

外贸企业网站安全系列 · 小白版

网站 SSL 证书 免费部署完全指南

(小白版)

外贸企业老板 / 运营人员专用 · 一步一步，让网址栏告别“不安全”

- ✓ 6 条路线：Linux / 宝塔 / cPanel / Cloudflare / IIS / SaaS
- ✓ **每一步**：点哪里 · 输入什么 · 应该看到什么
- ✓ 真实截图 + 真实命令输出 + 标注示意图
- ✓ 故障排查表 · FAQ · 一页速查表
- ✓ 新增：一键复制给 AI 智能体



版本 1.0 · 2026 年 10 月 10 日（文中官方资料均于该日核对）
证书本身免费：不需要为“金融级证书”付 2500 元。

目录

第0章	本指南怎么用 & 我该走哪条路	4
0.1	先说结论：证书是免费的	4
0.2	怎么读这本指南	4
0.3	我该走哪条路？	4
第1章	基础知识：10 分钟看懂 SSL	7
1.1	SSL / HTTPS 到底是什么	7
1.2	为什么我的网站显示“不安全”	7
1.3	有哪些免费证书	9
1.4	证书有效期：90 天，而且会越来越短	10
1.5	开始前你需要准备什么	10
第2章	自查：你的网站现在 HTTPS 正常吗？	11
2.1	用 Chrome 浏览器检查（最简单）	11
2.2	用 SSL Labs 在线检测（最全面）	12
2.3	用命令检查（给愿意多走一步的人）	13
第3章	动手前的准备：预检清单	15
3.1	预检清单（打勾再开始）	15
3.2	放行 80 / 443 端口：两道门都要开	15
3.3	DNS 生效需要时间	17
3.4	中国大陆服务器与 ICP 备案（简要说明）	17
第4章	路线 A：Linux 云服务器 + Certbot (Nginx / Apache)	18
4.1	第 0 步：登录服务器	18
4.2	第 1 步：备份配置并确认网站能用 http 打开	19
4.3	第 2 步：安装 Certbot	19
4.4	第 3 步：一条命令申请并安装证书 (Nginx)	20
4.5	Apache 用户	22
4.6	没法用插件时：webroot 方式	22
4.7	验证失败长什么样	23
4.8	第 4 步：确认自动续期	24
4.9	第 5 步：打开浏览器验收	26
第5章	路线 B：宝塔面板	27
5.1	申请前确认	27
5.2	用“文件验证”申请 Let's Encrypt（最常用）	27
5.3	开启强制 HTTPS	29
5.4	通配符证书：用 DNS 验证	29
5.5	确认自动续签	30
第6章	路线 C：cPanel 虚拟主机 (AutoSSL)	31
6.1	检查并运行 AutoSSL	31
6.2	看懂失败提示	31

6.3 开启强制 HTTPS 跳转	32
第7章 路线 D: Cloudflare（没有服务器权限也能做）	33
7.1 第 1 步：把域名接入 Cloudflare	33
7.2 第 2 步：到域名注册商修改 NS	34
7.3 第 3 步：选择 SSL/TLS 加密模式	35
7.4 第 4 步：给源站装证书（二选一）	36
7.5 第 5 步：开启“始终使用 HTTPS”	38
7.6 高级：用 API 自动化（给技术人员或 AI 智能体）	38
第8章 路线 F: Windows 服务器 + IIS（win-acme）	40
8.1 准备	40
8.2 下载与运行	40
8.3 按菜单操作	41
8.4 验证	41
第9章 路线 E: SaaS 建站平台（Shopify / Wix / WordPress.com 等）	42
9.1 证书一直“待处理 / Pending”怎么办	42
第10章 装好之后：这 6 件事一定要做	43
10.1 强制 HTTP 跳转到 HTTPS	43
10.2 修复“混合内容”	43
10.3 确认自动续期真的有效	44
10.4 设置证书到期监控（强烈建议）	44
10.5 更新 Google Search Console 和站点地图	44
10.6 最后跑一次 SSL Labs	45
第11章 让你的智能体帮你部署	46
11.1 怎么用（5 步）	46
11.2 安全须知（一定要看）	47
11.3 给网站管理员：这个按钮怎么做	47
第12章 故障排查表	49
第13章 常见问题（FAQ）	51
第14章 一页速查表（建议打印）	53
附录 参考资料、图片说明与未核实事项	54
A. 参考资料（均于 2026-10-10 访问核对）	54
B. 图片类型一览	55
C. 未能实机核实 / 需以实际为准的内容	55

