

DIGICERT TRUST LIFECYCLE MANAGER AUTOMATIZA LA GESTIÓN SEGURA DE CERTIFICADOS EN DIFERENTES CARGAS DE TRABAJO

Resumen ejecutivo

Nombre de la empresa: DigiCert

Sector: Tecnología

Sede central: Lehi (Utah)

Requisitos empresariales clave:

- Gestionar con eficacia los certificados digitales de las máquinas virtuales (VM) de la empresa.
- Optimizar los numerosos pasos que hay que seguir para aprovisionar e instalar certificados en distintas cargas de trabajo.
- Automatizar cada aspecto de la gestión del ciclo de vida de los certificados (CLM).

Solución:

- DigiCert Trust Lifecycle Manager

Principales ventajas:

- Gracias a las plantillas de configuración, el equipo de SRE puede aprovechar las funciones de inscripción automática de DigiCert Trust Lifecycle Manager, lo que les permite aprovisionar e instalar certificados en cuestión de minutos, en lugar de horas.
- La automatización optimiza la gestión de certificados y reduce la probabilidad de que se produzcan incidentes relacionados con los certificados o interrupciones de la actividad ocasionadas por errores o certificados caducados.
- Las integraciones con plataformas, nubes y dispositivos de terceros listas para usar ofrecen una gestión integral del ciclo de vida de los certificados que reduce drásticamente la carga de trabajo del equipo de TI a medida que crece el negocio.

Necesidad

Gestionar con eficacia la disponibilidad y seguridad de los hosts en un entorno de TI distribuido

El equipo de SRE (ingeniería de fiabilidad del sitio) de DigiCert se encarga de garantizar la continuidad y el rendimiento de la infraestructura de TI global de la empresa. Para mantener este nivel de disponibilidad sin correr riesgos, el equipo de SRE debe gestionar los certificados digitales que contienen las miles de máquinas virtuales (VM) de las que dependen los centros de datos que la empresa tiene en EE. UU., Europa y Japón.

El problema era que la tarea de gestionar todos esos certificados se complicaba cada vez más a medida que crecía el número de certificados utilizados como identidades para las cargas de trabajo ejecutadas en esas VM, según relata Binh Nguyen, vicepresidente de ingeniería de DigiCert. «Gestionar los certificados nunca ha sido fácil; pero, según aumentaba la cantidad que utilizábamos, se hacía casi imposible llevar un seguimiento de todos sin ningún tipo de ayuda —reconoce Nguyen—. Aprovisionar e instalar un solo certificado podía llevar horas por la cantidad de pasos que había que seguir».





«DigiCert Trust Lifecycle Manager ha transformado la forma en que gestionamos los certificados. Ahora somos muchísimo más eficientes y, además, nuestra infraestructura está considerablemente mejor protegida».
 Binh Nguyen, vicepresidente de ingeniería, DigiCert

Antes, la inscripción de certificados era un proceso engorroso y lento. Una vez que se aprobaba la solicitud de firma de certificado (CSR) y se emitía el certificado, el equipo debía descargarlo e instalarlo en el host a mano, un proceso que requería una serie de pasos que variaban en función del sistema objetivo. A continuación, tenían que comprobar que el certificado funcionase correctamente. «Había que repetir todo el proceso para cada uno de los certificado, y el riesgo de cometer errores aumentaba a cada paso —señala Nguyen—. Necesitábamos poder automatizar estos procesos, porque nosotros somos tan vulnerables a sufrir interrupciones por culpa de un certificado caducado como cualquier otra empresa que utilice la PKI para proteger su infraestructura».

Solución

DigiCert Trust Lifecycle Manager transformó la gestión del ciclo de vida de los certificados (CLM) en las VM

Para Nguyen, DigiCert Trust Lifecycle Manager fue un regalo caído del cielo. La solución permitía ver todos los certificados que utilizaban para proteger las miles de VM de la empresa y las cargas de trabajo que dependían de ellas y ofrecía formas de optimizar los diferentes procesos necesarios para gestionar los ciclos de vida de los certificados. Además, incluía una gran cantidad de funciones de automatización integradas en sus procesos y diseñadas para agilizar la adquisición de certificados y evitar que se produjesen interrupciones si alguno caducaba o se configuraba mal.

«DigiCert Trust Lifecycle Manager ha transformado la forma en que gestionamos los certificados. Ahora somos muchísimo más eficientes y, además, nuestra infraestructura está considerablemente mejor protegida», asegura Nguyen.

Simplificación de la inscripción automática con el uso de perfiles

Lo primero que debía hacer el equipo de SRE era optimizar la inscripción automática de los certificados desde la CSR inicial hasta la instalación y la fase de pruebas. DigiCert Trust Lifecycle Manager permitió simplificar procesos complejos gracias a sus plantillas de configuración, conocidas como «perfiles», que ofrecían reglas predeterminadas para la emisión, instalación y gestión de certificados digitales. Dado que Trust Lifecycle Manager incluye numerosos perfiles comunes, como los que se encargan de la inscripción automática para los servidores web, al equipo de Nguyen le resultó realmente sencillo configurarlos. «Pudimos configurar un perfil para nuestro agente ACME que nos permite supervisar el sistema objetivo desde un único panel de control. Ahora, el agente se encarga de realizar todos los pasos necesarios para renovar los certificados que vayan a caducar sin que nosotros tengamos que hacer nada», afirma Nguyen.

Los usuarios también podían crear perfiles con las plantillas de DigiCert Trust Lifecycle Manager, que eran muy fáciles de seguir y no requerían conocimientos especializados en PKI. La solución permitió al equipo de Nguyen aplicar las configuraciones necesarias para cada caso de uso. Para ello, establecieron perfiles utilizando plantillas con configuraciones predeterminadas que determinan las propiedades del certificado, como el tipo, la validez y la jerarquía de confianza.

DigiCert Trust Lifecycle Manager podía incluso configurar los períodos de validez de los certificados. En palabras de Nguyen: «No hay que ser especialista en PKI para configurar estas acciones porque Trust Lifecycle Manager se encarga de todo, desde la CSR hasta la instalación y la sustitución. Estos procesos, que antes llevaban horas, se realizan ahora en cuestión de minutos, gracias a que Trust Lifecycle Manager los automatiza todos».



Automatización de la CLM desde la detección hasta la renovación

Además de los perfiles, DigiCert Trust Lifecycle Manager integra una arquitectura de automatización gracias a la cual el equipo de Nguyen pudo automatizar todos los aspectos de la gestión del ciclo de vida de los certificados (CLM). Nguyen hizo hincapié en cómo las funciones de detección automatizada de la solución transformaron la forma en la que gestionan los certificados. «Nos ha quitado un gran peso de encima, porque ya no tenemos que preocuparnos de llevar un seguimiento de cada uno de los certificados de las VM —asegura Nguyen—. No solo encuentra los certificados y los añade al inventario independientemente de dónde se hayan emitido, sino que también nos dice quién es su propietario, cuándo van a caducar y si se ajustan o no a nuestras políticas de seguridad».

Otra ventaja de la arquitectura de automatización de DigiCert Trust Lifecycle Manager, más importante si cabe, es que permitió al equipo de Nguyen crear flujos de trabajo de automatización para desencadenar acciones concretas sin que ningún miembro del equipo tuviera que intervenir en el proceso. Por ejemplo, crearon un flujo de trabajo que revocaba automáticamente todo certificado que estuviera mal configurado, que contuviese vulnerabilidades o que hubiera sido emitido por una CA no autorizada. El flujo de trabajo se encargaba de sustituir el certificado en cuestión por otro aprobado emitido por CertCentral o por DigiCert ONE CA Manager, según el tipo de certificado que se estuviese reemplazando.

«Si lo que se pretende es mejorar la velocidad y la seguridad y, al mismo tiempo, reforzar la fiabilidad, esta solución es difícil de superar».



Integración perfecta con dispositivos de red y cargas de trabajo de terceros

Por último, DigiCert Trust Lifecycle Manager se integraba a la perfección en las distintas cargas de trabajo que se ejecutaban en las VM de la empresa, como los equilibradores de carga y los servidores web. Gracias a sus sensores y agentes, Trust Lifecycle Manager gestionó los certificados de los dispositivos de red de forma fiable y sin necesidad de añadir ningún script ni proceso que pudiera aumentar la complejidad o suponer un problema añadido para el equipo de SRE. «Es un alivio saber que nuestros servidores Apache no van a dejar de funcionar de repente por culpa de un certificado del que ni siquiera teníamos constancia», asegura Nguyen.

Otra cosa que valoró mucho Nguyen es la facilidad con la que DigiCert Trust Lifecycle Manager podía gestionar y automatizar todos los certificados que se utilizan como identidades de máquinas en los numerosos microservicios y aplicaciones que dependen de los servidores web y los equilibradores de carga de la empresa. «Casa una de estas piezas necesita un certificado para autenticarse y poder colaborar con las demás. Si lo piensas, la complejidad es abrumadora, pero no con Trust Lifecycle Manager», sentencia.

El equipo de Nguyen ya ha empezado a implementar DigiCert Trust Lifecycle Manager para gestionar los certificados de sus instancias en la nube. Además de ofrecer funciones avanzadas de CLM y PKI gestionada, Trust Lifecycle Manager puede crear ICA (autoridades de certificación intermedias) de forma dinámica, que se pueden lanzar según sea necesario. «Con Trust Lifecycle Manager, tenemos la agilidad necesaria para garantizar la seguridad de nuestra infraestructura a medida que crecemos —añade Nguyen—. Si lo que se pretende es mejorar la velocidad y la seguridad y, al mismo tiempo, reforzar la fiabilidad, esta solución es difícil de superar».

Empiece a disfrutar de las ventajas de DigiCert® Trust Lifecycle Manager hoy mismo. Póngase en [contacto](#) con nosotros.