O novato programado faz a varredura em FireAMP/AMP para valores-limite

Índice

Introdução

Você pode executar varreduras programadas em FireAMP diário, em semanário, ou mensalmente segundo suas exigências. Quando você cria varreduras programadas, você precisa de fornecer credenciais administrativas do usuário para suas máquinas. Este documento endereça as permissões exigidas do usuário esclarece varreduras programadas bem sucedidas.

Pré-requisitos

Requisitos

- Acesso ao painel de FireAMP
- As credenciais para um administrador esclarecem Windows PC
- FireAMP 3.x para Windows XP ou mais tarde - Varreduras programadas
- FireAMP 4.x para Windows XP ou mais tarde - Varreduras programadas e varreduras do valor-limite IOC

Antes de Começar

Quando você adiciona uma varredura programada em uma política de FireAMP, aumenta o número de série da política. Os valores-limite puxam para baixo a política nova quando enviam a pulsação do coração. Usando as credenciais fornecidas, FireAMP cria uma tarefa programada dentro de Windows, e executa mais tarde a tarefa. Devido a este projeto, nós precisamos de certificar-se de que a conta que nós nos usamos tem as permissões correta.

Antes que nós configuremos programado, a varredura lá é duas exigências principais para uma conta de usuário que você planeie usar.

> **Note**: Estas permissões igualmente aplicam-se para varreduras do valor-limite IOC.

1. A conta deve ser uma conta de administrador. Este poderia ser um administrador local ou um administrador de domínio.
2. A conta deve poder **entrar como o grupo**.

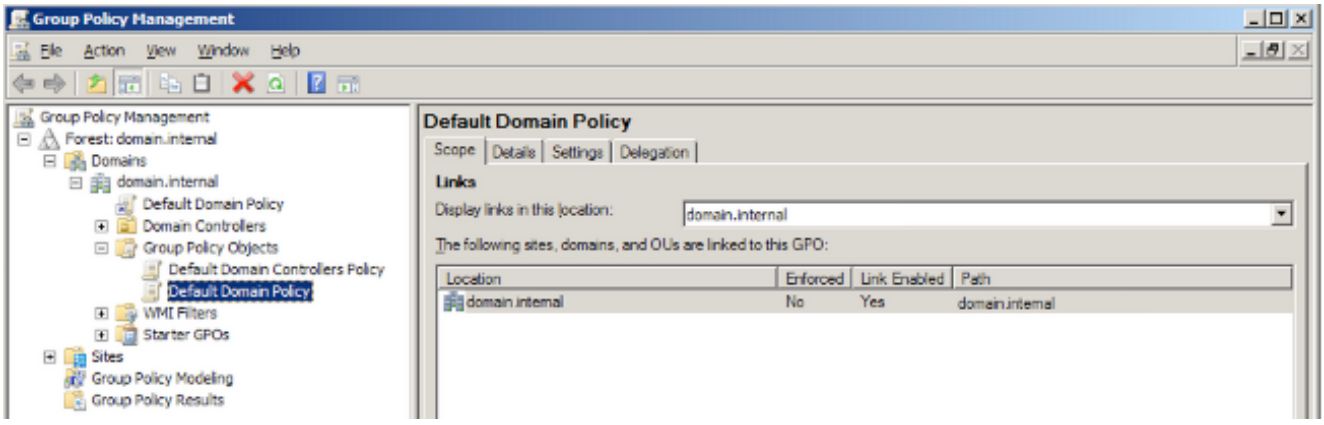
O fazer logon como a permissão do **grupo** é configurado através da política do grupo. Se isto não é configurado para seu domínio, a seguir as contas administrativas à revelia devem poder entrar como o grupo. Se é configurado para seu domínio, a conta deve pertencer a um grupo definido dentro do objeto da política do grupo (GPO).

Configuração

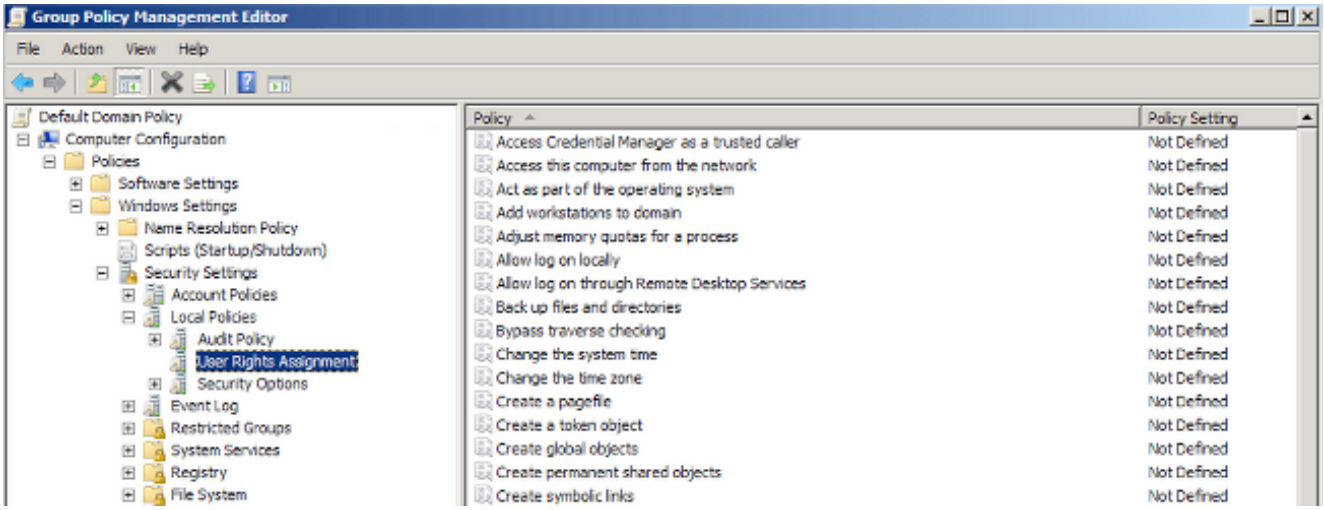
As seguintes etapas aplicam-se a um controlador de domínio que executa Windows Server 2008 R2:

> **Caution**: É sua responsabilidade assegurar a configuração das normas correta do grupo no Windows Server. Cisco não é responsável para nenhuma edições causada por configurações das normas incorretas do grupo.

1. Vá ao **Iniciar > Ferramentas Administrativas >** ao **Gerenciamento de políticas do grupo**.
2. Expanda a **floresta >** os **domínios >** o *Your_Domain_Name* **>** os **objetos da política do grupo**.



3. Clicar com o botão direito na política que você deseja alterar e para escolher “**edite**”.
4. Navegue à **configuração de computador >** às **políticas >** aos **ajustes do >** segurança dos **ajustes de Windows >** às **políticas local >** à **atribuição dos direitos do usuário**.



5. Fazer duplo clique no **fazer logon como tarefas de lote**.

6. Seleto **adicionar o usuário ou o grupo**.

7. O clique **consulta**, a seguir dá entrada com o usuário ou o nome do grupo desejado.

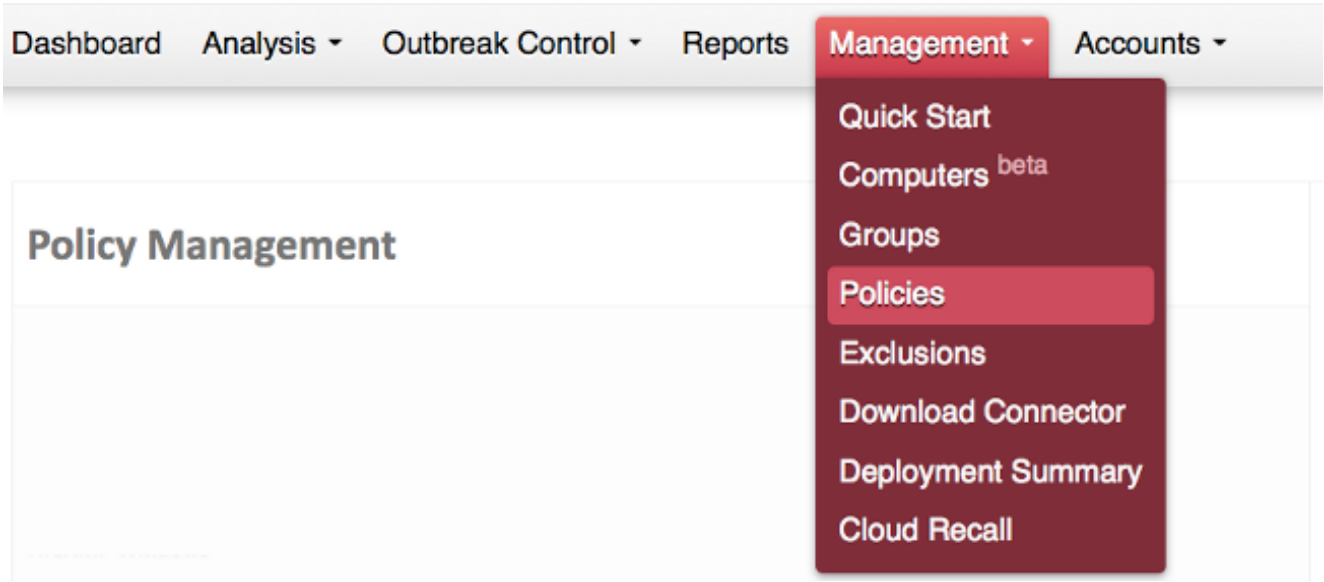
8. **Nome da verificação do** clique para tê-lo validado.

9. Clique sobre a **APROVAÇÃO** até que você receba de volta ao **editor do Gerenciamento de políticas do grupo**.

Aplique a política do grupo a seu domínio ou agrupe-a se não é já aplicado. Agora que nós configuramos a conta de usuário, nós configuraremos a varredura no painel de FireAMP.

1. Início de uma sessão ao painel de FireAMP.

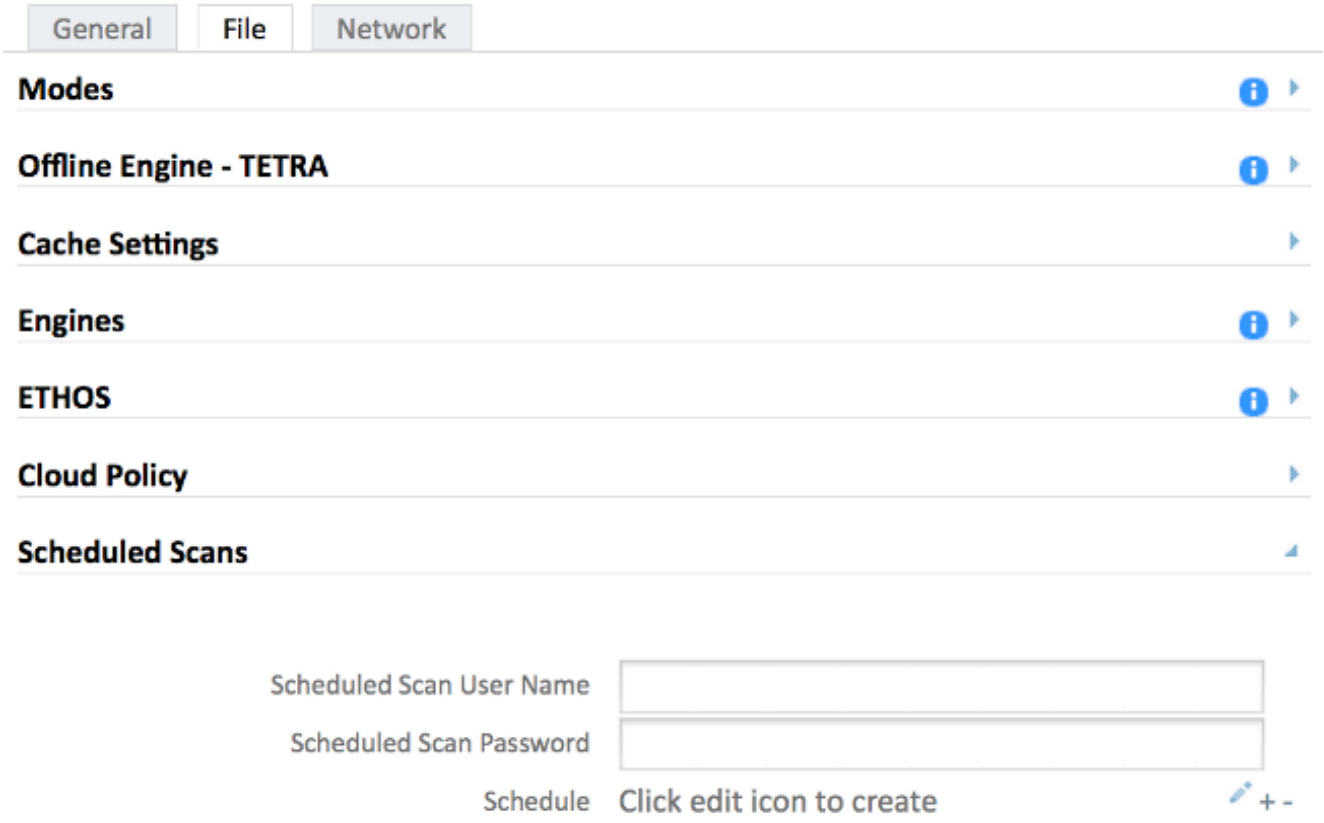
2. Navegue ao **Gerenciamento** > às **políticas**.



3. Edite a política desejada.

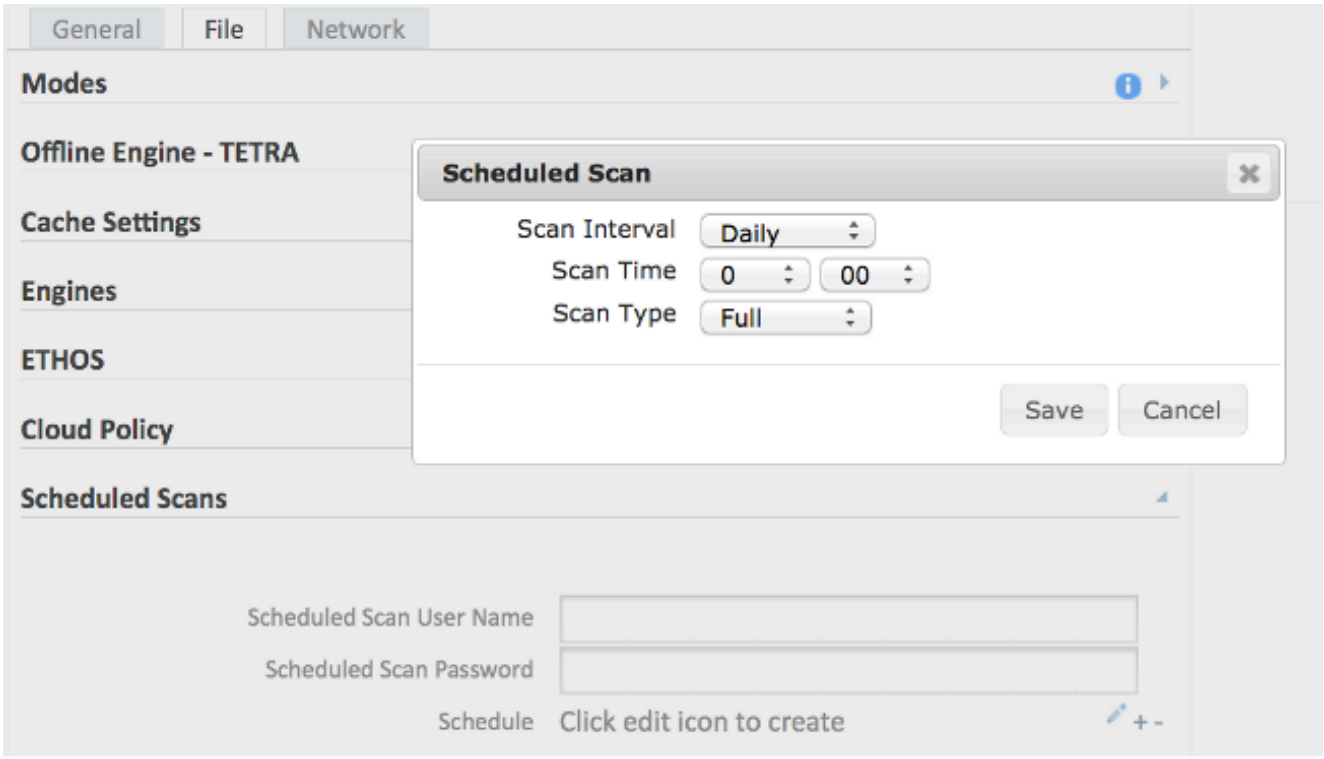
4. Navegue à aba do **arquivo > varreduras programadas**. Incorpore um nome de usuário e

senha.



Note: O nome de usuário deve estar no formato do `domínio \ username`. O sufixo de domínio não é necessário.

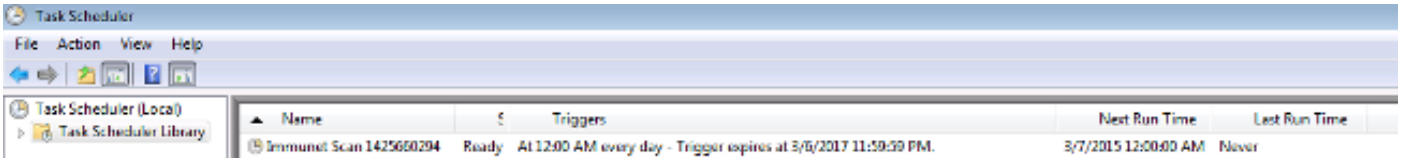
5. Configurar a programação. Use o lápis, mais e menos ícones para alterar, adicionam, removem programações da varredura. Você pode incorporar programações múltiplas aqui. Você pode selecionar ou diário, semanal, ou mensalmente além do que umas 24 estadias da hora iniciar a varredura. Você pode igualmente escolher o tipo da varredura (flash ou completo).



6. **A salvaguarda** seleta seleciona então a **atualização** para comprometer as alterações de política.

Verificação

Depois que as políticas são atualizadas nas máquinas, você deve ver umas ou várias tarefas no task scheduler de Windows com o nome **Immunet** como o tiro de tela abaixo:



Troubleshooting

A política é atualizada, mas uma tarefa programada não é encontrada

Se sua política atualiza mas você não vê uma tarefa programada, esta é muito provavelmente devido à conta que você usou ter a senha errada, ou à permissão insuficiente criar tarefas (não administrador).

A tarefa é criada, mas não é executado

Se a tarefa é criada, mas não é executado, a conta muito provavelmente não tem a capacidade **para entrar como o grupo**. Reveja por favor as etapas de configuração acima para assegurar-se de que sua conta esteja configurada corretamente.