Contenido

Introducción

Este documento describe cómo habilitar el registro del administrador del acceso a la red de AnyConnect (NAM) así como recoger e interpretar los registros. Los ejemplos incluidos en el documento describen diversos escenarios de la autenticación y los registros que reflejen los pasos tomados por el administrador del acceso a la red para autenticar al cliente.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Habilite el registro NAM

Si se identifica un problema que se puede relacionar con el módulo NAM, el primer paso es habilitar la característica de registro extendida. Esto se debe hacer en el punto final del cliente mientras que el módulo NAM se está ejecutando.

Paso 1. Abra la ventana de AnyConnect y aseegurese la está en el foco.

Paso 2. Presione esta combinación de claves, **mayús izquierdo + se fue Alt + L.** No hay respuesta.

Paso 3. Click derecho en el icono de AnyConnect en la bandeja del Sistema Windows. Un menú surge.

Paso 4. Seleccione la **registración extendida** así que hace una marca de tilde visualizar. El NAM ahora registra los mensajes detallados del debug.

Captura de paquetes de la configuración NAM

Cuando se habilita el registro extendido, el NAM también guarda ir del buffer de la captura de paquetes. El buffer por abandono se limita alrededor a 1MB. Si la captura de paquetes es necesaria, puede ser beneficioso aumentar el tamaño de almacén intermedio así que captura más actividades. Para ampliar el buffer, un archivo de la configuración XML debe ser modificado manualmente.

Paso 1. En el PC de Windows, hojee a:
**Cliente de la movilidad de C:\ProgramData\Cisco\Cisco AnyConnect \ administrador \ sistema seguros del acceso a la red **

Paso 2. Abrir archivo **internalConfiguration.xml.**

Paso 3. Localice la etiqueta <packetCaptureFileSize>1</packetCaptureFileSize> XML y ajuste el valor a 10 para que haya un tamaño de almacén intermedio 10MB, y así sucesivamente.

Paso 4. Reinicie PC del cliente para que el cambio tome el efecto.

Registre la colección

La colección del registro NAM se hace vía el diagnóstico y la herramienta de informe (DARDO), que es un módulo de la habitación de AnyConnect. En el instalador, seleccione un módulo y utilice la instalación completa ISO de AnnyConnect para instalar. El instalador de la interfaz de los servicios de medios de Cisco (MSI) se puede también encontrar dentro del ISO.

Después de que usted habilite el registro extendido y realice una prueba, ejecute simplemente el DARDO y pase con el diálogo, el conjunto del registro está situado por abandono en el escritorio de Windows.

Además del conjunto del DARDO, el registro de mensajes NAM es también útil localizar los datos pertinentes en el registro NAM. Para encontrar el registro de mensajes NAM, navegue al **historial de la ventana de configuración de AnyConnect > del administrador > del mensaje del acceso a la red**. El registro de mensajes contiene el grupo fecha/hora de cada evento de la conexión de red, que se puede utilizar para encontrar los registros relevantes al evento.

Lectura de los registros NAM

Los registros NAM, especialmente después de que usted habilita el registro extendido, contienen una gran cantidad de datos, más cuyo sea inútil y puede ser ignorado. Esta sección enumera hacia fuera las líneas del debug para demostrar cada paso NAM toma para establecer una conexión de red. Cuando usted trabaja a través de un registro, estas frases claves pueden ser

útiles establecer a la parte del registro relevante al problema.

Registre el resumen de una conexión de red sin la autenticación habilitada 802.1x

Explicación: Esto indica que el usuario ha seleccionado una red del módulo NAM, y el NAM ha recibido un **userEvent del COMIENZO**.

Explicación: Se han encendido la máquina de estado del acceso y la máquina de estado de la red.

Explicación: El caso del IPv4 conseguido **canceló** para reajustar los estados.

Explicación: El adaptador con ID **484E4FEF-392C-436F-97F0-CD7206CD7D48** fue seleccionado para conectar con la red **test123**, que es el nombre de la conexión de red configurada en el NAM.

Explicación: El NAM ha dedicado con éxito el adaptador para esta red. Ahora el NAM intenta asociarse (conectar) a esta red (que suceda ser inalámbrica):

Explicación: **el openNoEncryption** indica que la red está configurada como abierta. En el regulador del Wireless LAN utiliza puente de la autenticación de MAC (MAB) para autenticar.

Explicación: **el cs** se puede ver mucho en los registros NAM. Éstos son registros inútiles y deben ser ignorados.

Explicación: Éstos son mensajes simples del protocolo de acceso a objetos (JABÓN) usados para decir AnyConnect GUI visualizar el mensaje del estado de la conexión tal como **asociación** en este caso. Cualquier mensaje de error visualizado en la ventana NAM se puede encontrar en uno de los mensajes SOAP en el registro que se puede utilizar para localizar el problema fácilmente.

Explicación: El NAM recibe un evento **AUTH_SUCCESS**, que se engaña porque no hay autenticación que sucedió actualmente. Usted es consigue este evento simplemente porque usted conecta con una red abierta, tan por abandono autenticación es acertado.

Explicación: La asociación al Service Set Identifier (SSID) es acertada, mide el tiempo para manejar la autenticación.

Explicación: Puesto que esto es una red abierta, por abandono se autentica. En este momento, el NAM está conectado con la red y ahora comienza el proceso DHCP:

Explicación: El NAM adquiere con éxito una dirección IP.

Explicación: Una vez que se recibe una dirección IP el NAM enviará la petición ARP (protocolo Protocolo de resolución de la dirección (ARP) gateway (GET-**Conectividad**). Una vez que se recibe la respuesta ARP el cliente está conectado.

Registre el resumen de una conexión de red usando el 802.1x y el PEAP sobre la red alámbrica

Explicación: El NAM comenzó a conectar con la red **WiredPEAP**.

Explicación: El NAM correspondió con un adaptador a esta red.

Explicación: Conexión comenzada NAM con esta red alámbrica.

Explicación: El cliente envía **EAPOL_START**.

Explicación: El cliente recibe la petición de la identidad del Switch, él ahora busca los credenciales para enviar detrás.

Explicación: Por abandono, Anyconnect envía **anónimo** como identidad desprotegida (**identidad externa**), tan aquí él intenta **anónimo** y ve si el servidor es ACEPTABLE con él. El hecho de que la identidad sea **anónima** en comparación con el **host/anónima** indica que es una autenticación de usuario, bastante que la autenticación de la máquina.

Explicación: El servidor de RADIUS envía una trama de la Seguridad de la capa del Protocolo-transporte de la autenticación ampliable (EAP-TLS) sin ningún contenido. Su propósito es negociar el protocolo del EAP-TLS con el cliente.

Explicación: El NAM reconoce la petición del servidor de utilizar el EAP-TLS pero configuran al cliente para utilizar el protocolo extensible authentication protegido (PEAP). Ésta es la razón que el NAM devuelve una contrapropuesta para el PEAP.

Explicación: El servidor de RADIUS valida la identidad externa/desprotegida.

Explicación: La porción **protegida de** comienzo PEAP (establecer un túnel seguro para intercambiar las credenciales internas), después de que el cliente reciba una confirmación del servidor de RADIUS para continuar el uso del PEAP.

Explicación: El NAM envía un saludo del cliente encapsulado en el mensaje EAP y espera los saludos del servidor para venir. El servidor hola contiene el certificado ISE, así que tarda un cierto tiempo para acabar de transferir.

Explicación: El NAM extrajo el asunto del servidor ISE del certificado de servidor. Puesto que no tiene certificado de servidor instalado en el almacén de la confianza, usted no lo encuentra allí.

Explicación: El NAM busca la identidad **interna/protegida** que se enviará al servidor de RADIUS después de que se establezca el túnel. En este caso, "**utilice automáticamente mi nombre de inicio de Windows y la** opción de la **contraseña**" se ha habilitado en el adaptador atado con alambre, así que el NAM utiliza los credenciales de inicio de sesión de las ventanas en vez de pedir al usuario él.

Explicación: El NAM envió la clave del cliente y espec. de la cifra al servidor y recibió la confirmación. La negociación SSL es acertada y se establece un túnel.

Explicación: La identidad protegida se envía al servidor, que valida la identidad. Ahora el servidor pide la contraseña.

Explicación: El NAM recibe la petición de la contraseña y envía la contraseña al servidor.

Explicación: El servidor recibe la contraseña, la verifica y envía el EAP-éxito. La autenticación es acertada en este momento, y el cliente procede mientras que consigue la dirección IP del DHCP.