Proceso de detección del agente del Network Admission Control (NAC) para el Identity Services Engine (ISE)

Contenido

Introducción

Este documento describe cómo el agente del Cisco Network Admission Control (NAC) descubre un nodo de la directiva del Cisco Identity Services Engine (ISE), así como la configuración requerida para asegurar la comunicación satisfactoria entre el agente del NAC y el ISE.

prerrequisitos

Requisitos

Cisco recomienda que usted cumple estos requisitos:

- La máquina del cliente debe ser aprovisionado con el agente del NAC.
- El ISE se debe configurar correctamente para el flujo del aprovisionamiento del cliente.
- El cliente AAA (Switch o WLC) debe ser configurado con apropiado reorienta el ACL. Es crítico que este ACL reorienta cualquier comunicación sobre el puerto 80 y no reorienta la comunicación sobre el puerto 8905.
- La máquina del cliente debe poder resolver el nombre de host ISE.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Proceso de detección

Cuando el agente del NAC comienza, sigue esta secuencia:

1. Sonda de detección HTTP en el puerto 80 al host de la detección, si se configura uno.
2. Sonda de detección HTTPS en el puerto 8905 al host de la detección, si se configura uno.
3. Sonda de detección HTTP en el puerto 80 al default gateway.
4. El HTTPS vuelve a conectar la sonda en 8905 al nodo previamente entrado en contacto de la directiva ISE.
5. Relance a partir de la 1.

La validación de postura exitosa depende del agente que alcanza el nodo de la directiva que autenticó la sesión original 802.1x/MAB y la recepción de la información de la sesión. Esta información está disponible para el Switch pero no el agente. El agente intenta conectar con cualquier nodo cuando sube.

En los pasos 1 y 3, note que el tráfico HTTP de las aplicaciones del agente del NAC al puerto 80 específicamente para alcanzar el host de la detección o el default gateway. Este proceso ocurre porque el flujo del aprovisionamiento del cliente ISE requiere el puerto 80 ser reorientado al nodo de la directiva ISE que autenticó la sesión. Mientras el flujo del procesador del trayecto de control (CPP) y el URL reorienten la configuración esté correctos y trabajando, cualquier agente del NAC en la red no debe experimentar ningún problema que alcanza el nodo correcto de la directiva. Una advertencia a recordar es que la reorientación URL contiene el nombre de host del ISE, así que la máquina del cliente debe poder resolver eso al IP del nodo de la directiva.

Si el URL reorienta no está trabajando ni no se configura, después los pasos 2 y 4 se utilizan como Conmutación por falla. Se utilizan estos pasos solamente si usted ha configurado un host de la detección o si el agente ha conectado con este despliegue ISE previamente. Incluso si el agente consigue a un punto de decisión de políticas (PDP) usando el paso 2 o 4, no garantiza que la validación de la postura tendrá éxito porque la información de la sesión puede no estar disponible en ésa PDP.

Para trabajar alrededor de este problema, los grupos del nodo pueden ser configurados para compartir la información de la sesión. Sin embargo, es mucho más simple configurar y conseguir el funcionamiento del cambio de dirección URL.

Verificación

Para verificar si el agente del NAC pueda alcanzar el nodo de la directiva, abra a un navegador en la máquina del cliente y vaya a este URL: https:// <ise-hostname>:8905/auth/discovery

El ISE debe devolver una página que incluya este texto: X-Perfigo-CAS=<FQDN de *ISE*>

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems