Despliegue de Cisco AMP para las puntos finales con la persistencia de la identidad

Contenido

Introducción

Este documento describe que cómo la característica de la persistencia de la identidad en Cisco avanzó la protección de Malware (AMP) para las puntos finales permite que un Identificador único del objeto del ordenador universal (UUID) sea reutilizado cuando un ordenador o una máquina virtual (VM) reimaged o se cambia de frente. Esto previene la creación de los objetos duplicados del ordenador en un panel, y mantiene los datos contiguos para esos objetos del ordenador. Esto también ayuda a mantener los conectores de la punto final, a proporcionar a la continuidad de los datos, y a mantener la cuenta de la licencia el control.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de este los temas:

- Acceso a Cisco AMP para el panel de las puntos finales
- Configure la persistencia de la identidad antes de que usted despliegue inicialmente el conector
- La persistencia de la identidad se utiliza solamente en el sistema operativo Windows (el OS)

Note: La característica de la persistencia de la identidad se debe activar con el centro de la asistencia técnica de Cisco (TAC).

Componentes usados

La información en este documento se basa en Cisco AMP para el panel de las puntos finales.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Flujo de trabajo

La opción de la persistencia de la identidad utiliza este el flujo de trabajo cuando éste es permiso:

1. La opción de la persistencia de la identidad se configura en una directiva.
2. El AMP para el instalador de las puntos finales se genera del panel y se despliega en un nuevo ordenador o VM.
3. Un nuevo objeto del ordenador se crea con un UUID y el indicador de la persistencia de la identidad.

- Control del registro

Cuando el servicio del conector comienza, se realiza el control del registro de la nube. El control del registro evalúa la información de la máquina por ejemplo, del hostname y de la dirección MAC actuales. También evalúa la configuración de la persistencia de la identidad en la directiva contra la nube para determinar si un nuevo UUID necesita ser generado.

- Criterios del registro

Un objeto del ordenador tiene un indicador ocultado fijado que corresponda a la configuración de la persistencia de la identidad usada. Este indicador, junto con la información única (hostname o dirección MAC) se utiliza para proporcionar al UUID existente a cualquier máquina que haga juego los criterios. Si un indicador y la información única de la máquina no hace juego con ningún objeto existente del ordenador, un nuevos UUID y objeto se generan para la máquina.

> **Note**: Cuando usted utiliza el hostname, se utiliza el nombre de dominio completo (FQDN). Si usted tiene una máquina nombrada **prueba** y otra máquina nombrada **test.domain.com**, no hacen juego, y el UUID no se reutiliza.

- Ordenadores móviles

El movimiento de los ordenadores entre los grupos con diversas configuraciones de la persistencia de la identidad crea los duplicados. Esto es debido a un indicador ocultado que se asocie a cada configuración de la persistencia de la identidad. Cuando las configuraciones no hacen juego, se generan los duplicados. Ambos grupos deben hacer la misma directiva aplicar cuando trabajan con **a través de las** configuraciones de la **directiva**. Si las configuraciones son lo mismo pero las directivas son diferentes, se crean los duplicados.

> **Note**: Si usted quiere reproducirse o imagen un ordenador con Cisco AMP para las puntos finales instaladas, lea este documento.

- Elección de la dirección MAC

Una máquina puede tener direcciones MAC múltiples, sin embargo, no es posible influenciar manualmente el proceso de elección de la dirección MAC durante el registro del conector. Usted debe utilizar las configuraciones de la dirección MAC solamente si usted puede garantizar que sus máquinas tienen solamente una dirección MAC, si no utiliza el hostname.

- Grupo predeterminado

La persistencia de la identidad se debe también configurar para la directiva aplicada a su grupo

predeterminado. En caso que supriman una directiva o a un grupo con una máquina activa, la máquina se coloca en el grupo predeterminado cuando un control del registro se realiza la vez próxima. Si la persistencia de la identidad no se configura para el grupo predeterminado, después se genera el objeto duplicado.

