Pros de la restricción de acceso de la máquina - y - contra

Contenido

Introducción

Este documento describe un problema encontrado con la restricción de acceso de la máquina (MARCHA), y proporciona una solución al problema.

Con el crecimiento de los dispositivos personal-poseídos, es más importante que nunca que los administradores de sistema proporcionen una manera de restringir el acceso a ciertas partes de la red a los activos corporativo-poseídos solamente. El problema descrito en las preocupaciones de este documento cómo identificar con seguridad estas áreas de importancia y autenticarlas sin las interrupciones a la conectividad del usuario.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del 802.1x para entender completamente este documento. Este documento asume la familiaridad con la autenticación del 802.1x del usuario, y resalta los problemas y las ventajas atado al uso de MARCHA, y más generalmente, autenticación de la máquina.

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.

Problema

MARCHA intenta básicamente solucionar un problema común inherente en la mayor parte de los métodos actuales y populares del Protocolo de Autenticación Extensible (EAP), a saber esa autenticación y autenticación de usuario de la máquina son procesos separados, sin relación.

La autenticación de usuario es un método de autentificación del 802.1x que es familiar a la mayoría de los administradores de sistema. La idea es que las credenciales (nombre de usuario/contraseña) están dadas a cada usuario, y que el conjunto de las credenciales representa a una persona física (puede ser compartido entre varias personas también). Por lo tanto, un usuario puede iniciar sesión dondequiera adentro de la red con esas credenciales.

Una autenticación de la máquina es técnico lo mismo, pero no se indica al usuario típicamente que ingrese las credenciales (o el certificado); el ordenador o la máquina hace eso en sus el propio. Esto requiere la máquina ya tener credenciales salvadas. El nombre de usuario enviado es **host/<MyPCHostname>**, a condición de que su máquina tiene <MyPCHostname > fijado como nombre de host. Es decir envía el **host** seguido por su nombre de host.

Aunque esté relacionado no no directamente con Microsoft Windows y el Active Directory de Cisco, este proceso se rinda más fácilmente si la máquina se une a al Active Directory porque el nombre de host del ordenador se agrega a la base de datos del Dominio, y se negocian (y renovó cada 30 días por abandono) y se salvan las credenciales en la máquina. Esto significa que la autenticación de la máquina es posible de cualquier tipo de dispositivo, pero se rinde mucho más fácilmente y transparente si la máquina se une a al Active Directory, y las credenciales permanecen ocultadas del usuario.

MARCHA como solución

Es fácil decir que la solución está para el Sistema de control de acceso de Cisco (ACS) o el Cisco Identity Services Engine (ISE) para completar MARCHA, solamente hay ventajas y desventajas a considerar antes de que se implemente esto. Cómo implementar esto se describe mejor en los guías del usuario ACS o ISE, así que este documento describe simplemente independientemente de si considerar lo, y algunas barricadas posibles.

Los pros

MARCHA fue inventado porque las autenticaciones del usuario y de la máquina son totalmente separadas. Por lo tanto, el servidor de RADIUS no puede aplicar una verificación donde los usuarios deben iniciar sesión de los dispositivos propiedades de la empresa. Con MARCHA, el servidor de RADIUS (ACS o ISE, en el Cisco-lado) aplica, para una autenticación de usuario dada, que debe haber una autenticación válida de la máquina sobre las horas X (típicamente 8 horas, solamente la es configurable) que preceda la autenticación de usuario para el mismo punto final.

Por lo tanto, una autenticación de la máquina tiene éxito si las credenciales de la máquina son sabidas por el servidor de RADIUS, típicamente si la máquina se une a al dominio, y el servidor de RADIUS verifica esto con una conexión al dominio. Está totalmente hasta el administrador de la red a determinar si una autenticación acertada de la máquina proporciona el acceso total a la

red, o solamente un acceso restringido; típicamente, esto por lo menos abre la conexión entre el cliente y el Active Directory de modo que el cliente pueda realizar las acciones tales como la renovación de los objetos de la directiva del grupo de la contraseña del usuario o de la descarga (GPOs).

Si una autenticación de usuario viene de un dispositivo donde una autenticación de la máquina no ha ocurrido en los pares anteriores de las horas, después niegan el usuario, incluso si el usuario es normalmente válido.

El acceso total se concede solamente a un usuario si la autenticación es válida y completada de un punto final en donde una autenticación de la máquina ocurrió en los últimos pares de las horas.

El contra

Esta sección describe el contra del uso de MARCHA.

MARCHA y supplicant de Microsoft Windows

La idea detrás de MARCHA es ésa para que una autenticación de usuario tenga éxito, no sólo debe que el usuario tiene credenciales válidas, pero una autenticación acertada de la máquina se debe registrar de ese cliente también. Si hay cualquier problema con ese, el usuario no puede autenticar. El problema que se presenta es que puede esta característica a veces inadvertidamente cierre un cliente legítimo, que fuerza al cliente a reiniciar para recuperar el acceso a la red.

Microsoft Windows realiza la autenticación de la máquina solamente en el tiempo de arranque (cuando aparece la pantalla de inicio de sesión); tan pronto como el usuario ingrese los credenciales de usuario, se realiza una autenticación de usuario. También, si el usuario termina una sesión (las devoluciones a la pantalla de inicio de sesión), se realiza una nueva autenticación de la máquina.

Aquí está un ejemplo de escenario que muestra porqué MARCHA causa a veces los problemas:

El usuario X trabajó todo el día en su laptop, que fue conectada vía una conexión de red inalámbrica. Al final del día, él cierra simplemente la laptop y las hojas funcionan. Esto coloca la laptop en la hibernación. El next day, él se vuelve en la oficina y abre su laptop. Ahora, él no puede establecer una conexión de red inalámbrica.

Cuando Microsoft Windows hiberna, toma una foto del sistema en su estado actual, que incluye el contexto de quién fue abierta una sesión. Durante la noche, la entrada Marcha-ocultada para la laptop del usuario expira y se purga. Sin embargo, cuando la laptop se acciona encendido, no realiza una autenticación de la máquina. En lugar de otro entra derecho una autenticación de usuario, puesto que eso era lo que registró la hibernación. La única forma de resolver esto es apagar al usuario, o reiniciar su ordenador.

Aunque MARCHA sea una buena característica, tiene el potencial para causar la interrupción del funcionamiento de la red. Estas interrupciones son difíciles de resolver problemas hasta que usted entienda que la manera MARCHA trabaja; cuando usted implementa MARCHA, es importante educar a los usuarios finales sobre cómo apagar correctamente los ordenadores y el cierre de sesión de cada máquina en el final de cada día.

MARCHA y diversos servidores de RADIUS

Es común tener varios servidores de RADIUS en la red para el balanceo de carga y los propósitos de la redundancia. Sin embargo, no todos los servidores de RADIUS soportan un caché compartido de la sesión de MARCHA. Solamente ACS versión 5.4 y posterior, y sincronización del caché de MARCHA del soporte de la versión 2.2 y posterior ISE entre los Nodos. Antes de estas versiones, no es posible realizar una autenticación de la máquina contra un servidor ACS/ISE, y realizar una autenticación de usuario contra otro, pues no corresponden con uno a.

MARCHA y transferencia de la Atar con alambre-Tecnología inalámbrica

El caché de MARCHA de muchos servidores de RADIUS confía en la dirección MAC. Es simplemente una tabla con la dirección MAC de las laptopes y el grupo fecha/hora de su autenticación acertada más reciente de la máquina. Esta manera, el servidor puede saber si el cliente era máquina autenticada sobre las horas del último X.

¿Sin embargo, qué sucede si usted inicia su laptop con una conexión alámbrica (y por lo tanto hace una autenticación de la máquina de su MAC atado con alambre) y después la conmuta a la Tecnología inalámbrica durante el día? El servidor de RADIUS no tiene ningún medio de correlacionar su dirección MAC inalámbrica con su dirección MAC atada con alambre y de saber que usted era máquina autenticada sobre las últimas horas X. La única forma es terminar una sesión y hacer que Microsoft Windows conduzca otra autenticación de la máquina vía la Tecnología inalámbrica.

Solución

Entre muchas otras funciones, Cisco AnyConnect tiene la ventaja de los perfiles preconfigurados que accionan la máquina y la autenticación de usuario. Sin embargo, las mismas limitaciones según lo considerado con el supplicant de Microsoft Windows se encuentran, en lo que respecta a la autenticación de la máquina que ocurre solamente cuando usted termina una sesión o reinicia.

También, con las versiones 3.1 de AnyConnect y posterior, es posible realizar el EAP-FAST con el EAP-encadenamiento. Esto es básicamente una sola autenticación, donde usted envía dos pares de credenciales, del nombre de usuario de la máquina/de contraseña y del nombre de usuario del usuario/de la contraseña, al mismo tiempo. El ISE, entonces, marca más fácilmente que ambos son acertados. Sin el caché usado y ninguna necesidad de extraer una sesión anterior, esto presenta la mayor confiabilidad.

Cuando el PC inicia, AnyConnect envía una autenticación de la máquina solamente, porque no hay información del usuario disponible. Sin embargo, sobre el ingreso del usuario al sistema, AnyConnect envía los credentails de la máquina y del usuario simultáneamente. También, si usted hace disconnected o desenchufa/replug el cable, la máquina y los credenciales de usuario se envían otra vez en una sola autenticación del EAP-FAST, que diferencia de las versiones anteriores de AnyConnect sin el EAP-encadenamiento.

EAP-TEAP es la mejor solución a largo plazo pues se hace especialmente para apoyar este el tipo de autenticaciones, pero EAP-TEAP todavía no se soporta en el supplicant nativo de muchos OS a partir de este día