El iniciado programado analiza en FireAMP/amperio para los puntos finales

Contenido

Introducción

Usted puede funcionar con las exploraciones programadas en FireAMP diario, el semanario, o mensualmente dependiendo de sus requisitos. Cuando usted crea las exploraciones programadas, usted necesita proporcionar las credenciales del usuario administrador para sus máquinas. Este documento dirige los permisos requeridos del usuario explica las exploraciones programadas acertadas.

Prerrequisitos

Requisitos

- Acceso al panel de FireAMP
- Las credenciales para un administrador explican Windows PC
- FireAMP 3.x para Windows XP o más adelante - Exploraciones programadas
- FireAMP 4.x para Windows XP o más adelante - Exploraciones programadas y exploraciones del punto final IOC

Antes de comenzar

Cuando usted agrega una exploración programada en una directiva de FireAMP, aumenta el número de serie de la directiva. Los puntos finales tiran hacia abajo la nueva directiva cuando envían el latido del corazón. Usando las credenciales suministradas, FireAMP crea una tarea programada dentro de Windows, y posterior ejecuta la tarea. Debido a este diseño, necesitamos

aseegurarnos que la cuenta que utilizamos tenga los permisos correctos.

Antes de que configuremos haber programado, la exploración allí es dos requisitos principales para una cuenta de usuario que usted planee utilizar.

> Nota: Estos permisos también solicitan las exploraciones del punto final IOC.

1. La cuenta debe ser una cuenta del administrador. Esto podría ser administrador local o administrador de dominio.
2. La cuenta debe poder **abrir una sesión como lote**.

El inicio como permiso del **lote** se configura vía la directiva del grupo. El si esto no está configurado para su dominio, entonces las cuentas administrativas por abandono debe poder abrir una sesión como lote. Si se configura para su dominio, la cuenta debe pertenecer a un grupo definido dentro del objeto de la directiva del grupo (GPO).

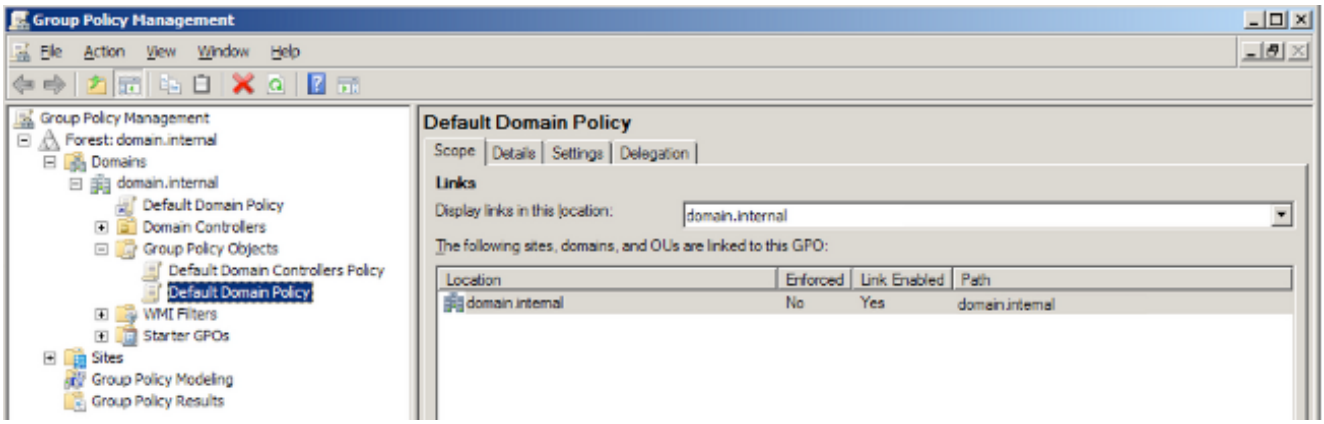
Configuración

Los pasos siguientes se aplican a un r2 corriente 2008 del Servidor Windows del controlador de dominio:

> Precaución: Es su responsabilidad asegurar la configuración de la política correcta del grupo en el Servidor Windows. Cisco no es responsable de ninguna problemas causada por las configuraciones de la política incorrectas del grupo.

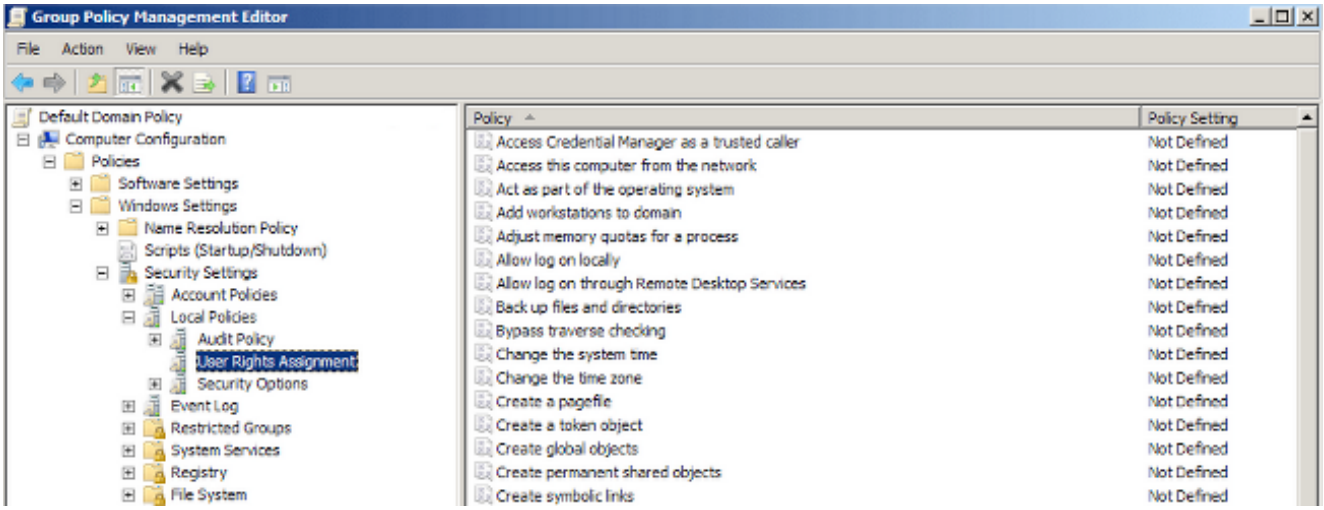
1. Vaya al **Start (Inicio) > Administrative Tools (Herramientas administrativas) >** a la **Administración de políticas del grupo**.

2. Amplíe el **bosque >** los **dominios >** el *Your_Domain_Name* **>** los **objetos de la directiva del grupo**.



3. Haga clic con el botón derecho del ratón en la directiva que usted desea modificarse y elegir "**edite**".

4. Navegue a la **configuración de Computadora >** a las **directivas >** a las **políticas locales >** a la **asignación de derechos de usuario del >** Security (Seguridad) de las **configuraciones de Windows las configuraciones >**.



5. El doble hace clic en la **conexión a la comunicación como trabajo en lote**.

6. Selecto **agregue el usuario o al grupo**.

7. El tecleo **hojea**, después ingresa el usuario o el nombre del grupo deseado.

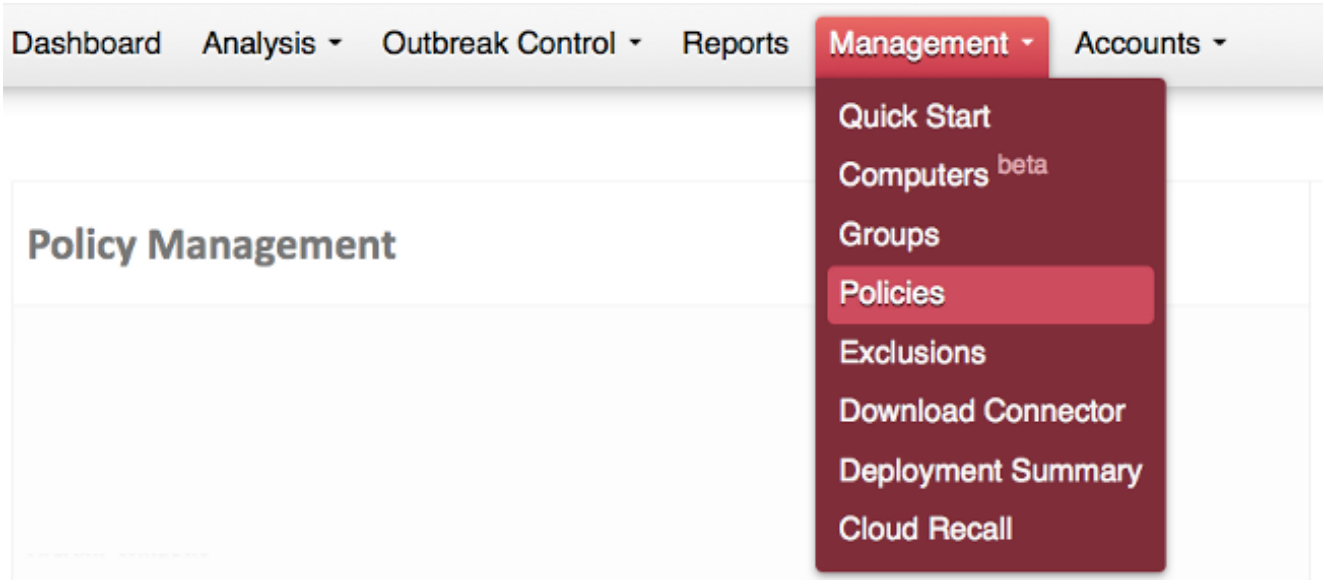
8. **Nombre del control del** tecleo hacerlo validar.

9. Haga clic en **OK** hasta que usted vuelva al **editor de la Administración de políticas del grupo**.

Aplique la directiva del grupo a su dominio o agrúpela si no es ya aplicado. Ahora que hemos configurado la cuenta de usuario, configuraremos la exploración en el panel de FireAMP.

