Desenvolvimento de Cisco AMP para valores-limite com persistência da identidade

Índice

Introdução

Este original descreve que como a característica da persistência da identidade em Cisco avançou a proteção do malware (AMP) para valores-limite permite que um identificador exclusivo do objeto do computador universalmente (UUID) esteja reutilizado quando um computador ou uma máquina virtual (VM) reimaged ou são desmovidos. Isto impede a criação de objetos duplicados do computador em um painel, e mantém dados contíguos para aqueles objetos do computador. Isto igualmente ajuda a manter os conectores do valor-limite, a fornecer a continuidade dos dados, e a manter a contagem da licença na verificação.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do este assuntos:

- Acesso a Cisco AMP para o painel dos valores-limite
- Configurar a persistência da identidade antes que você distribua inicialmente o conector
- A persistência da identidade é apoiada somente no operating system (OS) de Windows

Note: A característica da persistência da identidade deve ser permitida com centro de assistência técnica da Cisco (TAC).

Componentes Utilizados

A informação neste documento é baseada em Cisco AMP para o painel dos valores-limite.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração cancelada (do padrão). Se sua rede está viva, assegure-se de que você

compreenda o impacto potencial do comando any.

Trabalhos

A opção da persistência da identidade usa este trabalhos quando esta é permite:

1. A opção da persistência da identidade é configurada em uma política.
2. O AMP para o instalador dos valores-limite é gerado do painel e distribuído em um computador ou em um VM novo.
3. Um objeto novo do computador é criado com um UUID e a bandeira da persistência da identidade.

- Verificação do registro

Quando o serviço do conector começa, a verificação do registro da nuvem está executada. A verificação do registro avalia a informação da máquina como, do hostname e do MAC address atuais. Igualmente avalia o ajuste da persistência da identidade na política contra a nuvem a fim determinar se um UUID novo precisa de ser gerado.

- Critérios do registro

Um objeto do computador tem hidden uma bandeira ajustada que corresponda ao ajuste da persistência da identidade usado. Esta bandeira, junto com a informação exclusiva (hostname ou MAC address) é usada para fornecer o UUID existente a toda a máquina que combinar os critérios. Se uma bandeira e a informação exclusiva da máquina não combinam com nenhum objeto existente do computador, um UUID e um objeto novos estão gerados para a máquina.

> **Note**: Quando você usa o hostname, o nome de domínio totalmente qualificado (FQDN) está usado. Se você tem uma máquina nomeada **teste** e uma outra máquina nomeada **test.domain.com**, não combinam, e o UUID não é reutilizado.

- Computadores moventes

O movimento dos computadores entre grupos com ajustes diferentes da persistência da identidade cria duplicatas. Isto é devido hidden a uma bandeira que seja associada com cada ajuste da persistência da identidade. Quando os ajustes não combinam, as duplicatas estão geradas. Ambos os grupos devem ter a mesma política aplicada quando trabalham com **através de** ajustes da **política**. Se os ajustes são os mesmos mas as políticas são diferentes, as duplicatas estão criadas.

> **Note**: Se você quer clonar ou imagem que um computador com Cisco AMP para valores-limite instalou, leia este original.

- Eleição do MAC address

Uma máquina pode ter endereços MAC múltiplo, contudo, não é possível influenciar manualmente o processo de eleição do MAC address durante o registro do conector. Você deve usar os ajustes do MAC address somente se você pode garantir que suas máquinas têm somente um MAC address, se não usa o hostname.

- Grupo padrão

A persistência da identidade deve igualmente ser configurada para a política aplicada a seu grupo padrão. Caso uma política ou um grupo forem suprimidos com uma máquina ativa, a máquina

está colocada no grupo padrão quando uma verificação do registro é executada a próxima vez. Se a persistência da identidade não é configurada para o grupo padrão, a seguir o objeto duplicado está gerado.

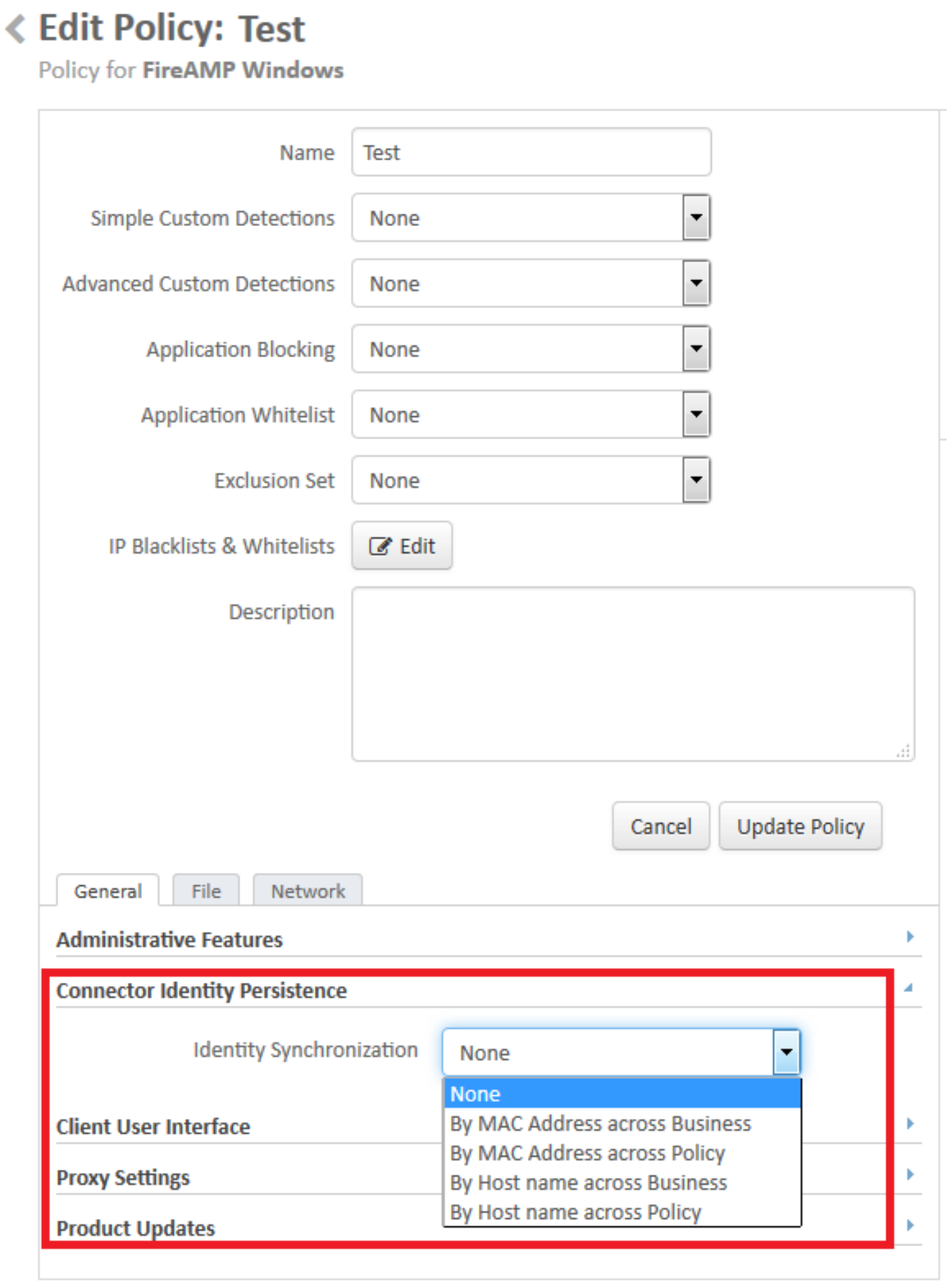
> **Note**: Em alguns casos, um VM clonado pôde ser colocado no grupo padrão um pouco do que o grupo que foi clonado de. Se isto ocorre, mova o VM no grupo correto no console de FireAMP.

Configurar

Siga as etapas aqui a fim distribuir o conector com a persistência da identidade:

Etapa 1. Aplique a persistência desejada da identidade que ajusta-se a suas políticas:

- Navegue ao **Gerenciamento > às políticas**
- Selecione a política desejada. O clique **edita**
- Navegue ao **tab geral**. É selecionado, à revelia
- Selecione a **persistência da identidade do conector**. **A sincronização da identidade** deixa cair aparece para baixo segundo as indicações da imagem.



Note: A capacitação de uma característica depois que a instalação dos valores-limite pode fazer com que os objetos duplicados sejam gerados para cada máquina.

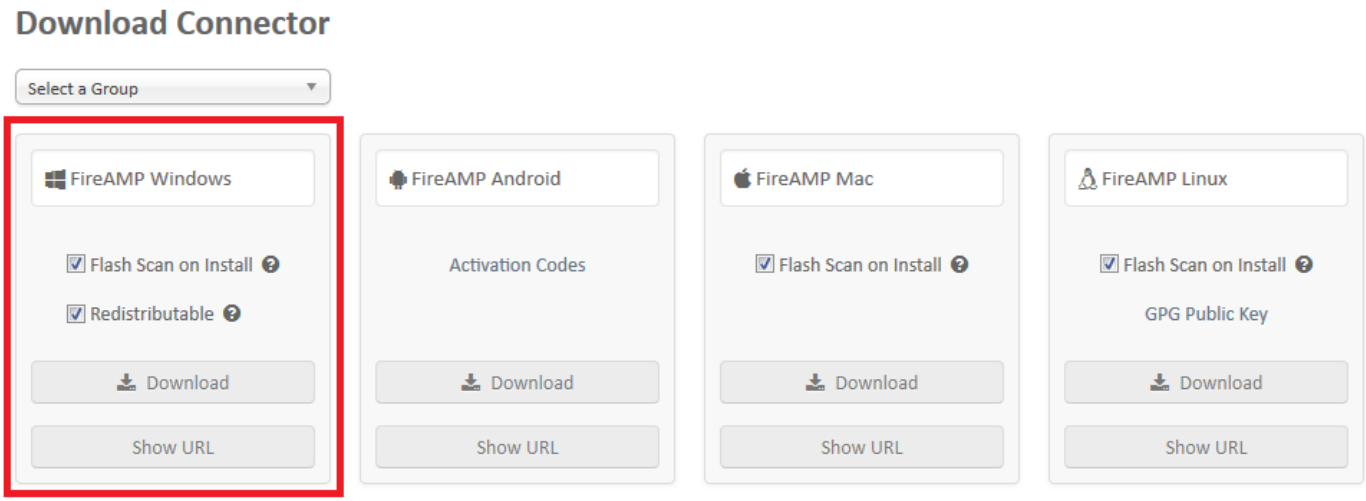
Selecione uma opção da **sincronização da identidade** que seja o melhor para seu ambiente. Estas opções estão disponíveis:

- Nenhum: A característica não é permitida. O conector UUIDs não é sincronizado com o conector novo instala sob nenhuma circunstância. Cada instalação nova gerencie um objeto novo da máquina.
- Pelo MAC address através do negócio: Os conectores novos procuram o conector o mais recente que tem o mesmo MAC address a fim sincronizar através de todas as políticas no negócio que têm a sincronização da identidade ajustada a um valor a não ser nenhuns. Quando selecionado, um objeto da máquina é criado e embandeirado para sincronizar com toda a máquina que usar esse MAC address através da conta inteira.
- Pelo MAC address através da política: Os conectores novos procuram o conector o mais recente que tem o mesmo MAC address a fim sincronizar com dentro da mesma política. Quando selecionado, um objeto da máquina é criado e embandeirado para sincronizar com toda a máquina que usar esse MAC address e é atribuído registrado contra a política específica.
- Pelo nome de host através do negócio: Os conectores novos procuram o conector o mais recente que tem o mesmo hostname a fim sincronizar com através de todas as políticas no negócio que têm a sincronização da identidade ajustada a um valor a não ser nenhuns. Quando selecionado, um objeto da máquina é criado e embandeirado para sincronizar com toda a máquina que usar esse hostname através da conta inteira. **Note**: Se você escolhe usar a persistência da identidade, Cisco recomenda que você se usa pelo **nome de host através do negócio**. Uma máquina tem um hostname, mas pode ter mais de um MAC address. A configuração através de seu negócio pode reduzir a complexidade da configuração enquanto faz os objetos globalmente disponíveis um pouco do que pela política.
- Pelo nome de host através da política: Os conectores novos procuram o conector o mais recente que tem o mesmo hostname a fim sincronizar com dentro da mesma política. Quando selecionado, um objeto da máquina é criado e embandeirado para sincronizar a toda a máquina que usar esse hostname e registrado à política específica.

Etapa 2. Transfira o pacote da instalação do painel da nuvem segundo as indicações da imagem:

- Navegue ao **conector do Gerenciamento > da transferência**
- Selecione o nome do grupo desejado, e opções
- Clique a **transferência**
- Use **Redistributable** para o software de distribuição da terceira parte, ou as instalações autônomas

> **Note**: Cisco não apoia a criação dos pacotes ou da instalação que usa o software de distribuição da terceira parte.



Etapa 3. Distribua o conector às máquinas em sua organização.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A fim verificar se os trabalhos da persistência da identidade, seguem estas etapas:

1. Instale o conector a fim gerar um objeto do computador que seja embandeirado para a sincronização da identidade.
2. Depois que o objeto foi criado, faça uma anotação do **<uuid> do** local.xml arquivar no diretório de instalação C:\Program Files\Sourcefire\fireAMP\local.xml**. Você** deve ver uma linha similar a esta:
   `<uuid>1234567890-abcd-efgh-ijkl-mnopqrst</uuid>`
3. Mais tarde, desinstale o conector. Escolha **não** ter todos os arquivos removidos do caminho de instalação.
4. Recarregue o PC e reinstale o AMP para valores-limite com o mesmo pacote que mais cedo.
5. Verifique o **arquivo local.xml** outra vez conforme as etapas inicial e assegure-se de que combine o UUID do local.xmlfile original**.**

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

- Assegure-se de que os pacotes da instalação e os ajustes da persistência da identidade estejam consistentes.
- Se você permite o cargo-desenvolvimento da persistência da identidade, e usa um pacote mais velho a fim instalar o conector sem persistência da identidade permitida, o conector gerencie duplicatas como se registram, e atualiza as políticas com configurações atual.
- Se suas máquinas parecem compartilhar de um UUID, assegure-se de que não compartilhe da informação exclusiva, tal como endereços MAC dentro dos ambientes virtualizados.

Informações Relacionadas

- Valores-limite avançados da proteção do malware
- Suporte técnico & documentação - Cisco Systems