Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Let's Encrypt на Nginx и IIS: TLS без ручного продления

Как мы строим автовыпуск и автопродление сертификатов на Linux/Nginx и Windows/IIS/RD Gateway

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У заказчика 3–15 публичных имён: сайт, CRM, веб-клиент 1С, RD Gateway, почтовый веб. Сертификаты ставили вручную и «навсегда» — раз в год кто-то забывает, и сервис встаёт с красным замком. Мы переводим все точки на ACME с автопродлением: сертификат живёт 90 (с 2027 — 64, с 2028 — 45) дней и обновляется без человека, а срок контролирует мониторинг.

Почему это важно бизнесу

- Просроченный сертификат = стоп для веб-клиента 1С, RD Gateway и форм заявок: сотрудники и клиенты не заходят
- При HSTS браузер вообще не даёт «продолжить» — простой длится, пока не найдут админа с доступом
- Платный OV/EV не добавляет шифрования; экономия 10–20 тыс. руб/год на каждое имя без потери защиты
- Ручное продление раз в 90 дней уже нежизнеспособно, а с 10.02.2027 срок падает до 64, с 16.02.2028 — до 45 дней
- Один забытый хук после продления — и сервер месяцами отдаёт старый сертификат, пока не «протухнет»

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

90→64→45

Срок сертификата: 90 дней сейчас; профиль classic → 64 дня с 10.02.2027, 45 дней с 16.02.2028;...

Let's Encrypt, Lifetimes

1/3

Порог продления Certbot ≥4.0: осталось меньше трети срока (30 дней из 90, 15 из 45) + сверка с...

Certbot User Guide, Renewal

2 раза/сут

Таймер snap.certbot.renew.timer в systemd; продления по ARI вне лимитов, частые прогоны безопа...

наш стандарт (Certbot snap)

55 дн

ScheduledTask.RenewalDays=55 в settings.json simple-acme: продление на 55-й день, задача 09:00...

simple-acme 2.4.0, Settings reference

5 / 7 дн

Лимит дублей на набор имён (+5 ошибок валидации/час) — тесты только на acme-staging-v02 и rene...

Let's Encrypt, Rate Limits

10 дн

{$CERT.EXPIRY.WARN}=10 (дефолт 7) в шаблоне Zabbix «Website certificate by Zabbix agent 2» — а...

наш стандарт (Zabbix 7.0 LTS)

РЕАЛИЗАЦИЯ 1 ИЗ 3

Nginx на Debian/Ubuntu: Certbot из snap + deploy-hook

Что настраиваем

Сайт, CRM и публикация 1С через Apache/Nginx на Debian 12 / Ubuntu 24.04, 1–20 имён на узле

Как мы это делаем

1. Сносим apt-пакет certbot, ставим snap install --classic certbot (5.x), симлинк в /usr/local/bin; ключ по умолчанию ECDSA P-256 (--key-type ecdsa, с Certbot 2.0)
2. Выпуск: certbot --nginx -d host -d www.host --redirect --agree-tos -m ops@…; в конфигах только симлинки /etc/letsencrypt/live/<name>/fullchain.pem и privkey.pem
3. Nginx с nginx.org (1.28): http2 on; есть с 1.25.1, в дистрибутивных 1.22/1.24 — listen 443 ssl http2. ssl_protocols TLSv1.2 TLSv1.3; ssl_session_tickets off; без ss…
4. Хук /etc/letsencrypt/renewal-hooks/deploy/10-reload.sh: nginx -t && systemctl reload nginx (+ reload dovecot/postfix, если ключ общий); проверка certbot renew --dry…
5. HSTS add_header Strict-Transport-Security max-age=63072000 включаем только после первого успешного автопродления, зафиксированного в /var/log/letsencrypt/letsencryp…

РЕЗУЛЬТАТ

Сертификаты на всех именах узла продлеваются таймером без участия инженера; reload Nginx происходит в том же прогоне, поэтому «обновился на диске, но отдаётся старый» исключено. Смена срока на 64/45 дней не потребует правок — порог 1/3 и ARI отрабатывают сами.

КЛЮЧЕВОЙ НЮАНС

Сертификат считается готовым к продлению при <1/3 срока; хуки из renewal-hooks/deploy запускаются по алфавиту и только при реальном перевыпуске — поэтому reload обязан жить именно там, а не в cron.

РЕАЛИЗАЦИЯ 2 ИЗ 3

IIS и RD Gateway на Windows Server: simple-acme (наследник win-acme)

Что настраиваем

Windows Server 2019/2022: сайты IIS, RD Web + RD Gateway, HTTP-публикация 1С через IIS; 1–11 имён

Как мы это делаем

1. Ставим simple-acme 2.4.0 (преемник win-acme 2.2.9.1, .NET 10, поддержка ARI) в C:\Tools\simple-acme; выпуск: wacs.exe --source iis --siteid 1 --installation iis
2. settings.json: ScheduledTask.RenewalDays 55, StartBoundary 09:00, RandomDelay 04:00; Security.EncryptConfig true; хранилище WebHosting; Csr.Rsa.KeyBits 3072
3. RD Gateway: --store pfxfile + --installation script → Set-RDCertificate -Role RDGateway -ImportPath {CertPfx} (RDWebAccess/RDPublishing — отдельные вызовы); без бро…
4. Schannel через GPO/реестр: SCHANNEL\Protocols\TLS 1.0|1.1\Server → Enabled=0, DisabledByDefault=1; TLS 1.3 только на WS2022+; порядок наборов — политика «SSL Cipher…
5. HSTS штатно в IIS 10 (1709+): <hsts enabled="true" max-age="31536000" includeSubDomains="true" redirectHttpToHttps="true"/> на сайте; задача «simple-acme renew» в п…

РЕЗУЛЬТАТ

Одна задача планировщика обслуживает все сертификаты сервера и сама перепривязывает binding'и IIS и RD Gateway; после апдейтов ОС контроль — schtasks /query и wacs.exe --renew --force. Журнал в %ProgramData%\simple-acme\…\Log и e-mail при ошибке.

КЛЮЧЕВОЙ НЮАНС

Security.PrivateKeyExportable по умолчанию false — для RDS-ролей нужен PFX, поэтому берём store pfxfile со скриптом; в имени задачи прописан ACME-URL, при смене DefaultBaseUri задачу пересоздаём (--setuptasksc…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Wildcard и узлы за NAT: DNS-01 с делегированием _acme-challenge

Что настраиваем

*Многофилиальные поддомены *.company.ru, IIS без открытого 80/tcp, внутренние имена без входящего трафика*

Как мы это делаем

1. Если у регистратора есть API — snap install certbot-dns-<provider> (+ trust-plugin-with-root=ok), credentials-файл 0600 (--dns-cloudflare-credentials …); wildcard т…
2. Если API нет (типично для РФ-регистраторов) — CNAME _acme-challenge.company.ru → зона acme-dns на нашем узле; на клиентской стороне DNS больше ничего не трогаем
3. Certbot: --dns-… или --manual-auth-hook со скриптом acme-dns; simple-acme: --validation acme-dns --acmednsserver https://… с PreValidateDns true — ждём распростране…
4. Один SAN-сертификат до 100 имён (classic) вместо десятков отдельных; профиль tlsserver (45 дней, до 25 имён) включаем точечно через --preferred-profile tlsserver дл…
5. Мониторинг: Zabbix 7.0, шаблон Website certificate by Zabbix agent 2 (web.certificate.get), {$CERT.EXPIRY.WARN}=10 → Telegram; письма об истечении LE не шлёт с 04.0…

РЕЗУЛЬТАТ

Сертификаты выпускаются без открытия портов и без ручных TXT-записей, продление полностью автономно; wildcard закрывает новые филиалы без перевыпуска, а сбой продления виден за 10 дней до истечения.

КЛЮЧЕВОЙ НЮАНС

ACME проверяет TXT именно на _acme-challenge.<имя>; делегирование через CNAME/NS разрешено докой Let's Encrypt, ключ API регистратора при этом на сервере клиента вообще не хранится.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Забытый deploy-hook**
  Certbot перевыпускает файл, но Nginx держит старый в памяти. Хук reload только в renewal-hooks/deploy; проверяем openssl s_client | x509 -enddate

- ✕ **Прямые пути на cert1.pem**
  Указан archive/…/cert3.pem вместо live/…/fullchain.pem — после продления ссылка не двигается. Только симлинки из live/

- ✕ **Certbot из apt**
  Пакет дистрибутива отстаёт на годы и не знает ARI/профилей (Certbot ≥4.1). Ставим только snap --classic и следим за snap refresh

- ✕ **Тесты на боевом ACME**
  5 дублей за 7 дней на набор имён и 5 ошибок валидации в час — упёрлись и ждём. Отладка на acme-staging-v02 и renew --dry-run

- ✕ **HSTS раньше автопродления**
  max-age на год + протухший сертификат = браузер без кнопки «продолжить». HSTS включаем после одного успешного цикла продления

- ✕ **ssl_stapling с Let's Encrypt**
  OCSP-URL в сертификатах нет с 07.05.2025, ответчики выключены 06.08.2025 — директива только сыплет warning'и в error.log. Убираем