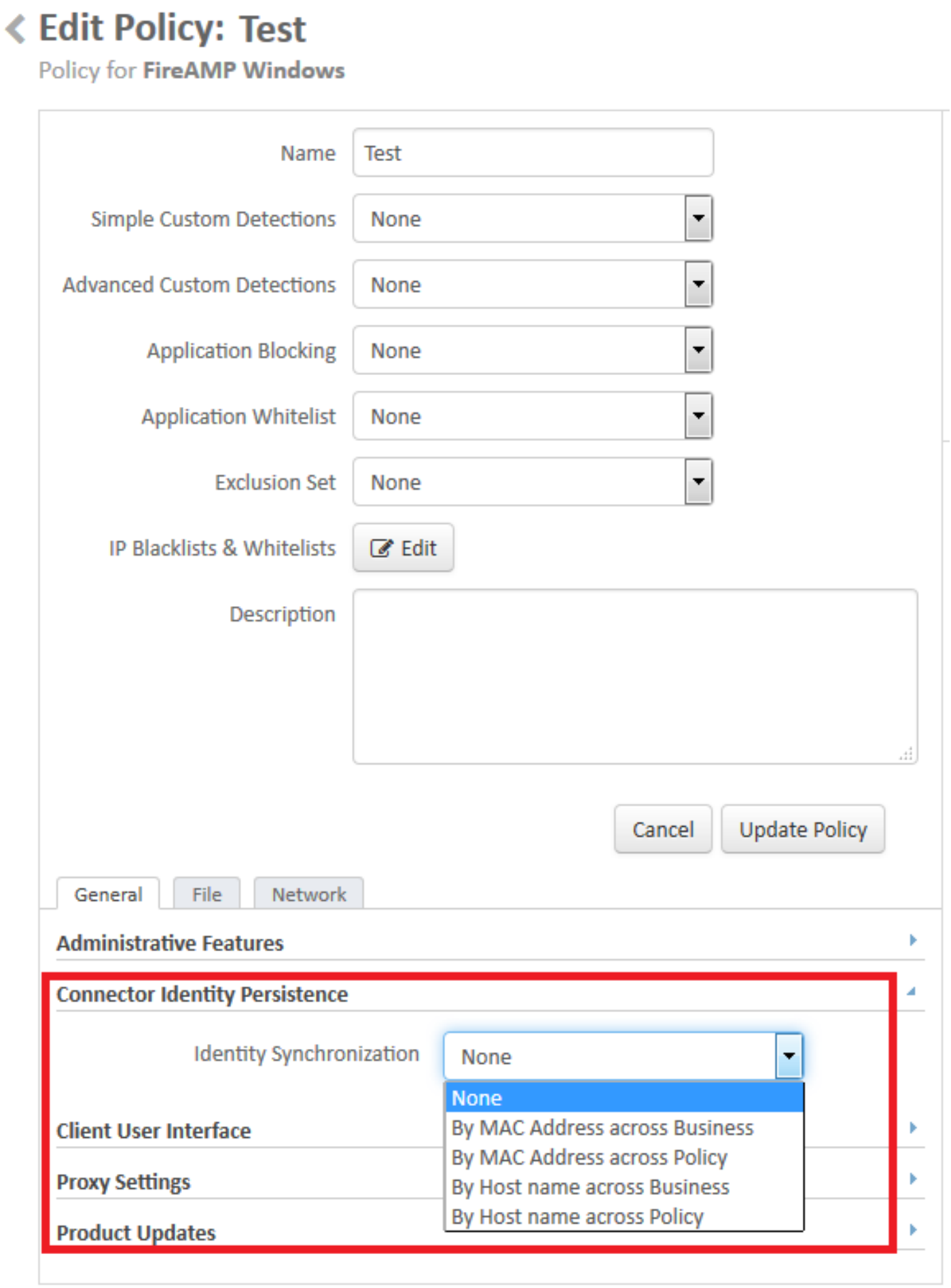
> **Note**: En algunos casos, una VM reproducida se pudo colocar en el grupo predeterminado bastante que el grupo que lo reprodujeron de. Si ocurre esto, trasládese la VM al grupo correcto en la consola de FireAMP.

Configurar

Siga los pasos aquí para desplegar el conector con la persistencia de la identidad:

Paso 1. Aplique la persistencia deseada de la identidad que fija a sus directivas:

- Navegue a la **Administración > a las directivas**
- Seleccione la directiva deseada. El tecleo **corrige**
- Navegue a la **ficha general**. Se selecciona, por abandono
- Seleccione la **persistencia de la identidad del conector**. **La sincronización de la identidad** cae abajo aparece tal y como se muestra en de la imagen.



Note: El enablement de una característica después de que la instalación de las puntos finales pueda hacer los objetos duplicados ser generado para cada máquina.

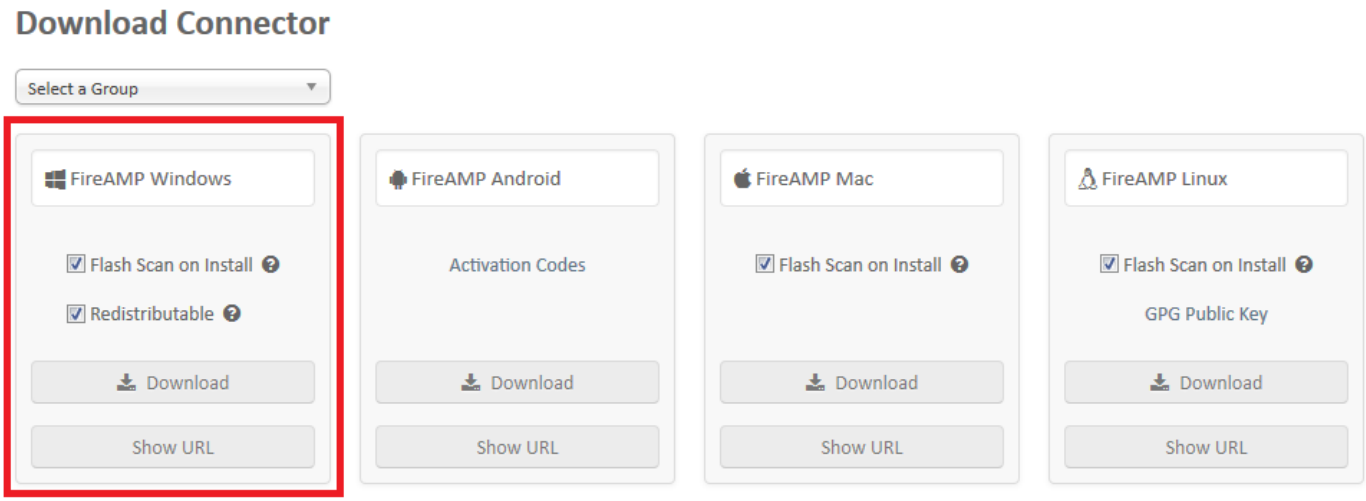
Seleccione una opción de la **sincronización de la identidad** que sea el mejor para su entorno. Estas opciones están disponibles:

- Ninguno: La característica no se activa. El conector UUIDs no se sincroniza con el nuevo conector instala bajo ninguna circunstancia. Cada nueva instalación genera un nuevo objeto de la máquina.
- Por la dirección MAC a través del negocio: Los nuevos conectores buscan el conector más reciente que tiene la misma dirección MAC para sincronizar a través de todas las directivas en el negocio que tengan sincronización de la identidad fijada a un valor con excepción de ningunos. Cuando está seleccionado, un objeto de la máquina se crea y se señala por medio de una bandera para sincronizar con cualquier máquina que utilice esa dirección MAC a través de la cuenta entera.
- Por la dirección MAC a través de la directiva: Los nuevos conectores buscan el conector más reciente que tiene la misma dirección MAC para sincronizar con dentro de la misma directiva. Cuando está seleccionado, un objeto de la máquina se crea y se señala por medio de una bandera para sincronizar con cualquier máquina que utilice esa dirección MAC y se asigna registrado contra la directiva específica.
- Por el nombre de host a través del negocio: Los nuevos conectores buscan el conector más reciente que tiene el mismo hostname para sincronizar con a través de todas las directivas en el negocio que tengan sincronización de la identidad fijada a un valor con excepción de ningunos. Cuando está seleccionado, un objeto de la máquina se crea y se señala por medio de una bandera para sincronizar con cualquier máquina que utilice ese hostname a través de la cuenta entera. **Note**: Si usted elige utilizar la persistencia de la identidad, Cisco recomienda que usted utiliza **por el nombre de host a través del negocio**. Una máquina tiene un hostname, pero puede tener más de una dirección MAC. La configuración a través de su negocio puede reducir la complejidad de la configuración mientras que hace los objetos global disponibles bastante que por la directiva.
- Por el nombre de host a través de la directiva: Los nuevos conectores buscan el conector más reciente que tiene el mismo hostname para sincronizar con dentro de la misma directiva. Cuando está seleccionado, se crea y se señala por medio de una bandera para sincronizar a cualquier máquina que utilice ese hostname y se registra un objeto de la máquina a la directiva específica.

Paso 2. Descargue el paquete de la instalación del panel de la nube tal y como se muestra en de la imagen:

- Navegue al **conector de la Administración > de la transferencia directa**
- Seleccione el nombre del grupo deseado, y las opciones
- Haga clic la **transferencia directa**
- Utilice **Redistributable** para el despliegue de software del otro vendedor, o las instalaciones offline

> **Note**: Cisco no utiliza la creación de los paquetes o de la instalación que utiliza el despliegue de software del otro vendedor.



Paso 3. Despliegue el conector a las máquinas en su organización.

Verifique

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar si los trabajos de la persistencia de la identidad, siguen los siguientes pasos:

1. Instale el conector para generar un objeto del ordenador que se señale por medio de una bandera para la sincronización de la identidad.
2. Después de que se haya creado el objeto, anote el **<uuid> del** fichero local.xml en el directorio de instalación C:\Program Files\Sourcefire\fireAMP\local.xml**. Usted** debe ver una línea similar a esto:
   `<uuid>1234567890-abcd-efgh-ijkl-mnopqrst</uuid>`
3. Luego, desinstale el conector. Elija **no** tener todos los ficheros quitados del trayecto de instalación.
4. Reinicie la PC y reinstale el AMP para las puntos finales con el mismo paquete que anterior.
5. Controle el **fichero local.xml** otra vez según los pasos iniciales y asegúrese de que hace juego el UUID del local.xmlfile original**.**

Troubleshooting

Esta sección proporciona a la información que usted puede utilizar para resolver problemas su configuración.

- Asegúrese de que los paquetes de la instalación y las configuraciones de la persistencia de la identidad sean constantes.
- Si usted activa el poste-despliegue de la persistencia de la identidad, y utiliza un más viejo paquete para instalar el conector sin la persistencia de la identidad activada, el conector genera los duplicados como se registran, y pone al día las directivas con las configuraciones actuales.
- Si sus máquinas aparecen compartir un UUID, asegúrese de que él no comparta la información única, tal como direcciones MAC dentro de los entornos virtualizados.

Información Relacionada

- Puntos finales avanzadas de la protección de Malware
- Soporte técnico y documentación - Cisco Systems