Engineer

ACME

протокол, що видає сертифікат без участі людини

Що це таке

ACME (Automatic Certificate Management Environment) — протокол, яким програма просить центр сертифікації видати сертифікат, доводить, що контролює імена, для яких його просить, і повертається по новий, перш ніж старий спливе. Заповнювати форми чи чекати листів із підтвердженням не треба. RFC 8555 зробив його стандартом у березні 2019 року, а Let's Encrypt — центр сертифікації, через який із ним знайомиться більшість.

Клієнт починає з власного ключа облікового запису, окремого від ключа будь-якого сертифіката, і підписує ним кожен запит. Далі шлях до сертифіката проходить через п'ять ресурсів на сервері:

```
newAccount   один раз зареєструвати ключ облікового запису
newOrder     перелічити імена, які має покрити сертифікат
authz        одна авторизація на ім'я, кожна з варіантами перевірки
finalize     надіслати запит на підпис (CSR), коли все підтверджено
certificate  завантажити виданий ланцюжок і встановити його
```

Перевірка (challenge) — спосіб, яким клієнт показує, що контролює ім'я. Сервер видає токен; клієнт поєднує його з відбитком ключа облікового запису, тож доказ належить саме цьому обліковому запису, і викладає результат туди, куди може дістатися лише той, хто керує іменем. Важать три типи:

- **http-01** віддає значення файлом за адресою `/.well-known/acme-challenge/<token>` на самому імені. Перший запит центру сертифікації завжди йде звичайним HTTP на порт 80.

- **dns-01** кладе хеш значення в TXT-запис `_acme-challenge` під іменем. Лише цей тип із трьох може довести контроль над wildcard-іменем на кшталт `*.example.com` .
- **tls-alpn-01**, доданий RFC 8737 у лютому 2020 року, відповідає на порту 443 під час рукостискання TLS з окремим протоколом ALPN. Він для зворотного проксі, який тримає порт 443 і не може використати порт 80.

RFC 9773, опублікований у червні 2025 року, додав ACME Renewal Information, або ARI. Центр сертифікації публікує рекомендоване вікно поновлення для кожного виданого ним сертифіката, а клієнт питає про це вікно замість того, щоб вгадувати. Так центр може зсунути поновлення раніше, наприклад перед масовим відкликанням, і нікому не доведеться правити конфігураційний файл.

Застосуйте поняття до рішення

Застосуйте «Що таке ACME?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Облікові записи, паролі й права налаштовані так, щоб доступ відповідав роботі, а звільнені втрачали його того ж дня.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Написала 1 000 правил RBAC для Linux-серверів — 1,000 правил доступу написано, щоб усунути вразливість

Написала 1 000 правил RBAC для Linux-серверів Зв'язатися з нами →

Чому це важливо

Чи може людина й далі поновлювати сертифікати вручну, — уже не питання смаку. У цього питання тепер є дати.

CA/Browser Forum встановлює правила, яких дотримується кожен публічно довірений центр сертифікації. За його бюлетенем SC-081v3, ухваленим у квітні 2025 року, сертифікат, виданий від 15 березня 2026 року, може діяти щонайбільше 200 днів. З 15 березня 2027 року межа — 100 днів, а з 15 березня 2029 року — 47. Строк, протягом якого можна повторно використати доказ контролю над доменом, скорочується так само: 200 днів зараз, 100 з 2027 року і лише 10 з 2029-го. За остаточними правилами ім’я, яке поновлюють на двох третинах терміну дії, потребує нового сертифіката приблизно щомісяця, і майже кожне таке поновлення вимагає свіжої перевірки.

Let’s Encrypt випереджає цей графік. Його стандартні сертифікати сьогодні діють 90 днів. З 10 лютого 2027 року вони діятимуть 64 дні, а авторизацію можна буде повторно використати 10 днів; з 16 лютого 2028 року — 45 днів, а повторне використання скоротиться до 7 годин. В оголошенні Let’s Encrypt прямо сказано, що ручне поновлення не рекомендоване. А 4 червня 2025 року він перестав надсилати листи з нагадуванням про кінець терміну дії, тож зникла навіть та страховка, що ловила забуте поновлення.

Ручне поновлення відпадає, тож ACME — вихідна точка. Лишається вирішити, де житимуть його рухомі частини:

- **Перевірка.** http-01 — простий старт для одного сервера, що відповідає на порту 80. dns-01 вартий додаткового налаштування для wildcard-імен, для кількох серверів за одним іменем і для хостів, недосяжних з інтернету. tls-alpn-01 — для проксі, які тримають порт 443, але не мають порту 80.
- **Клієнт.** Він може жити всередині вебсервера, працювати поруч із хуком, що встановлює кожен новий сертифікат, або на окремій машині, яка проходить перевірки централізовано й копіює сертифікати на сервери.
- **Наглядач.** Щось поза клієнтом має помітити, що поновлення не відбулося, бо підвів саме клієнт.

Як це виглядає на практиці

У ролі DevOps-інженера компанія забрала роботу із сертифікатами з людських рук для ста застосунків на Docker на хостах Ubuntu Linux, де трафік обслуговували і Apache, і Nginx. Кожен крок, від випуску сертифіката до поновлення й розгортання, узяв на себе ACME. Жоден крок циклу не чекав, поки хтось згадає дату. Усі сто застосунків лишалися з дійсними сертифікатами, і робити щось руками більше не доводилося.

Розгортання — крок, який найлегше недооцінити. Apache і Nginx читають сертифікат під час запуску чи перечитування конфігурації і далі віддають саме цю копію, тож клієнт, який лише записав новий файл, не поновив того, що бачить відвідувач. Де Apache і Nginx працюють в одному парку, кожному треба окремо дати команду перечитати конфігурацію, щойно з’явиться новий сертифікат.

Власний сайт компанії показує інший устрій, де клієнт — сам вебсервер. Тут Caddy сам поновлює сертифікат сайту в Let's Encrypt. Caddy розмовляє ACME напряму й не потребує окремих інструментів, тож кроку розгортання, про який можна забути, просто немає.

Де виникають проблеми

Перевірка завершується за тайм-аутом або повертає 404, хоча в браузері сайт відкривається. Запит http-01 приходить на порт 80, і щось на його шляху не так: брандмауер чи хмарна група безпеки, що відкриває лише 443, переспрямування на порт, відмінний від 80 і 443, або балансувальник навантаження, що віддає запит серверу, який токена не отримував. Let's Encrypt проходить до десяти переспрямувань, і лише на ці два порти. Тримайте порт 80 відкритим, віддавайте шлях перевірки з кожного бекенда або зі спільного сховища, а де порту 80 не дістати, перейдіть на dns-01.

Ключ DNS API на вебсервері може переписати всю зону. Wildcard-ім'я вимагає dns-01, тож клієнтові треба створювати TXT-записи, а найпростіше отримати ключ, що може змінити кожен запис облікового запису. Якщо вебсервер зламають, нападник зможе переспрямувати й пошту, й усі інші імена. Беріть ключ, обмежений записами `_acme-challenge`, якщо провайдер таке пропонує, або делегуйте `_acme-challenge` через CNAME в окрему зону лише для перевірок, або проходьте перевірку з окремої машини й копіюйте сертифікати. Зміни DNS поширюються не одразу, тож клієнтові, можливо, доведеться чекати до години, перш ніж просити про перевірку.

Після нового розгортання контейнери стартують без сертифікатів. Кожен контейнер просить власний сертифікат під час запуску і зберігає його лише у своїй файловій системі, тож кожен перезапуск просить знову. Якщо розгортати досить часто або запускати багато контейнерів разом, обмеження частоти запитів центру сертифікації відхилять зайві замовлення; RFC 8555 має для цієї помилки окрему назву, `rateLimited`. Let's Encrypt попереджає, що в гіршому разі жоден екземпляр не отримає сертифіката. Тримайте сертифікати й ключі в постійному сховищі, і нехай новий екземпляр бере звідти дійсний сертифікат, перш ніж замовляти новий.

Фіксований таймер поновлення дає сертифікатам спливти, щойно терміни дії скоротяться. Завдання поновлює, скажімо, кожні 60 днів — темп, підібраний під 90-денні сертифікати. Сертифікат на 64 дні лишає таймеру чотири дні запасу, а на 45 днів спливає приблизно за два тижні до

того, як таймер спрацює. RFC 9773 називає фіксовані інтервали однією зі звичок, що заважають центрам сертифікації змінювати терміни дії. Увімкніть ARI, якщо клієнт його підтримує. Let's Encrypt радить перевіряти його щонайменше двічі на день, а як запасний варіант поновлювати, коли лишається третина терміну дії.

Клієнт звітує про успіх, а відвідувачі досі бачать старий сертифікат. Новий файл лежить на диску, але ніхто не сказав вебсерверу перечитати конфігурацію, або скрипт, який клієнт запускає після поновлення, дав команду перечитати конфігурацію лише одному серверу із кількох. Старий сертифікат служить, доки не спливе. Давайте серверу команду перечитати конфігурацію саме з цього скрипта (deploy hook) і стежте ззовні за сертифікатом, який справді віддається, а не за файлом:

```
openssl s_client -connect example.com:443 -servername example.com \
    </dev/null 2>/dev/null | openssl x509 -noout -enddate
```

Що почитати далі

- RFC 8555: Automatic Certificate Management Environment (ACME) — облікові записи, замовлення, авторизації та перевірки http-01 і dns-01.
- RFC 9773: ACME Renewal Information (ARI) Extension — вікно поновлення, яке центр сертифікації пропонує для кожного сертифіката.
- RFC 8737: ACME TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension — перевірка tls-alpn-01, що повністю проходить на порту 443.
- Challenge Types — власне порівняння трьох перевірок від Let's Encrypt з обмеженнями кожної.
- Decreasing Certificate Lifetimes to 45 Days — дати Let's Encrypt для коротших сертифікатів і його поради щодо поновлення.
- Ballot SC-081v3 — голосування CA/Browser Forum, що встановлює межі у 200, 100 і 47 днів.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке ACME?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/acme/