Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenções](#)
[Processo de descoberta](#)
[Verificar](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como o agente do Cisco Network Admission Control (NAC) descobre um nó da política do Cisco Identity Services Engine (ISE), assim como a configuração exigida para assegurar uma comunicação bem sucedida entre o agente NAC e o ISE.

Pré-requisitos

Requisitos

Cisco recomenda que você cumpre estas exigências:

- A máquina cliente deve ser fornecida com agente NAC.
- O ISE deve ser configurado corretamente para o fluxo do abastecimento do cliente.
- O cliente de AAA (interruptor ou WLC) deve ser configurado com apropriado reorienta o ACL. É crítico que este ACL reorienta toda a comunicação na porta 80 e não reorienta uma comunicação na porta 8905.
- A máquina cliente deve poder resolver o hostname ISE.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Agente 4.9.x do Cisco Network Admission Control (NAC)
- Cisco Identity Services Engine (ISE) 1.1.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre

convenções de documentos.

Processo de descoberta

Quando o agente NAC começa, segue esta sequência:

1. Prova de descoberta HTTP na porta 80 ao host da descoberta, se se é configurado.
2. Prova de descoberta HTTPS na porta 8905 ao host da descoberta, se se é configurado.
3. Prova de descoberta HTTP na porta 80 ao gateway padrão.
4. O HTTPS reconecta a ponta de prova em 8905 ao nó previamente contactado da política ISE.
5. Repita de 1.

A validação de postura bem-sucedida depende do agente que alcança o nó da política que autenticou a sessão 802.1x/MAB original e a recepção da informação de sessão. Esta informação está disponível ao interruptor mas não ao agente. O agente tenta conectar a todo o nó quando vem acima.

Em etapas 1 e 3, observe que o tráfego de HTTP dos usos do agente NAC à porta 80 especificamente para alcançar o host da descoberta ou o gateway padrão. Este processo ocorre porque o fluxo do abastecimento do cliente ISE exige a porta 80 ser reorientado ao nó da política ISE que autenticou a sessão. Enquanto o fluxo do processador do trajeto do controle (CPP) e a URL reorientam a configuração estão corretos e trabalhando, todo o agente NAC na rede deve não experimentar nenhum problema que alcança o nó correto da política. Uma advertência a recordar é que a reorientação URL contém o hostname do ISE, assim que a máquina cliente deve poder resolver isso ao IP do nó da política.

Se a URL reorienta não está trabalhando nem não está configurada, a seguir etapas 2 e 4 estão usadas como o Failover. Estas etapas estão usadas somente se você configurou um host da descoberta ou se o agente tem conectado a este desenvolvimento ISE previamente. Mesmo se o agente obtém a um ponto de decisão de política (PDP) que usa etapa 2 ou 4, não garante que a validação da postura sucederá porque a informação de sessão não pode estar disponível naquela PDP.

A fim trabalhar em torno desta edição, os grupos do nó podem estabelecer-se para compartilhar da informação de sessão. Contudo, é muito mais simples configurar e obter o funcionamento da reorientação URL.

Verificar

A fim verificar se o agente NAC poderá alcançar o nó da política, abra um navegador na máquina cliente e vá a esta URL: https:// <ise-hostname>:8905/auth/discovery

O ISE deve retornar uma página que inclua este texto: X-Perfigo-CAS=<FQDN de *ISE*>

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems