La versión 4.0 de AnyConnect y agente de la postura del NAC no surge en la guía del Troubleshooting ISE

Contenido

Introducción

El Identity Services Engine (ISE) proporciona las capacidades posturing que requieren el uso del agente del Network Admission Control (NAC) (para Microsoft Windows, Macintosh, o vía webagent) o de la versión 4.0 de AnyConnect. El módulo de la postura de la versión 4.0 ISE de AnyConnect funciona exactamente como el agente del NAC y por lo tanto se refiere como el agente del NAC en este documento. La mayoría del síntoma común del error de la postura para un cliente es que el agente del NAC no surge puesto que un escenario de trabajo hace siempre la Ventana del agente del NAC surgir y analizar su PC. Este documento le ayuda a estrechar abajo las muchas causas que pueden llevar la postura para fallar, que significa que el agente del NAC no surge. No se significa para ser exhaustivo porque los registros del agente del NAC se pueden decodificar solamente por el Centro de Asistencia Técnica de Cisco (TAC) y las causas raíz posibles son numerosas; sin embargo apunta aclarar la situación y establecer claramente el problema más lejos “el agente no surge que simplemente con el análisis de la postura” y le ayudará probablemente a solucionar la mayoría de las causas comunes.

Prerrequisitos

Requisitos

Los escenarios, los síntomas, y los pasos enumerados en este documento se escriben para que le resuelva problemas los problemas después de que la configuración inicial se complete ya. Para la configuración inicial, refiera a los servicios de la postura en la guía de configuración de Cisco ISE en el cisco.com.

Componentes Utilizados

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

- ISE Version1.2.x
- Agente del NAC para la versión 4.9.x ISE
- Versión 4.0 de AnyConnect

  Nota: La información debe también ser aplicable a otras versiones del ISE a menos que los Release Note indiquen los cambios del comportamiento importantes.

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.

Metodología de Troubleshooting

¿Qué hace que el agente surge?

El agente surge cuando descubre un nodo ISE. Si el agente detecta que no tiene acceso a la red completo y está en un escenario del cambio de dirección de la postura, busca constantemente un nodo ISE.

Hay un documento del cisco.com que explica los detalles del proceso de detección del agente: Proceso de detección del agente del Network Admission Control (NAC) para el Identity Services Engine. Para evitar la duplicación contenta, este documento discute solamente el punto clave.

Cuando un cliente conecta, experimenta una autenticación de RADIUS (filtración o 802.1x MAC) en el extremo cuyo, el ISE vuelve la lista de control de acceso (ACL) y el cambio de dirección URL del cambio de dirección al dispositivo de red (Switch, el dispositivo de seguridad adaptante (ASA), o el regulador inalámbrico) para restringir el tráfico del cliente para permitir solamente que obtenga las resoluciones de una dirección IP y del Domain Name Server (DNS). Todo el tráfico HTTP que viene del cliente se reorienta a un URL único en el ISE que termina con CPP (postura y aprovisionamiento del cliente), excepto el tráfico destinado al portal sí mismo ISE. El agente del NAC envía un paquete regular HTTP GET al default gateway. Si el agente no recibe ninguna respuesta o cualquier otra respuesta que un cambio de dirección de CPP, se considera tener total conectividad y no procede con posturing. Si recibe un HTTP de respuesta que es un cambio de dirección a CPP URL en el final de un nodo específico ISE, después continúa el proceso y los contactos de la postura ese nodo ISE. Surge solamente y comienza el análisis cuando recibe con éxito los detalles de la postura de ese nodo ISE.

El agente del NAC también alcanza hacia fuera a la dirección IP configurada del host de la detección (no espera más de una ser configurado). Espera ser reorientado allí también para conseguir el cambio de dirección URL con el ID de sesión. Si la dirección IP de la detección es un

nodo ISE, después no persigue porque espera para ser reorientada para conseguir el ID de sesión correcto. El host de la detección no es tan generalmente necesario, sino puede ser útil cuando está fijado como cualquier dirección IP en el rango de la reorientación ACL para accionar un cambio de dirección (como en los escenarios de VPN, por ejemplo).

Posibles Causas

El cambio de dirección no sucede

Ésta es la mayoría de la causa común con mucho. Para validar o invalidar, abre a un navegador en el PC donde el agente no surge y ve si le reorientan a la página de la descarga del agente de la postura cuando usted teclea cualquier URL. Usted puede también teclear una dirección IP al azar tal como http://1.2.3.4 para evitar un problema posible DNS (si una dirección IP reorienta pero no lo hace un nombre del sitio web, usted puede mirar el DNS).

Si usted consigue reorientado, usted debe recoger el conjunto de los registros del agente y del soporte ISE (con el módulo de la postura y del suizo para hacer el debug del modo) y TAC de Cisco del contacto. Esto indica que el agente descubre un nodo ISE pero algo no puede durante el proceso obtener los datos de la postura.

Si sucede ningún cambio de dirección, usted tiene su primera causa, que todavía requiere la investigación adicional de la causa raíz. Un buen comienzo es marcar la configuración en el dispositivo de acceso a la red (regulador del Wireless LAN (WLC) o Switch) y moverse al siguiente elemento en este documento.

Los atributos no están instalados en el dispositivo de red

Este problema es un subcase del **cambio de dirección no sucede** escenario. Si no sucede el cambio de dirección, la primera cosa es verificar (pues el problema ocurre en un cliente dado) que la capa del Switch coloca al cliente correctamente en el estatus correcto o del acceso de red inalámbrica.

Aquí está la salida de ejemplo del **comando detail del number> del <interface de la interfaz de la acceso-sesión de la demostración** (usted puede ser que tenga que agregar el **detalle** en el extremo en algunas Plataformas) adquirido el Switch donde el cliente está conectado. Usted debe verificar que el estatus sea “éxito de Authz”, que el URL reorienta el ACL correctamente señala al previsto reorientan el ACL, y que el URL reorienta las puntas al nodo previsto ISE con **CPP** en el final del URL. El campo ACS ACL no es obligatorio porque muestra solamente si usted configuró una lista de acceso transferible en el perfil de la autorización en el ISE. Es, sin embargo, importante mirarlo y verificarlo que no hay conflicto con la reorientación ACL (véase los documentos sobre la configuración de la postura en caso de la duda).

```
01-SW3750-access#show access-sess gi1/0/12 det
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
```

```
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Para resolver problemas un WLC que ejecuta AireOS, ingrese al **detalle < MAC address > del cliente de red inalámbrica de la demostración** y ingrese el **detalle del < MAC address > del MAC address del cliente de red inalámbrica de la demostración** para resolver problemas un WLC que funciona con el Cisco IOS XE. Las pantallas de datos y usted similares deben verificar la reorientación URL y ACL y si el cliente está en el estado “POSTURE_REQD” o similar (él varían dependiendo de la versión de software).

Si los atributos no están presentes, usted debe abrir los detalles de la autenticación en el ISE del cliente que usted resolvía problemas (navegue a las **operaciones > a las autenticaciones**) y verificarlos en la sección del resultado que los atributos del cambio de dirección fueron enviados. Si no fueron enviados, usted debe revisar la directiva de la autorización para entender porqué los atributos no fueron vueltos para este cliente particular. Probablemente uno de las condiciones no hizo juego, así que es una buena idea resolverlas problemas uno por uno.

Recuerde que, con respecto a la reorientación ACL, el ® del Cisco IOS reorienta en las declaraciones del permiso (así que los IP Addresses ISE y DNS necesite ser negado) mientras que AireOS en el WLC reorienta en los enunciados de negación (así que él se permite para el ISE y el DNS).

Los atributos existen pero el dispositivo de red no reorienta

La causa principal en este caso es un problema de configuración. Usted debe revisar la configuración del dispositivo de red contra la guía de configuración y los ejemplos de configuración en el cisco.com. Si éste es el caso, el problema existe típicamente en todos los puertos o (APS) de los Puntos de acceso del dispositivo de red. Si no, el problema pudo ocurrir solamente en algunos switchports o algunos AP. Si éste es el caso, usted debe comparar la configuración de ésos donde ocurre el problema comparado a los puertos o a los AP donde la postura trabaja muy bien.

FlexConnect AP es sensible porque pueden cada uno tener una configuración única y es fácil hacer un error en un ACL o un VLA N en algunos AP y no otros.

Otro problema común es que el VLA N del cliente no tiene un SVI. Esto se aplica solamente al Switches y se discute detalladamente en el cambio de dirección del tráfico ISE en el Catalyst 3750 Series Switch. Todo pudo parecer bueno de la perspectiva de los atributos.

Lista de acceso transferible de interferencia (DACL)

Si, al mismo tiempo que los atributos del cambio de dirección, usted avanzan un DACL de nuevo al Switch (o el Airespace-ACL para un regulador inalámbrico), después podría bloquear su cambio de dirección. El DACL se aplica primero y determina qué se cae totalmente y qué continúa ser procesada. Después la reorientación ACL es aplicada y determina se reorienta qué.

Qué esto concreto significa es ése la mayor parte del tiempo, usted querrá permitir todo el tráfico HTTP y HTTPS en su DACL. Si usted lo bloquea, no será reorientada puesto que será caída antes eso. No es problemas de seguridad, porque ese tráfico será reorientado sobre todo en la reorientación ACL después de, así que no se permite realmente en la red; sin embargo, usted necesita permitir que esos dos tipos de tráfico en el DACL para que él tenga una ocasión de golpear la reorientación ACL justo después de.

Mala versión agente del NAC

Es fácil olvidar que las versiones agente específicas del NAC están validadas contra las versiones específicas del ISE. Muchos administradores actualizan su cluster ISE y olvidan cargar la versión agente relacionada del NAC en la base de datos de los resultados del aprovisionamiento del cliente.

Si usted utiliza una versión agente anticuada del NAC para su código ISE, sea consciente que puede ser que trabaje pero también no pudo. No es tan ninguna sorpresa que algunos clientes trabajan y no lo hacen otros. Una manera de verificar es ir a la sección de la descarga del cisco.com de su versión ISE y el control que las versiones agente del NAC son allí. Típicamente hay varios soportados para cada versión ISE. Esta página web recolecta todas las matrices: Información sobre compatibilidad de Cisco ISE.