第0章

本指南怎么用 & 我该走哪条路

0.1 先说结论：证书是免费的

如果有人向你收 2500 元，说要给网站装一张“金融级 SSL 证书”，请先停一下。让浏览器显示“安全”的证书，绝大多数网站用的都是**免费证书**（例如 Let's Encrypt，一个由非营利组织运营、给全球七亿多个网站发证书的机构）。浏览器只判断证书**有效还是无效**，不存在“金融级、军工级”这种级别。

你要花的只是**时间**：按本指南操作，熟悉的人 20 分钟，第一次做的人留出 1~2 小时，基本都能搞定。

小贴士 这本指南适合谁

外贸公司的老板、运营、跟单、文员——完全不懂技术也没关系。每一步都写了“要点哪里 / 要输入什么 / 你应该看到什么 / 看不到怎么办”。遇到专业词，后面都会用一句话解释。

0.2 怎么读这本指南

- 1 先看本章 0.3 节，用“6 道题流程图”找到你属于哪条路线（A~F）。
- 2 读第 1~3 章：明白原理，做好部署前检查（这一步能避开 80% 的失败）。
- 3 只读你那条路线的章节（第 4~9 章），其他章节可以跳过。
- 4 装完后读第 10 章：强制跳转、混合内容、自动续期、到期监控，一个都不能少。
- 5 卡住了就翻第 12 章故障排查表；想让 AI 帮你做，看第 11 章。
- 6 最后一页是一页速查表，可以打印贴在工位上。

说明 图片说明

本指南的每张图都标了类型：**【真实截图】**是在真实浏览器或真实网站上截的；**【真实命令输出】**是在实验服务器上真实运行命令得到的文字，用终端样式排版；**【示意图】**是根据官方文档画的界面示意，菜单名称已核对，但不同版本的颜色、位置可能不同，**以你看到的实际界面为准**。

0.3 我该走哪条路？

网站“装证书”的方法，取决于网站**放在哪里**、你能**登录哪种后台**。按下面的流程图从第 1 题往下答：



示意图 图 1 6 道题找到你的路线

路线	你的情况	去哪一章	难度
A	自己的 Linux 云服务器（阿里云、腾讯云、AWS、Vultr 等），能用 SSH 登录，网站跑在 Nginx 或 Apache 上	第 4 章	★★★
B	服务器上装了“宝塔面板”	第 5 章	★
C	买的是“虚拟主机”，后台叫 cPanel	第 6 章	★
D	域名接入了 Cloudflare（或者你没有服务器权限，只能管域名）	第 7 章	★★
E	Shopify、Wix、WordPress.com 或其他 SaaS 建站平台	第 9 章	★
F	Windows 服务器，用 IIS 建站	第 8 章	★★

💡 小贴士 名词一句话解释

服务器：一台 24 小时开机、存放你网站文件的电脑。**SSH**：用命令远程登录 Linux 服务器的方法。**Nginx / Apache / IIS**：服务器上负责“把网页发给访客”的软件。**面板**（宝塔、cPanel）：把这些操作做成网页按钮的管理后台。**SaaS 建站平台**：你只管内容、服务器由平台负责的建站服务。

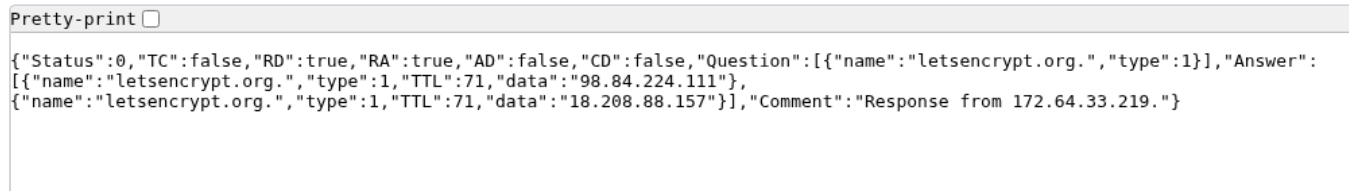
不知道自己是哪种？三个办法

办法一：直接问建站公司（最快）。复制下面这段话发给他们：

“您好，我们网站要装免费 SSL 证书（Let's Encrypt）。请告诉我：① 网站放在哪里（哪家云服务器 / 虚拟主机 / 建站平台）？② 用的是宝塔、cPanel，还是直接 SSH？③ 域名 DNS 在哪里管理（阿里云 / 腾讯云 / Cloudflare / 其他）？④ 服务器在中国大陆吗？域名备案了吗？”

办法二：用浏览器查（不用装任何软件）。

- 1 打开 `https://dns.google/resolve?name=你的域名&type=NS`（把“你的域名”换成例如 `my-trade-demo.com`）。这是 Google 的公共 DNS 查询页，会返回一段文字。
- 2 看 "data" 后面的内容：如果出现 `ns.cloudflare.com`，你走**路线 D**；出现 `hichina.com` / `alidns.com` 一般是阿里云，`dnspod.net` 一般是腾讯云。
- 3 再把地址里的 `type=NS` 改成 `type=A`，看到的 `data` 就是网站服务器的 IP 地址（一串数字，如 `47.xx.xx.xx`）。



真实截图 图2 在浏览器里用 dns.google 查询域名解析（返回的就是 IP 地址）

- 4 打开 `https://who.is/whois/你的域名`，可以看到域名在哪家注册商、NS 是什么（部分信息可能因隐私保护被隐藏）。

办法三：用命令查（Windows 打开“命令提示符”，Mac 打开“终端”）。

```
BASH
nslookup -type=NS my-trade-demo.com
nslookup my-trade-demo.com
curl -sI https://my-trade-demo.com
```

逐行解释：

- 第 1 行：查域名的 DNS 服务器（NS，Name Server，即“这个域名的解析由谁负责”）。
- 第 2 行：查域名指向的 IP 地址。
- 第 3 行：只取网页的“响应头”（-s 安静模式，-I 只要头部）。看其中 `server:` 一行：`cloudflare` → 路线 D；`nginx` / `Apache` → 路线 A 或 B；`Microsoft-IIS` → 路线 F；出现 `x-shopify` 字样 → Shopify（路线 E）。

⚠ 注意 先确认“谁有权限”

无论哪条路线，你都需要对应后台的**登录权限**：服务器 SSH、宝塔面板、cPanel、Cloudflare 账号、域名注册商账号中的一个或几个。如果这些都在建站公司手里，请让他们配合，或者要求他们开一个子账号给你。**不要在微信、邮件里明文发送密码。**

第1章

基础知识：10 分钟看懂 SSL

1.1 SSL / HTTPS 到底是什么

- **HTTP**：网站和访客之间传数据的“普通方式”，像寄明信片，沿途的人都能看到、能改。
- **HTTPS**：HTTP 加上加密（S 代表 Secure），像把信装进只有收件人能拆开的保险信封。
- **SSL 证书**（现在技术上叫 TLS 证书，大家习惯仍叫 SSL）：网站的“电子营业执照”。浏览器靠它确认“你访问的确实是这个网站，而且连接已经加密”。

HTTP 和 HTTPS 的区别（一张图看懂）

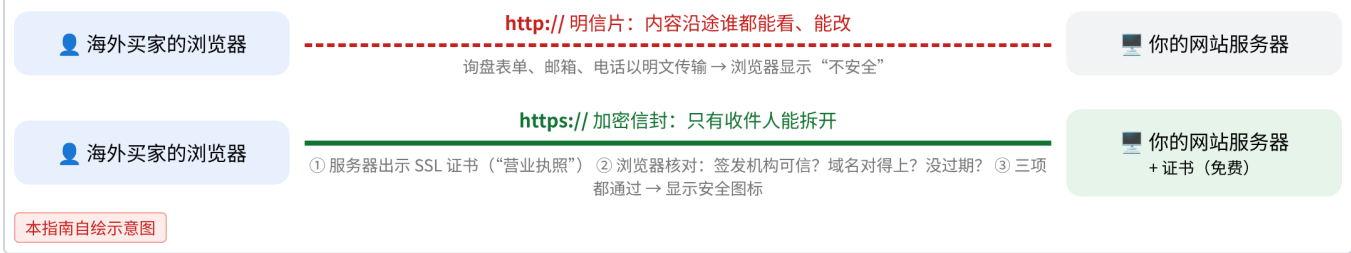


示意图 图3 HTTP 与 HTTPS 的区别

浏览器打开一个 https 网站时，会自动核对三件事：

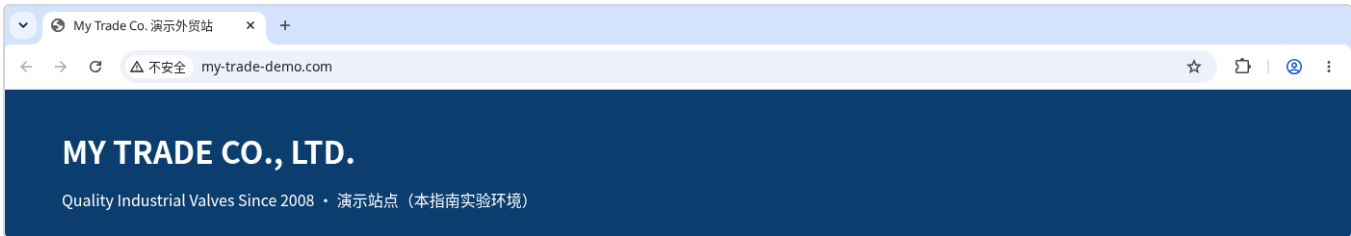
- 1 证书是不是由**受信任的机构**（CA，Certificate Authority，证书颁发机构）签发的？
- 2 证书上写的**域名**和你访问的域名对不对得上？
- 3 证书**有没有过期**？

