Vencimiento del certificado y inscripción automática para la reinscripción automática en la CA de Cisco IOS

Contenido

Introducción

Todos los certificados digitales tienen una hora de vencimiento integrada en el certificado que asigna el servidor de la autoridad de certificación (CA) emisora durante la inscripción. Cuando se utiliza un certificado digital para la autenticación VPN IPSec de ISAKMP, hay una verificación automática de la hora de vencimiento del certificado del dispositivo comunicador y de la hora del sistema en el dispositivo (terminal VPN). De esta forma se garantiza que el certificado que se utiliza es válido y no ha vencido. También es por eso que *debe* establecer el reloj interno en cada punto final de VPN (router). Si el protocolo de tiempo de red (NTP) (o el protocolo simple de tiempo de red [SNTP]) no es posible en los routers criptográficos VPN, utilice el comando **set clock** manual.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en todos los routers que ejecutan la imagen cXXXX-advsecurityk9-mz.123-5.9.T para esa plataforma respectiva .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

¿Cuándo se considera que un certificado digital ha caducado o no ha caducado?

- Un certificado ha caducado (no es válido) si la hora del sistema es posterior a la hora de vencimiento del certificado o anterior a la hora de emisión del certificado.
- Un certificado no ha caducado (válido) si la hora del sistema está entre la hora de emisión del certificado y la hora de vencimiento del certificado.

El propósito de la función de inscripción automática es proporcionar al administrador de la CA un mecanismo para permitir que un router actualmente inscrito se vuelva a inscribir automáticamente con su servidor de la CA en un porcentaje configurado de la vida útil del certificado del router. Se trata de una función importante para la capacidad de gestión y compatibilidad de los certificados como mecanismo de control. Si utilizó una CA determinada para emitir certificados a miles de routers VPN de sucursales con un año de vida (sin inscripción automática), entonces exactamente en un año de la fecha de emisión, todos los certificados caducan y todas las sucursales pierden conectividad a través de IPSec. Alternativamente, si la función de inscripción automática se establece en "inscripción automática 70", como en este ejemplo, en el 70% de la vida útil del certificado emitido (1 año), cada router emite automáticamente una nueva solicitud de inscripción al servidor de CA del IOS® de Cisco que se muestra en el punto de confianza.

Nota: Una excepción a la función de inscripción automática es que si está establecida en *menos o igual a 10*, se realiza en minutos. Si es *mayor que 10*, entonces es un porcentaje de la vida útil del certificado.

Hay algunas advertencias que el administrador de CA de Cisco IOS debe tener en cuenta con la inscripción automática. El administrador debe ejecutar estas acciones para que la inscripción sea correcta:

1. Conceda o rechace manualmente cada solicitud de reinscripción en el servidor de la CA de Cisco IOS (a menos que se utilice "Grant auto" en el servidor de la CA de Cisco IOS).El servidor de CA de Cisco IOS todavía necesita conceder o rechazar cada una de estas solicitudes (suponiendo que la CA de Cisco IOS no tiene habilitada la función "Grant auto"). Sin embargo, no se requiere ninguna acción administrativa en el router de inscripción para iniciar el proceso de reinscripción.
2. Guarde el nuevo certificado reinscrito en el router VPN de reinscripción, si procede.Si no hay cambios de configuración sin guardar pendientes en el router, el nuevo certificado se guarda automáticamente en la memoria RAM no volátil (NVRAM). El nuevo certificado se escribe en la NVRAM y se elimina el certificado anterior.Si hay cambios de configuración sin guardar pendientes, debe ejecutar el comando **copy run start** en el router de inscripción para guardar los cambios de configuración y el nuevo certificado reinscrito en la NVRAM. Una vez que se completa el comando **copy run start**, el nuevo certificado se escribe en la NVRAM y se elimina el certificado anterior.**Nota:** Cuando una nueva reinscripción es exitosa, *no* revoca el certificado anterior para ese dispositivo inscrito en el servidor de la CA. Cuando los dispositivos VPN se comunican, se envían el número de serie del certificado (un número único).**Nota:** Por ejemplo, si se encuentra en el 70% de la vida útil del certificado y una sucursal VPN se ha de volver a inscribir en la CA, esa CA tiene dos certificados para ese nombre de host. Sin embargo, el router de inscripción sólo tiene uno (el más reciente). Si lo decide, puede revocar administrativamente el certificado antiguo o permitir que caduque

normalmente.**Nota:** Las versiones de código más recientes de la función de inscripción automática tienen la opción de "regenerar" los pares de claves utilizados para la inscripción.Esta opción es "not default" (no predeterminado) para regenerar pares de claves.Si se elige esta opción, tenga en cuenta el ID de bug de Cisco CSCea90136. Esta corrección de errores permite que el nuevo par de claves se coloque en archivos temporales mientras que la nueva inscripción de certificados se realiza a través de un túnel IPSec existente (es decir, utilizando el par de claves antiguo).La inscripción automática tiene la opción de generar nuevas claves en el momento de la renovación de la certificación. Actualmente, esto causa una pérdida de servicio durante el tiempo que se tarda en obtener un nuevo certificado. Esto se debe a que hay una nueva clave pero ningún certificado que la coincida.Esta función conserva la clave y el certificado antiguos hasta que el nuevo certificado esté disponible.La generación automática de claves también se implementa para la inscripción manual. Se generan claves (según sea necesario) para la inscripción automática o manual.Versión encontrada - 12.3PIH03Versión que se corregirá en - 12.3TVersión aplicada a - 12.3PI03Integrado en: NingunoPara obtener más información, póngase en contacto con el Soporte Técnico de Cisco.

Información Relacionada

- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems