Engineer

ACME

el protocolo que emite certificados sin intervención humana

Qué es

ACME, Automatic Certificate Management Environment, es el protocolo con el que un programa solicita un certificado a una autoridad certificadora, demuestra que controla los nombres solicitados y vuelve a por uno nuevo antes de que caduque el anterior. Nadie rellena formularios ni responde a correos de confirmación durante el proceso. RFC 8555 lo estandarizó en marzo de 2019, y Let's Encrypt es la autoridad a través de la cual lo conoce la mayoría.

El cliente comienza con una clave de cuenta propia, separada de las claves de los certificados, y firma con ella cada solicitud. Obtener un certificado recorre después cinco recursos del servidor:

```
newAccount   register the account key once
newOrder     list the names the certificate should cover
authz        one authorization per name, each offering challenges
finalize     send a certificate signing request once all are valid
certificate  download the issued chain, then install it
```

Un desafío demuestra el control de un nombre. El servidor entrega un token; el cliente lo combina con una huella de la clave de cuenta, lo que vincula la prueba a esa cuenta, y publica el resultado donde solo podría ponerlo quien controle el nombre. Importan tres tipos de desafío:

- **http-01** sirve el valor como archivo en `/.well-known/acme-challenge/<token>` bajo el propio nombre. La primera solicitud de la autoridad siempre usa HTTP sin cifrar en el puerto 80.
- **dns-01** publica un hash del valor en un registro TXT en `_acme-challenge` bajo el nombre. Es el único de los tres que demuestra el control de un comodín como `*.example.com` .

- **tls-alpn-01**, añadido por RFC 8737 en febrero de 2020, responde en el puerto 443 durante una negociación TLS con un protocolo ALPN específico. Encaja en un proxy inverso que controla el puerto 443 y no puede usar el 80.

RFC 9773, publicado en junio de 2025, añadió ACME Renewal Information, o ARI. La autoridad publica un intervalo sugerido para renovar cada certificado emitido y el cliente lo consulta en lugar de adivinarlo. Así puede adelantar renovaciones, por ejemplo antes de una revocación masiva, sin que nadie edite un archivo de configuración.

Utilice el concepto en una decisión

Aplique «¿Qué es ACME?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

Poder seguir renovando certificados a mano ha dejado de ser una preferencia. Ahora tiene fechas concretas.

CA/Browser Forum fija las reglas que siguen todas las autoridades de confianza pública. Su propuesta SC-081v3, aprobada en abril de 2025, limita a 200 días los certificados emitidos desde el 15 de marzo de 2026. El límite baja a 100 días el 15 de marzo de 2027 y a 47 el 15 de marzo de 2029. El tiempo durante el que se puede reutilizar una prueba de control del dominio baja en paralelo: de los 200 días actuales a 100 y después a solo 10. Con las reglas finales, un nombre renovado a los dos tercios de su vigencia necesita un certificado aproximadamente cada mes, y casi cada renovación exige un nuevo desafío.

Let’s Encrypt se adelanta al calendario. Sus certificados predeterminados duran hoy 90 días. Desde el 10 de febrero de 2027 durarán 64, con autorizaciones reutilizables durante 10 días, y desde el 16 de febrero de 2028 durarán 45, con reutilización de solo 7 horas. Su propio anuncio desaconseja renovar a mano. También dejó de enviar recordatorios de caducidad el 4 de junio de 2025, de modo que ya no existe aquella red de seguridad ante una renovación olvidada.

La renovación manual queda descartada y ACME pasa a ser la opción predeterminada. Falta decidir dónde viven sus piezas:

- **El desafío.** http-01 es el comienzo sencillo para un único servidor que responde en el puerto 80. dns-01 justifica su configuración adicional para comodines, varios servidores tras un mismo nombre y hosts inaccesibles desde Internet. tls-alpn-01 corresponde a proxies que controlan el puerto 443 y no disponen del 80.
- **El cliente.** Puede residir dentro del servidor web, ejecutarse a su lado con un hook que instale cada certificado nuevo o hacerlo en otra máquina que valide de forma centralizada y copie los certificados a sus destinos.
- **La vigilancia.** Algo externo al cliente debe detectar cuándo no se ha producido una renovación, porque el cliente es precisamente la pieza que acaba de fallar.

Cómo se aplica en la práctica

En su labor de ingeniería DevOps, la empresa automatizó el trabajo de certificados para cien aplicaciones Docker en hosts Ubuntu Linux, con tráfico servido tanto por Apache como por Nginx. ACME ejecutaba todos los pasos: emitir cada certificado, renovarlo antes de caducar y desplegarlo. Ningún paso dependía de recordar una fecha. Las cien aplicaciones mantuvieron certificados válidos y desapareció el trabajo manual.

Es fácil infravalorar el despliegue. Apache y Nginx leen el certificado al iniciar o recargar y siguen sirviendo esa copia. Un cliente que solo escribe un archivo nuevo no ha renovado nada visible para el visitante. Si ambos comparten un conjunto de servidores, cada uno necesita su recarga al llegar un certificado nuevo.

El propio sitio de la empresa muestra la otra disposición: el cliente es el servidor web. En él, Caddy renueva por sí mismo el certificado de Let’s Encrypt. Caddy habla ACME de forma nativa y no necesita herramientas separadas, por lo que no hay un paso de despliegue que olvidar.

Dónde surgen los problemas

El desafío agota el tiempo o devuelve 404 aunque el sitio cargue bien en el navegador. La solicitud http-01 llega al puerto 80 y algo falla en la ruta: un cortafuegos o grupo de seguridad que solo abre 443, una redirección a otro

puerto que no sea 80 o 443, o un balanceador que envía la solicitud a un servidor sin el token. Let's Encrypt sigue hasta diez redirecciones, solo a esos dos puertos. Mantenga abierto el 80, sirva el desafío desde cada backend o desde almacenamiento compartido y use dns-01 cuando no pueda disponer del 80.

La clave de la API DNS del servidor web puede reescribir toda la zona. Un comodín exige dns-01 y el cliente necesita crear registros TXT. La credencial más fácil de obtener suele permitir cambiar todos los registros de la cuenta. Si un atacante entra en el servidor web, también puede redirigir correo y todos los demás nombres. Use una credencial limitada a `_acme-challenge` si el proveedor la ofrece, apunte `_acme-challenge` mediante CNAME a una zona reservada para desafíos o valide en otra máquina y copie los certificados. Los cambios DNS tardan en propagarse; el cliente puede tener que esperar hasta una hora antes de avisar de que el desafío está listo.

Tras redesplegar, los contenedores nuevos arrancan sin certificados. Cada uno solicita su certificado al arrancar y lo conserva solo en su propio sistema de archivos, así que cada reinicio solicita otro. Con suficientes redespliegues o inicios simultáneos, los límites de la autoridad rechazan pedidos adicionales; RFC 8555 llama a ese error `rateLimited`. Let's Encrypt advierte de que, en el peor caso, ninguna instancia obtiene certificado. Guarde certificados y claves en almacenamiento duradero y haga que las instancias nuevas usen uno válido de allí antes de pedir otro.

Un temporizador fijo deja caducar los certificados cuando se acortan las vigencias. Supongamos que el trabajo renueva cada 60 días, pensado para certificados de 90. Uno de 64 días deja cuatro de margen; uno de 45 caduca unas dos semanas antes del siguiente disparo. RFC 9773 cita los intervalos fijos entre los hábitos que impiden a las autoridades cambiar vigencias. Active ARI si el cliente lo admite. Let's Encrypt recomienda consultarlo al menos dos veces al día y, como respaldo, renovar cuando quede un tercio de la vigencia.

El cliente informa de éxito y los visitantes aún ven el certificado antiguo. El archivo nuevo está en disco, pero nadie ordenó recargar al servidor, o el hook recargó solo uno de varios. El antiguo sigue en servicio hasta caducar. Recargue desde el hook de despliegue y vigile desde fuera el certificado realmente servido, no el archivo:

```
openssl s_client -connect example.com:443 -servername example.com \
```

```
    </dev/null 2>/dev/null | openssl x509 -noout -enddate
```

Lecturas adicionales

- RFC 8555: Automatic Certificate Management Environment (ACME) — cuentas, pedidos, autorizaciones y desafíos http-01 y dns-01.
- RFC 9773: extensión ACME Renewal Information (ARI) — el intervalo de renovación sugerido por la autoridad para cada certificado.
- RFC 8737: extensión de desafío ACME TLS Application-Layer Protocol Negotiation (ALPN) — el desafío tls-alpn-01, respondido enteramente en el puerto 443.
- Tipos de desafío — comparación de Let's Encrypt entre los tres desafíos y sus límites.
- Reducción de la vigencia de certificados a 45 días — fechas de Let's Encrypt para certificados más breves y recomendaciones de renovación.
- Propuesta SC-081v3 — votación de CA/Browser Forum que fija los límites de 200, 100 y 47 días.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es ACME?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/acme/