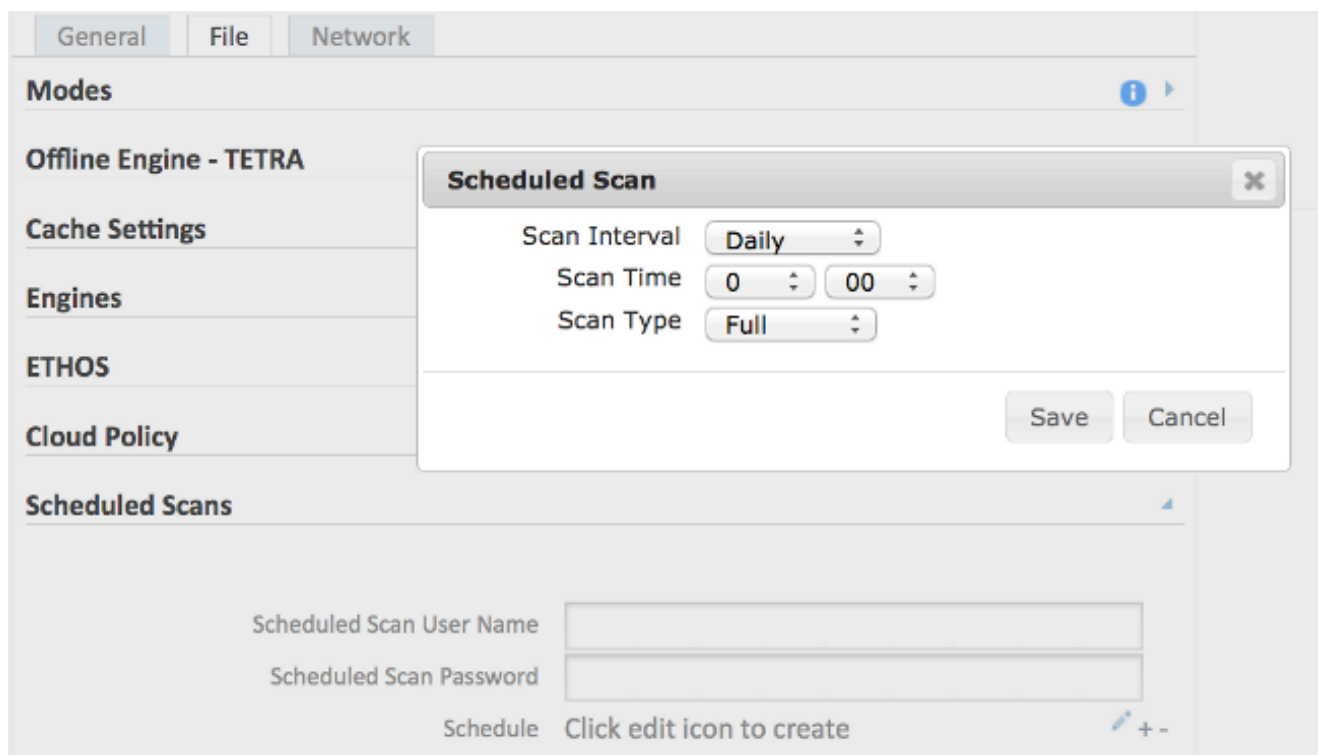
Scheduled Scan User Name

Scheduled Scan Password

Schedule [Click edit icon to create](#) ✎ + -

Remarque: Le nom d'utilisateur doit être dans le format de `domaine \ nom d'utilisateur`. Le suffixe de domaine n'est pas nécessaire.

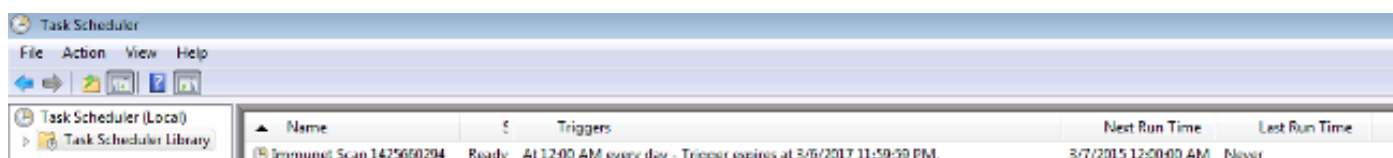
5. Configurez le programme. Utilisez le crayon, plus et sans des icônes pour modifier, ajoutent, enlèvent des programmes de balayage. Vous pouvez écrire de plusieurs programmes ici. Vous pouvez sélectionner quotidien, hebdomadaire, ou le mensuel en plus des 24 temps d'heure pour initier le balayage. Vous pouvez également choisir le type de balayage (éclair ou plein).



6. La sauvegarde choisie sélectionnent alors la mise à jour pour commettre les changements de politique.

Vérification

Après que les stratégies soient mises à jour sur les ordinateurs, vous devriez voir un ou plusieurs tâches dans le programmeur de tâche de Windows avec le nom **Immunit** comme le tir d'écran ci-dessous :



Dépannage

La stratégie est mise à jour, mais une tâche programmée n'est pas trouvée

Si votre stratégie met à jour mais vous ne voyez pas une tâche programmée, c'est très probablement due au compte que vous avez utilisé avoir le mot de passe incorrect, ou à l'autorisation insuffisante de créer des tâches (pas administrateur).

La tâche est créée, mais ne s'exécute pas

Si la tâche est créée, mais ne s'exécute pas, le compte très probablement n'a pas la capacité d'ouvrir une session en tant que lot. Veuillez passer en revue les étapes ci-dessus de configuration pour s'assurer que votre compte est configuré correctement.