

FireAMP/エンドポイント向け AMP でスケジュール済みスキャンを開始する

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[はじめに](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[ポリシーは更新済ですが、定期タスクはありません](#)

[タスクは作成されますが、動作しません](#)

概要

FireAMP 毎日の、ウィークリー、または毎月必要条件によるスケジュールされたスキャンをできます。スケジュールされたスキャンを作成するとき、マシンに管理上のユーザーの資格情報を提供する必要があります。この資料は正常なスケジュールされたスキャン用のユーザアカウントの必要なアクセス許可をアドレス指定します。

前提条件

要件

- FireAMP ダッシュボードへのアクセス
- Windows パソコンの管理者 アカウントのための信任状
- Windows XP またはそれ以降のための FireAMP 3.x -スケジュールされたスキャン
- Windows XP またはそれ以降のための FireAMP 4.x -スケジュールされたスキャンおよびエンドポイント IOC スキャン

はじめに

FireAMP ポリシーのスケジュールされたスキャンを追加するとき、ポリシー シリアル番号を高めます。エンドポイントはハートビートを送信するとき新しいポリシーをおろします。供給された信任状を使用する、FireAMP は Windows 内の定期タスクを、およびそれ以降実行しますタスクを作成します。このような理由で、私達使用するアカウントに正しい許可があることを確かめる必要があります設計して下さい。

スケジュールされる設定する前に、そのスキャンは使用するために計画するユーザアカウントのための2つの主要な必要条件です。

注: これらの権限はまたエンドポイント IOC スキャン用に適用します。

1. アカウントは管理者アカウントである必要があります。これはローカルなシステム管理者またはドメイン管理者である可能性があります。
2. アカウントはバッチとしてログオンできる必要があります。

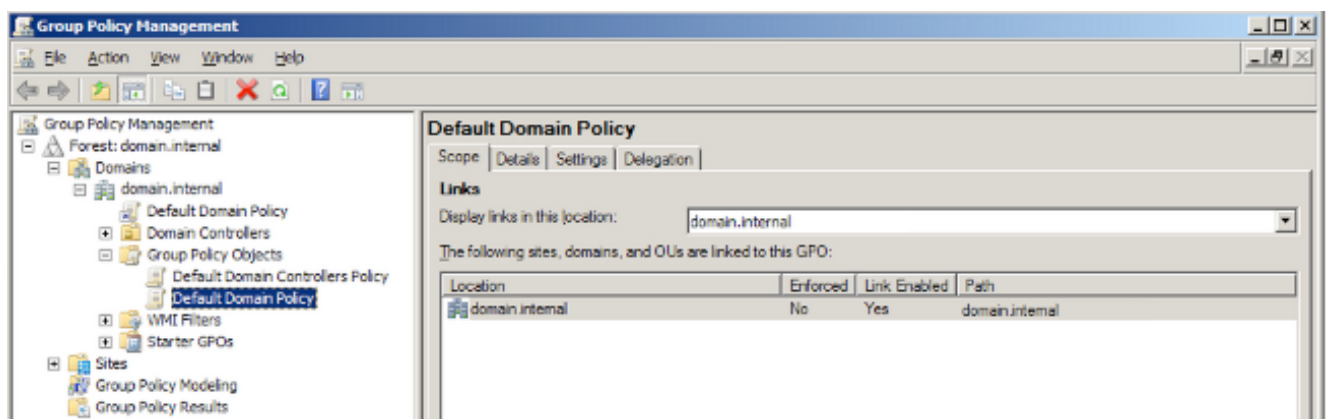
バッチ権限としてログオンはグループポリシーによって設定されます。これがドメインのために設定されない場合、管理者アカウントはバッチとしてログオンデフォルトでできるはずですが、それがドメインのために設定される場合、アカウントはグループポリシーオブジェクト (GPO) の内で定義されるグループに属する必要があります。