El HTTP Web Proxy (Proxy Web) es funcionando por los clientes

El concepto de un HTTP Web Proxy (Proxy Web) es que los clientes no resuelven los IP Addresses del sitio web DNS ellos mismos ni entran en contacto los sitios web directamente; bastante, envían simplemente su petición al servidor proxy, que toma el cuidado de ella. Los problemas comunes con una configuración habitual son que el cliente resuelve un sitio web (tal como www.cisco.com) directamente enviando el HTTP GET para él al proxy, que consigue interceptado y legítimo reorientado al portal ISE. Sin embargo, en vez entonces de enviar el HTTP siguiente GET a la dirección IP porta ISE, el cliente continúa enviando esa petición al proxy.

En caso de que usted decida no reorientar el tráfico HTTP destinado al proxy, sus usuarios tienen acceso directo al toda la Internet (puesto que todo el tráfico pasa con el proxy) sin la autenticidad o posturing. La solución es modificar las configuraciones de buscador del cliente y agregar realmente una excepción para la dirección IP ISE en las configuraciones de representación. Esta manera, cuando el cliente tiene que alcanzar el ISE, envía la petición directamente al ISE y no al proxy. Esto evita el Loop infinito adonde el cliente consigue constantemente reorientado pero nunca ve la página de registro.

Observe que el agente del NAC no es afectado por las configuraciones de representación ingresadas en el sistema y continúa actuando normalmente. Esto significa que si usted utiliza Web Proxy (Proxy Web), usted no puede tener el funcionamiento de la detección del agente del NAC (porque utiliza el puerto 80) y tener los usuarios uno mismo-instalar el agente que los reorientan una vez a la página de la postura cuando hojean (puesto que ese utiliza el puerto del proxy y el Switches típico no puede reorientar en los puertos múltiples).

Los host de la detección se configuran en el agente del NAC

Especialmente después de la versión 1.2 ISE, se recomienda para no configurar ningún host de la detección en el agente del NAC a menos que usted tenga experiencia en lo que hace y no hace. El agente del NAC se supone descubrir el nodo ISE que autenticó el dispositivo del cliente a través de la detección HTTP. Si usted confía en los host de la detección, usted puede ser que tenga el agente del NAC entrar en contacto otro nodo ISE que el que autenticaron el dispositivo y que no trabaja. La versión 1.2 ISE rechaza un agente que descubra el nodo con el proceso del host de la detección porque quisiera que el agente del NAC consiguiera el ID de sesión de la reorientación URL, así que se desalienta este método.

En algunos casos, usted puede ser que quiera configurar un host de la detección. Entonces debe ser configurado con cualquier dirección IP (incluso si es no existente) que sea reorientada por la reorientación ACL, y no debe idealmente estar en la misma subred como el cliente (si no el cliente ARP indefinidamente para él y nunca enviar el paquete de detección HTTP).

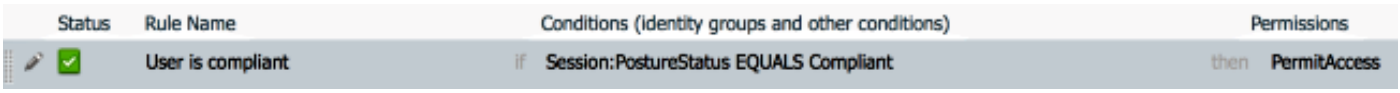
El agente del NAC no surge a veces

Cuando el problema es más intermitente y las acciones tales como desenchufar/replugging la Conectividad del cable/del wifi hacen que trabaja, es un problema más sutil. Podría ser un problema con los ID de sesiones RADIUS donde el ID de sesión es borrado en el ISE por las estadísticas RADIUS (estadísticas de la neutralización para ver si cambian algo).

Si usted utiliza ISE Version1.2, otra posibilidad es que el cliente envía muchos paquetes HTTP de modo que ninguno venga de un navegador o del agente del NAC. La versión 1.2 ISE analiza el campo del agente de usuario en los paquetes HTTP para considerar si viene del agente del NAC o de un navegador, pero muchas otras aplicaciones envían el tráfico HTTP con un campo del agente de usuario y no mencionan ningún sistema operativo o información útil. La versión 1.2 ISE entonces envía un cambio de la autorización de desconectar al cliente. La versión 1.3 ISE no es afectada por este beause del problema que trabaja de una diversa manera. La solución es actualizar a la versión 1.3 o permitir todas las aplicaciones detectadas en la reorientación ACL para no reorientarlas hacia el ISE.

Invierta el problema: El agente surge en varias ocasiones

El problema opuesto puede presentarse donde el agente surge, hace el análisis de la postura, valida al cliente, y después surge otra vez poco después en vez de permitir la conectividad de red y de permanecer silencioso. Esto sucede porque, incluso después una postura acertada, el tráfico HTTP todavía se reorienta al portal de CPP en el ISE. Es una buena idea entonces pasar con la directiva de la autorización ISE y control que usted tiene una regla que envíe un acceso del permiso (o la regla similar con los ACL y los VLA N posibles) cuando considera un cliente obediente y NO un cambio de dirección de CPP otra vez.



Información Relacionada

- Servicios de la postura en la guía de configuración de Cisco ISE
- Proceso de detección del agente del NAC para el ISE
- Cambio de dirección del tráfico ISE en el Catalyst 3750 Series Switch
- Soporte Técnico y Documentación - Cisco Systems