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

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。 この資料によって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が当たります。

前提条件

要件

- FireAMP ダッシュボードへのアクセス
- Windows PC の管理者 アカウントのための資格情報
- 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。 供給された資格情報を使用する、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、私達持っている正しい 許可を使用するアカウント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、そこ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。

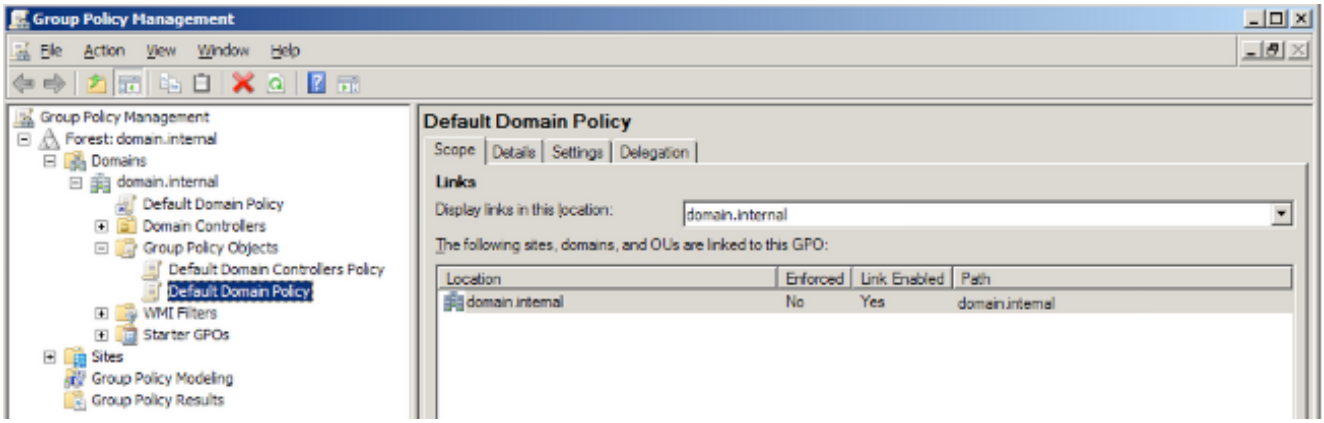
バッチ権限**としてログインは**グループ ポリシーによって設定されます。 これがドメインのために設定されない場合、管理者アカウントはバッチとしてログオン デフォルトでできるはずです。 それがドメインのために設定される場合、アカウントはグループ ポリシー オブジェクト（GPO）の内で定義されるグループに属する必要があります。

設定

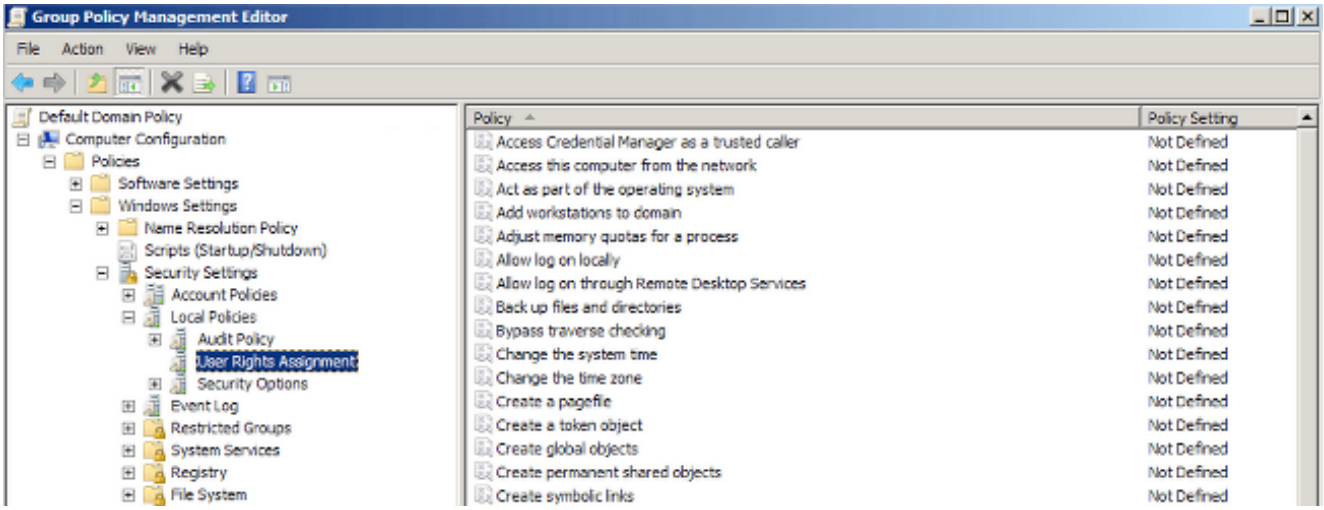
次のステップは Windows サーバ 2008 R2 を実行しているドメインコントローラに適用されます:

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 コンフィギュレーション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**に行って下さい。
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**拡張して下さい。



3. 修正し、"Edit"を 選択するたいポリシーの右クリック。
4. **設定** > Security **設定 > ローカル ポリシー > ユーザ 権限 割り当ては計算機構成 > ポリシー** > ウィンドウにナビゲート します。



5. **一括 ジョブとしてログイン**のダブル クリック。

6. **ユーザを**『Add』 を選択 するか、**またはグループ化して下さい。**

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。

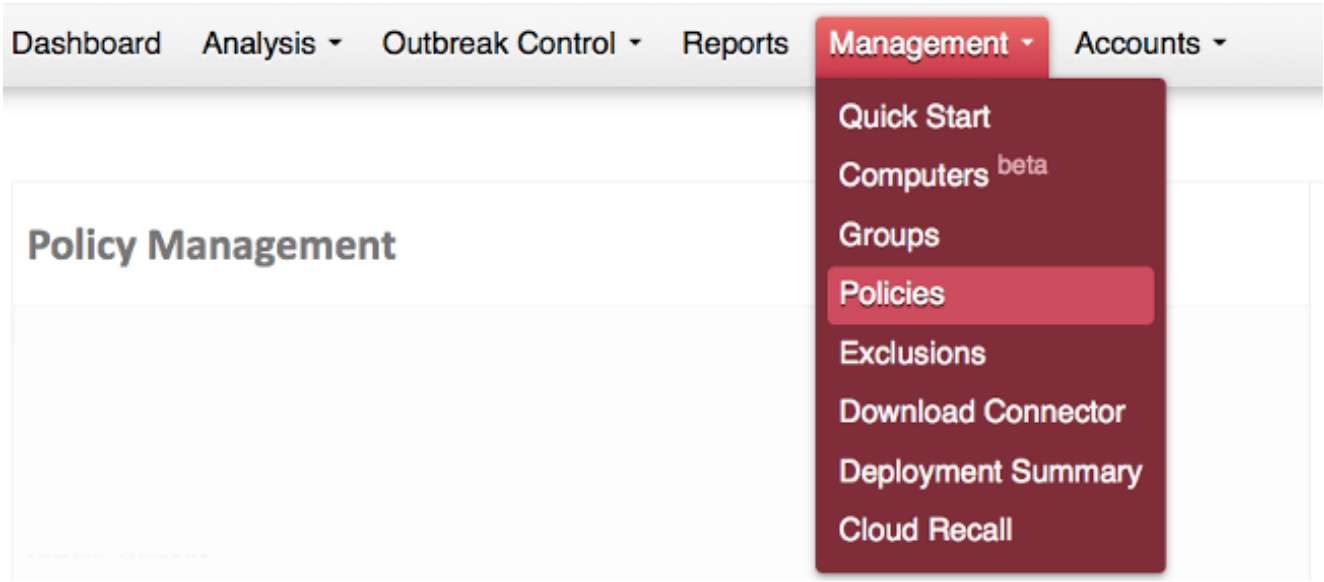
8. それを検証してもらうために『Check Name』 をクリック して下さい。

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。

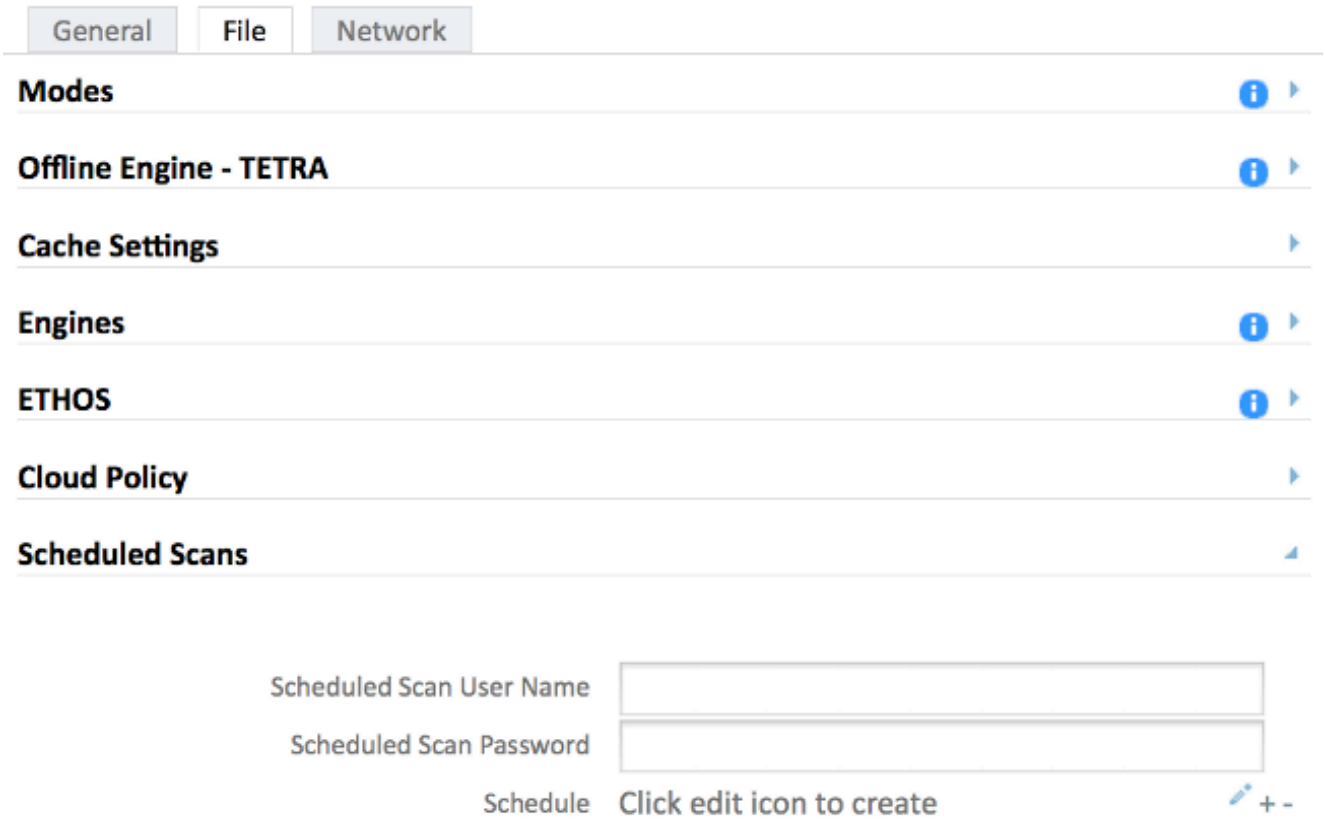
1. FireAMP ダッシュボードへのログイン。

2. [Management] > [Policies] に移動します。



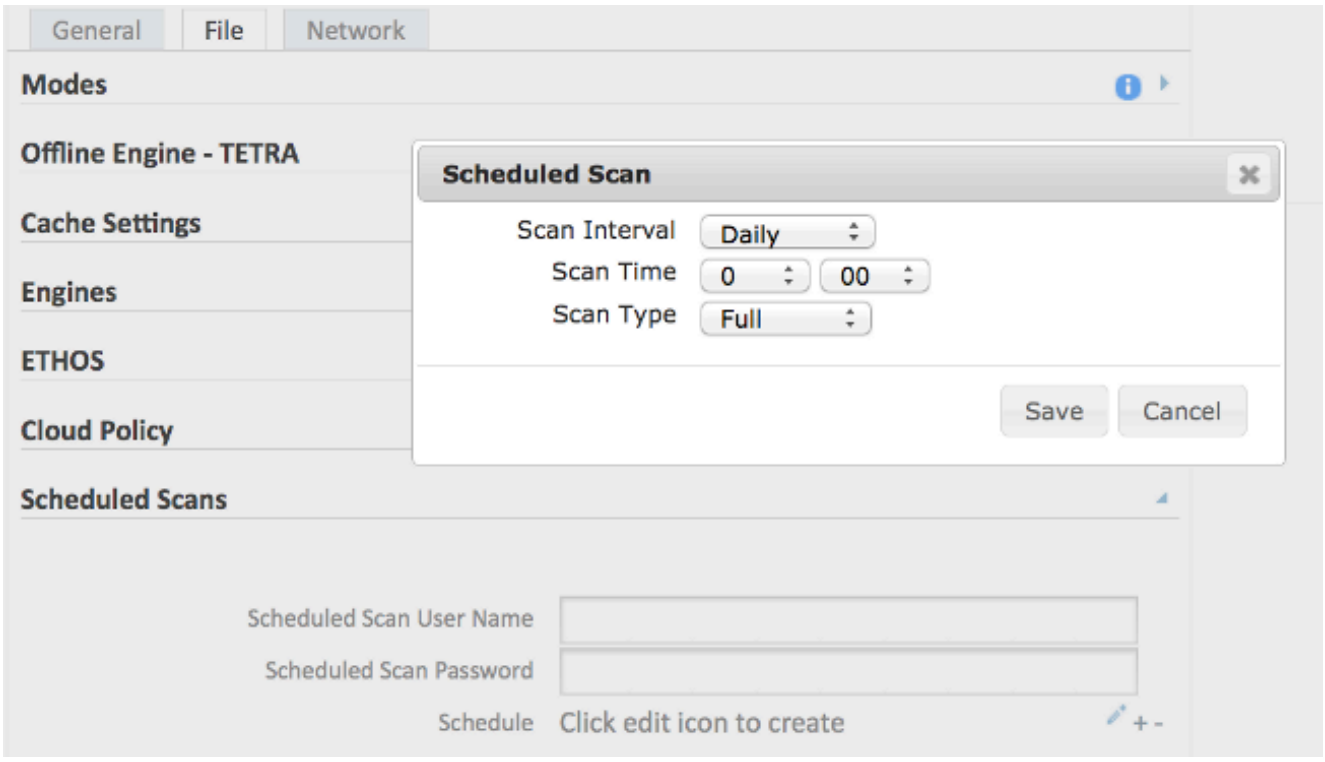
3. 望ましいポリシーを編集して下さい。

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



注: ユーザネームは\ 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ないです。

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、追加しましたり、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 (フラッシュするか完全) 。

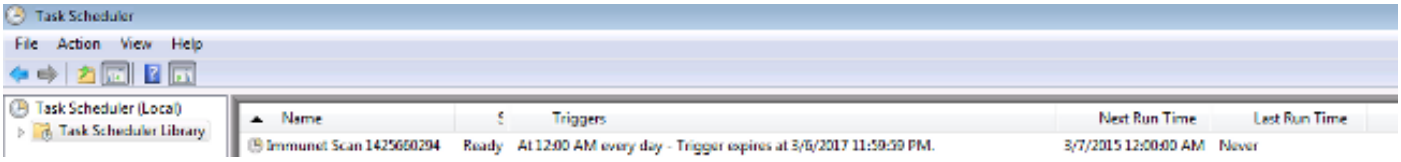


6. それからポリシーの変更を保存するために『Update』 を選択 します 『SAVE』 を選択 し

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 ショットのようなネーム **Immunet** 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:



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。