設定

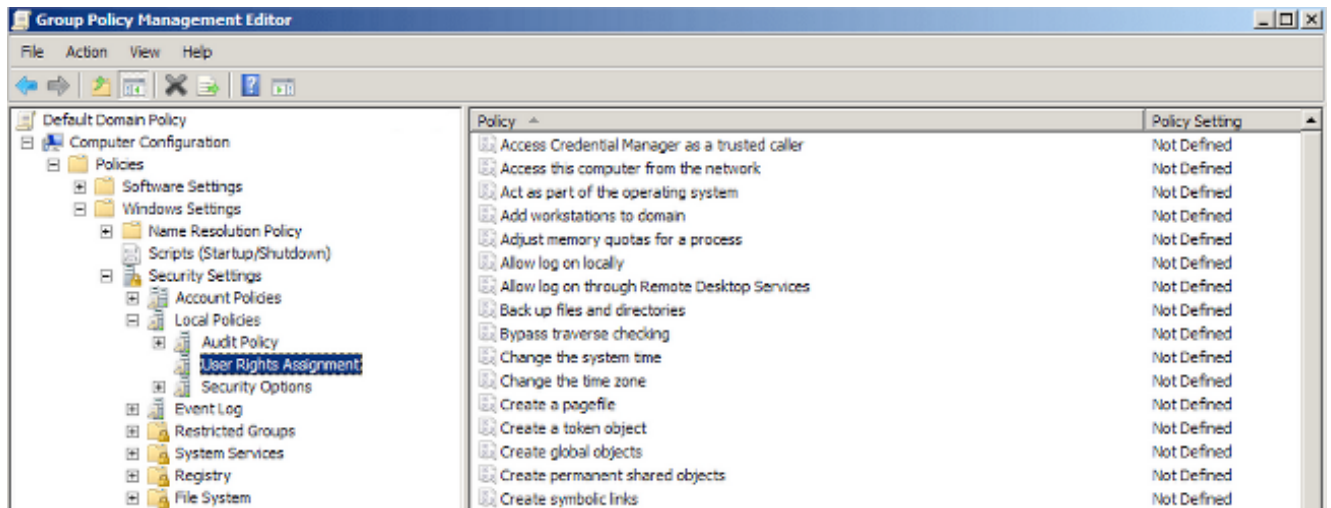
次のステップは Windows サーバ 2008 R2 を実行しているドメインコントローラに適用されます:

注意: それは Windows サーバの正しいグループポリシー設定を確認する責任です。Cisco は不正確なグループポリシー設定によって引き起こされるあらゆる問題に責任がありません。

1. Start > Administrative Tools > グループポリシー管理に行ってください。
2. フォレスト > ドメイン > *Your_Domain_Name* > グループポリシーオブジェクトを拡張してください。



3. 修正し、"Edit"を選択するたいポリシーの右クリック。
4. 計算機構成 > ポリシー > ウィンドウに設定 > Security 設定 > ローカルポリシー > ユーザ権限割り当てナビゲートして下さい。



5. 一括 ジョブとしてログオンでダブル クリックして下さい。

6. ユーザかグループを『Add』 を選択して下さい。

7. 『Browse』 をクリックし、そして望ましいユーザかグループ名を入力して下さい。

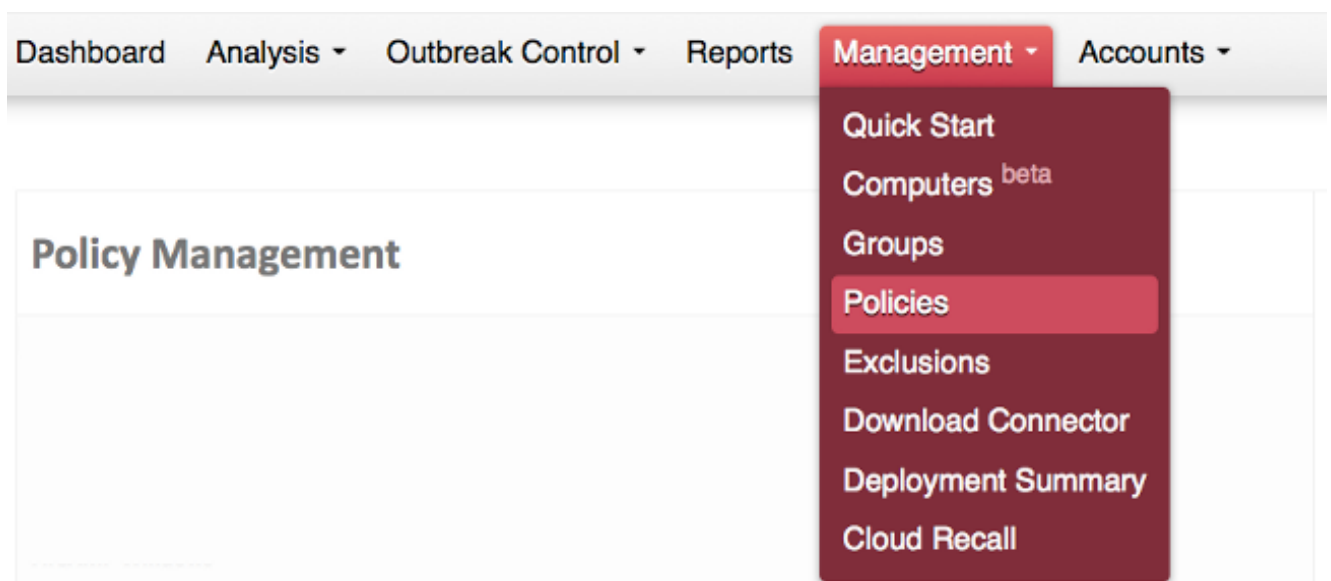
8. それを検証してもらうために『Check Name』 をクリックして下さい。

