

Automatización de Sectigo

El cifrado de clave pública (PKI) es el estándar de oro en privacidad, identidad y seguridad digital, y debería ser indiscutiblemente la base de seguridad para cada dispositivo, servidor, usuario y aplicación en la empresa. Sin embargo, utilizar procesos manuales para instalar, monitorear y renovar todos los certificados PKI requeridos actualmente requiere mucha mano de obra, es técnicamente exigente y resulta riesgoso. Además, los costos pueden acumularse rápidamente. Una instalación manual mínima de un certificado TLS/SSL (un solo servidor web e instancia de dominio) implica múltiples pasos y puede sumar fácilmente de \$50 a \$100 por servidor web.

Sumado a esto, la industria avanza hacia vidas útiles de certificados más cortas: primero de tres años a dos, y luego de dos años a uno. Con el próximo cambio hacia la reducción del ciclo de vida de los certificados TLS/SSL, se espera que aumenten los costos de instalación y gestión. Y el momento no podría ser peor. A medida que más empresas amplían el uso de dispositivos móviles, Internet de las cosas (IoT), DevOps y otros entornos digitales, la necesidad de PKI se escala, al igual que la urgencia de poder emitir, revocar y reemplazar certificados de forma rápida, confiable y a escala empresarial.

Automatización de la instalación de certificados TLS/SSL

Claramente, la automatización es ahora crítica para cualquier sistema de gestión de certificados. No solo reduce el costo total de propiedad, sino que también hace cumplir el cumplimiento criptográfico y previene posibles interrupciones del servicio causadas por errores humanos.

Sin embargo, dados los dispares sistemas, aplicaciones y dispositivos que usan e integran certificados digitales, es poco probable que un enfoque único para todos aborde las necesidades de automatización de diversos casos de uso. Es por eso que Sectigo ofrece varias opciones de automatización diferentes.

Para la instalación de certificados TLS/SSL, Sectigo proporciona:

- **Soporte para el protocolo ACME (Automated Certificate Management Environment):**
Sectigo Certificate Manager admite ACME, lo que le permite automatizar la emisión e instalación de certificados para una amplia gama de servidores web, balanceadores de carga, enrutadores, cortafuegos y otros equipos de red. Sectigo admite tipos de certificados DV, OV y EV a través de ACME y proporciona control total a los administradores de TI. Muchas herramientas de DevOps admiten ACME para inscribir y gestionar certificados, y hay una gran cantidad de herramientas de código abierto disponibles para este propósito. Estas herramientas son populares entre los administradores de TI y se mejoran frecuentemente con nuevas funciones.

Si Sectigo implementa el lado del servidor o de la Autoridad de Certificación del estándar ACME, funcionará con clientes compatibles con ACME, y respaldaremos cualquier proyecto de cliente que requiera esa integración (lo que requiere que el cliente sea compatible con ACME). Consulte la tabla a continuación para obtener una lista de las plataformas admitidas actualmente.

- **Un agente de automatización de Sectigo:**

Con el Agente de Red de Sectigo (Network Agent), puede automatizar la gestión de certificados para una variedad de sistemas, incluidos Apache, Apache Tomcat, Windows IIS y balanceadores de carga F5 BIG-IP. El Agente de Red que reside en las instalaciones del cliente está integrado con la solución en la nube Sectigo Certificate Manager para programar la emisión, instalación y renovación de certificados.

- **API REST:**

En algunos casos, las empresas prefieren integrar las aplicaciones más estrechamente con Sectigo, lo cual es posible mediante la API REST de Sectigo. Aunque esto requiere desarrollo adicional en el lado de la aplicación, le permite aprovechar la gestión de certificados y personalizar su flujo de trabajo.

- **Integración con terceros:**

Sectigo busca continuamente oportunidades para integrarse con proveedores terceros para ayudar a los clientes a lograr una automatización completa. Por ejemplo, el balanceador de carga BIG-IP de F5 proporciona integración desde su sistema de gestión para automatizar la gestión de certificados de Sectigo.

Automatización de la Validación de Control de Dominio (DCV)

Con el acortamiento de la vida útil de los certificados, mantener los dominios validados se ha convertido en un requisito continuo. Los procesos de validación manual requieren mucho tiempo, son propensos a errores e insostenibles a escala. Sectigo Certificate Manager agiliza este proceso con Validación de Control de Dominio (DCV) automatizada e integrada como parte de sus capacidades más amplias de automatización del ciclo de vida de los certificados. Mediante conectores DNS, SCM se integra directamente con los proveedores de DNS admitidos para crear y validar automáticamente los desafíos de registros CNAME. Esto elimina la intervención manual, reduce el riesgo de renovaciones fallidas y garantiza que los dominios permanezcan continuamente validados.

SCM continúa ampliando su lista de proveedores DNS admitidos, incluyendo actualmente:

Cloudflare

Amazon Route 53

Azure DNS

GoDaddy DNS

Akamai Edge DNS

DNSimple

OVHcloud

Consulta la lista completa de proveedores de DNS compatibles con SCM [aquí](#).



Automatización de la instalación de certificados de cliente y dispositivo

Muchos sistemas, aplicaciones y dispositivos utilizan certificados que no son SSL. Para la instalación de certificados que no son SSL, Sectigo proporciona:

- **Protocolo EST (Enrollment over Secure Transport):**

Sectigo admite el protocolo EST, que se utiliza para gestionar equipos de red de muchos proveedores. De hecho, varios proveedores ya tienen soporte EST integrado. EST también es popular en entornos de Internet de las Cosas (IoT) dada la eficiencia del protocolo y el soporte de claves de Criptografía de Curva Elíptica (ECC). También hay varios clientes EST de código abierto disponibles. Sectigo Certificate Manager muestra y gestiona los certificados emitidos.

- **Protocolo SCEP (Simple Certificate Enrollment Protocol):**

En el entorno de Sectigo, SCEP se puede utilizar para inscribir certificados en Linux, macOS y otros sistemas operativos. Los dispositivos móviles, el servidor NDES de Microsoft y los MDM suelen utilizar SCEP.

- **Agente de automatización de Sectigo MS:**

Un agente Sectigo MS que se sitúa entre Microsoft Active Directory Certificate Service y Sectigo Certificate Manager. Escucha las solicitudes de certificados a través del Protocolo de Inscripción de Certificados de Cliente de Windows (WCCE) y proporciona automáticamente el certificado al escritorio sin ninguna intervención del empleado.

Como puede ver, Sectigo ofrece una variedad de opciones de instalación de certificados, así como la comodidad y seguridad de una solución fluida con un único panel de control para la emisión y gestión de certificados públicos y privados. Además, con Sectigo, nunca se encontrará con un límite de volumen de certificados, como podría suceder con las alternativas de código abierto. Sectigo permite a su equipo de seguridad hacer cumplir fácilmente la política de seguridad criptográfica; proteger las comunicaciones; evitar la pérdida de datos a través de accesos no autorizados; y preparar para el futuro los sistemas, aplicaciones y dispositivos en toda la empresa.



Automatización TLS/SSL con SCM:

Clientes ACME e integraciones nativas

Red de entrega de contenido (CDN)

Proveedor	Aplicación	Soporte ACME nativo	Cliente ACME utilizado	Integración creada por Sectigo (lista para usar)	Tecnología de integración de Sectigo
Akamai	Terraform			Conector Sectigo para Akamai Terraform	API REST
Akamai	CLI			Conector Sectigo para Akamai CLI	API REST

Contenedorización

Proveedor	Aplicación	Soporte ACME nativo	Cliente ACME utilizado	Integración creada por Sectigo (lista para usar)	Tecnología de integración de Sectigo
Amazon	Elastic Kubernetes Service	✓	jetstack (cert-manager)		
Google	Google Kubernetes Engine	✓	jetstack (cert-manager)		
Kubernetes	Kubernetes	✓	jetstack (cert-manager)		
Microsoft	Azure Kubernetes Services	✓	jetstack (cert-manager)		
Redhat	Openshift Container Platform	✓	jetstack (cert-manager)		
Docker	Docker	✓	ACME.sh		

Herramientas DevOps

Proveedor	Aplicación	Soporte ACME nativo	Cliente ACME utilizado	Integración creada por Sectigo (lista para usar)	Tecnología de integración de Sectigo
Ansible	Ansible	✓	Ansible ACME	Integración de Sectigo con Ansible	API REST
Chef	Chef			Integración de Sectigo con Chef	API REST
HashiCorp	Terraform	✓	Vancluever	Integración de Sectigo con Terraform	API REST
Jenkins	Jenkins			Integración de Sectigo con Jenkins	API REST
Jetstack	Jetstack	✓	jetstack (cert-manager)		
Puppet				Integración de Sectigo con Puppet	API REST
SaltStack				Integración de Sectigo con SaltStack	API REST



Servidores Web / Balanceadores de carga / Cortafuegos

Proveedor	Aplicación	Soporte ACME nativo	Cliente ACME utilizado	Integración creada por Sectigo (lista para usar)	Tecnología de integración de Sectigo
A10	Thunder ADC	✓	Integrado en A10	Conector Sectigo para A10	API REST
Amazon	AWS Certificate Manager			Conector Sectigo para AWS	ACME
Apache	Apache	✓	Certbot mod_md	Agente de red	Agente de red / API REST
Cisco	Cisco FTD			Conector Sectigo para Cisco FTD	API REST
Citrix	ADC			Conector Citrix para Citrix	API REST
Citrix	Gateway			Conector Citrix para Citrix	API REST
Citrix	FAS			Agente MS	APIs
F5	BIG-IP	✓	Kojot ACME	Conector Sectigo para F5 BIG-IP Agente de red	ACME Agente de red / API REST
F5	NGINX	✓	Certbot ACME.sh		
Google	Google Load Balancer			Conector Sectigo para GCP	ACME
HAProxy	HAProxy	✓	Certbot ACME.sh	Conector Sectigo para HAProxy	ACME
Kemp	LoadMaster	✓	ACME.sh	Conector Sectigo para Kemp	API REST
Microsoft	IIS	✓	Win-ACME posh ACME Certify the Web	Conector Sectigo para Kemp	API REST
PaloAlto	PAN OS	✓	ACME.sh		
VMWare	Avi Vantage			Conector Sectigo para Avi Vantage	API REST

Almacén de claves (Key Vault)

Proveedor	Aplicación	Soporte ACME nativo	Cliente ACME utilizado	Integración creada por Sectigo (lista para usar)	Tecnología de integración de Sectigo
Hashicorp	HashiCorp Vault			Integración de Sectigo con HashiCorp Vault	API REST
Microsoft	Azure Key Vault	✓	az-acme	SCM PK Agent	APIs

Lenguaje de programación

Proveedor	Aplicación	Soporte ACME nativo	Cliente ACME utilizado	Integración creada por Sectigo (lista para usar)	Technologie d'intégration Sectigo
Golang	Golang	✓	Lets Encrypt Go		
Java	Java	✓	ACME4j	Conector Sectigo para Java	API REST
Python	Python	✓	certbot		
Ruby	Ruby	✓	acme-client		



Otros

Proveedor	Aplicación	Soporte ACME nativo	Cliente ACME utilizado	Integración creada por Sectigo (lista para usar)	Tecnología de integración de Sectigo
BeyondTrust	BeyondTrust	✓	Native Beyond Trust		
Kong HQ	Kong Gateway	✓	Nativo en Kong ACME.sh		
NodeJS	Python	✓	certbot		

Esta lista no es exhaustiva. Continuamente añadimos soporte para nuevas aplicaciones. Contáctenos para obtener la información más reciente.

Acerca de Sectigo

Sectigo es líder en la gestión del ciclo de vida de los certificados (CLM) y ofrece soluciones innovadoras e integrales para proteger tanto las identidades humanas como las de las máquinas de algunas de las marcas más destacadas del mundo. Su plataforma CLM, nativa en la nube, automatizada y universal, simplifica y mejora la seguridad empresarial mediante la emisión y gestión de certificados digitales de todas las autoridades de certificación (CA) de confianza. Con más de dos décadas de experiencia, Sectigo se erige como una de las CA más grandes y consolidadas, prestando servicio a más de 700 000 clientes en todo el mundo.

Al ofrecer una confianza digital sin igual, Sectigo sigue capacitando a las organizaciones para que implementen protocolos de seguridad robustos con eficiencia y confianza