1. Login al panel de FireAMP.

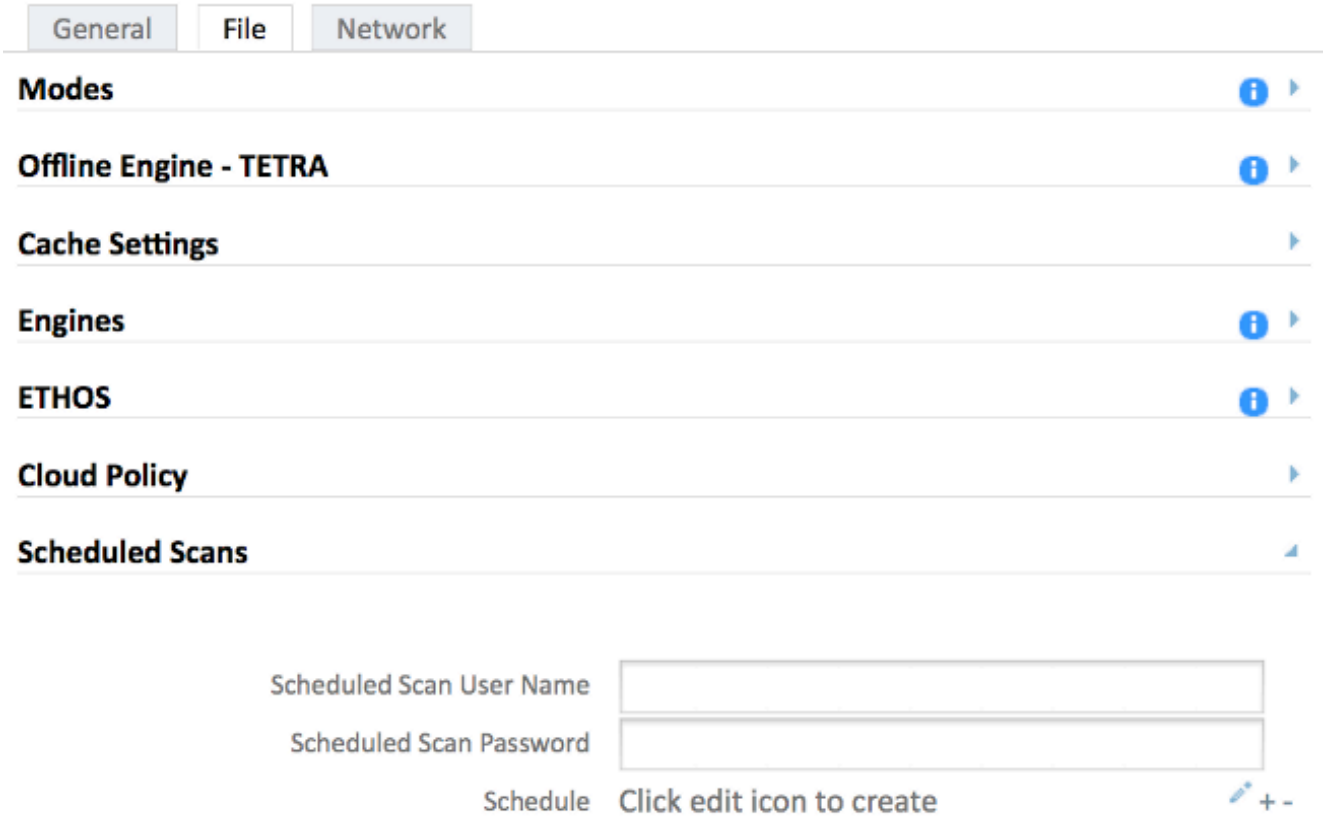
2. Navegue a la **Administración** > a las **directivas**.



3. Edite la directiva deseada.

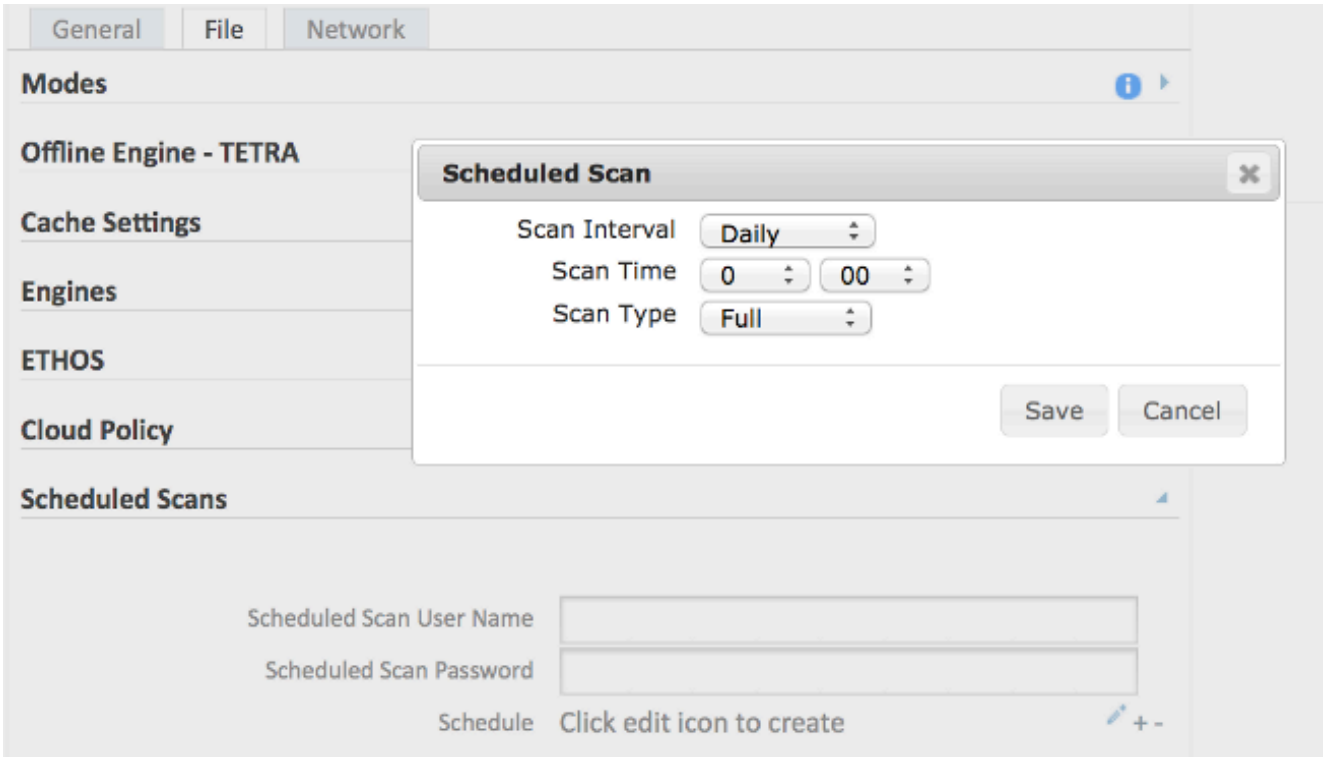
4. Navegue a la lengueta del **archivo** > las **exploraciones programadas**. Ingrese un nombre de

usuario y contraseña.



Nota: El Nombre de usuario debe estar en el formato del `dominio \ del nombre de usuario`. El sufijo del dominio no es necesario.

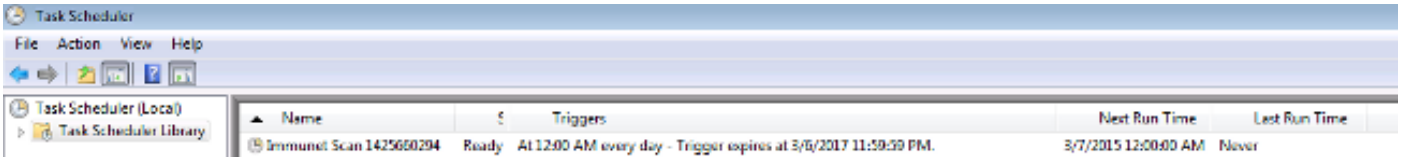
5. Configure el horario. Utilice el lápiz, más y menos los iconos para modificarse, agregan, quitan los horario de la exploración. Usted puede ingresar los horario múltiples aquí. Usted puede seleccionar o diario, semanal, o mensualmente además de los 24 ratos de la hora de iniciar la exploración. Usted puede también elegir el tipo de la exploración (Flash o lleno).



6. **La salvaguardia** selecta entonces selecciona la **actualización** para confiar los cambios de política.

Verificación

Después de que las directivas se pongan al día en las máquinas, usted debe ver una o más tareas en el Programador de tareas de Windows con el nombre **Immunet** como el tiro de pantalla abajo:



Resolución de problemas

La directiva es actualizada, pero una tarea programada no se encuentra

Si su directiva se pone al día pero usted no ve una tarea programada, esto es muy probablemente debido a la cuenta que usted utilizó tener la contraseña incorrecta, o al permiso insuficiente de crear las tareas (no administrador).

La tarea se crea, pero no puede ejecutarse

Si la tarea se crea, pero no puede ejecutarse, la cuenta no tiene muy probablemente la capacidad **de abrir una sesión como lote**. Revise por favor los pasos para la configuración antedichos para asegurarse de que su cuenta está configurada correctamente.