9. グループ ポリシー管理エディタに到達するまで『OK』 をクリックして下さい。

まだ適用していない場合グループ ポリシーをドメインに適用するか、またはグループ化して下さい。 ユーザアカウントを設定したので、FireAMP ダッシュボードのスキャンを設定します。

1. FireAMP ダッシュボードへのログイン。

2. [Management] > [Policies] に移動します。



3. 望ましいポリシーを編集して下さい。

4. File タブに > スケジュールされたスキャン ナビゲートして下さい。 ユーザ名とパスワードを入力します。

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 ✎ +-

注: ユーザーネームは \ 形式にある必要があります。ドメインサフィックスは必要ではありません。

5. スケジュールを設定して下さい。修正するのにアイコンとおよび引く鉛筆を、追加したり、取除きますスキャン スケジュールを使用して下さい。複数のスケジュールをここに入力することができます。スキャンを始める時間時間 24 に加えて、または毎月週間毎日を選択できます。またスキャン型を選択できます (フラッシュが完全)。

General File Network

Modes i ▶

Offline Engine - TETRA

Cache Settings

Engines

ETHOS

Cloud Policy

Scheduled Scans ▶

Scheduled Scan ✕

Scan Interval

Scan Time

Scan Type

Scheduled Scan User Name

Scheduled Scan Password

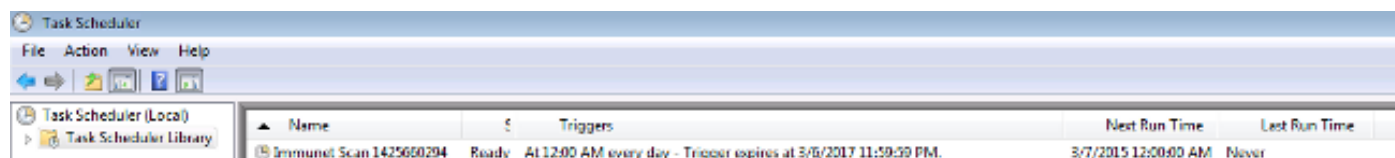
Schedule Click edit icon to create ✎ +-

6. それからポリシーの変更を保存するために『Update』 を選択 します 『SAVE』 を選択 し

て下さい。

確認

ポリシーがマシンでアップデートされた後、下記のようにスクリーンショットのような名前 Immnet の Windows タスク スケジューラの 1つ以上のタスクを参照するはずですが:



トラブルシューティング

ポリシーは更新済ですが、定期タスクはありません

ポリシーがアップデートすればが、定期タスクを参照しなければタスク (ない管理者) を作成する、これは間違ったパスワードを持っていることを使用したアカウント、または不十分な権限が多分原因です。

タスクは作成されますが、動作しません

タスクが作成されるが、動作しなければアカウントに多分バッチとしてログオンする機能がありません。アカウントが正しく設定されるようにするために上記のコンフィギュレーションのステップを確認して下さい。