- ✕ **simple-acme после апдейта ОС**
  После in-place upgrade задача планировщика может исчезнуть. Проверяем schtasks /query /tn "simple-acme renew*", пересоздаём wacs.exe --setuptasksched…

- ✕ **Жёсткий cron «раз в 60 дней»**
  С 64/45-дневными сертификатами такой интервал пропустит продление. Только клиент с порогом 1/3 срока и ARI, запуск ежедневно

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Certbot из snap (≥4.1, ARI) / simple-acme 2.4, TLS 1.2+1.3, TLS 1.0/1.1 выключены
- Deploy-hook на reload сервиса и проверенный certbot renew --dry-run
- Отладка только на staging-ACME; логи /var/log/letsencrypt и %ProgramData%\simple-acme
- Скрипт-проверка openssl x509 -enddate раз в сутки с алертом в Telegram

НОРМАЛЬНО

- Zabbix 7.0: шаблон Website certificate by Zabbix agent 2, {$CERT.EXPIRY.WARN}=10
- HSTS включён после первого автопродления; ssl_session_tickets off, http2 on (nginx ≥…
- DNS-01 через плагин или acme-dns для wildcard и узлов без 80-го порта
- RD Gateway/RD Web через Set-RDCertificate (по одной роли) из installation-скрипта si…

ХОРОШО

- Один SAN до 100 имён на узел, ключ ECDSA P-256 (Nginx) / RSA 3072 (IIS, RDS)
- Профиль tlsserver (45 дней, ≤25 имён) обкатан на тестовом имени, ARI включён у всех…
- Cipher suite order через GPO, шаблон ssl-сниппета Nginx в git и в Ansible-роли
- E-mail/Telegram-уведомление simple-acme об ошибках + еженедельный отчёт по срокам

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Все публичные имена (сайт, CRM, 1С-веб, RD Gateway, почта) выпускаются через ACME, а не вручную?
- [ ] Certbot стоит из snap (5.x), а не из apt; на Windows — simple-acme 2.4 с задачей планировщика?
- [ ] После продления сервис перечитывает сертификат: deploy-hook на Nginx, installation-plugin на IIS?
- [ ] certbot renew --dry-run и wacs.exe --renew --force проходят без ошибок в журнале?
- [ ] Конфиги ссылаются на /etc/letsencrypt/live/<name>/fullchain.pem, а не на archive/…N.pem?
- [ ] TLS 1.0/1.1 выключены (ssl_protocols, Schannel Enabled=0), включён TLS 1.3?
- [ ] Мониторинг срока: Zabbix-шаблон (web.certificate.get) или скрипт с порогом ≥10 дней и алертом в мессенджер?
- [ ] HSTS включён только там, где автопродление уже отработало хотя бы один цикл?
- [ ] Wildcard и узлы за NAT переведены на DNS-01 (плагин или CNAME на acme-dns)?
- [ ] Автоматизация выдержит переход на 64-дневные (02.2027) и 45-дневные (02.2028) сертификаты без правок?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит всех сертификатов компании: сроки, цепочки, версии TLS, кто и как продлевает
- Внедрение Certbot/simple-acme на Nginx, Apache, IIS, RD Gateway и веб-публикациях 1С под ключ
- Wildcard и DNS-01: подключаем API регистратора или поднимаем acme-dns с CNAME-делегированием
- Мониторинг сроков в Zabbix 7.0 с алертами в Telegram и регламентом реакции
- Сопровождение: разбор сбоев продления, переход на 45-дневные сертификаты и профили ACME

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

Техническая база

01 Certbot User Guide: Renewing certificates, renewal-hooks, --key-type, --pr… (eff-certbot.readthedocs.io — 5.8.0)

02 Let's Encrypt: Certificate Lifetimes, Certificate Profiles, Rate Limits, C… (letsencrypt.org — 2026)

03 Let's Encrypt: Ending OCSP Support (переход на CRL), Ending Expiration Ema… (letsencrypt.org — 2025)

04 simple-acme Reference: settings.json (ScheduledTask, Security, Csr), pfxfi… (simple-acme.com — 2.4.0)

05 Module ngx_http_ssl_module, ngx_http_v2_module (директива http2 с 1.25.1) (nginx.org — 1.28 / 1…)

06 TLS registry settings; Protocols in TLS/SSL (Schannel SSP); cipher suite o… (learn.microsoft.com — 2025)

07 IIS <hsts> element; Set-RDCertificate (RemoteDesktop); RDS: provider (learn.microsoft.com — WS2022/2…)

08 Zabbix template «Website certificate by Zabbix agent 2», web.certificate.g… (zabbix.com — 7.0 LTS)

Основано на официальной документации продуктов и нашей практике внедрения.