三项都通过，地址栏显示正常的“安全”状态；任何一项不通过，就出现“不安全”或整页红色警告。

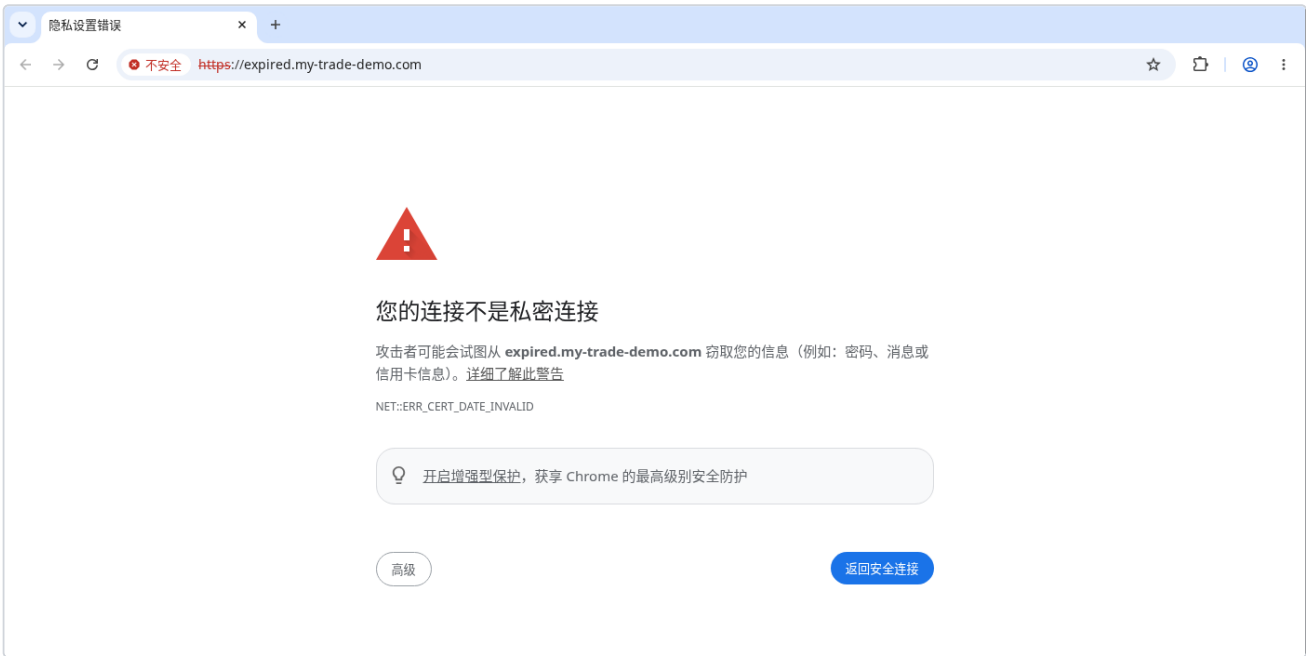
1.2 为什么我的网站显示“不安全”

你看到的	最可能的原因	本指南在哪里解决
地址栏左侧写着“不安全”，网址是 <code>http://</code> 开头	根本没装证书，或装了但没有强制跳转到 https	第 4~9 章 + 第 10.1 节
整页红色警告“您的连接不是私密连接”，代码 <code>NET::ERR_CERT_DATE_INVALID</code>	证书 过期 了（最常见！）	第 10.3 节自动续期
整页警告，代码 <code>NET::ERR_CERT_COMMON_NAME_INVALID</code>	证书上的域名和网址 对不上 （例如证书只含 <code>www</code> ，访问的是不带 <code>www</code> 的）	第 12 章
整页警告，代码 <code>NET::ERR_CERT_AUTHORITY_INVALID</code>	证书不是受信任机构签的（自签名证书、测试证书，或把 Cloudflare 源证书直接给访客用了）	第 7、12 章
网址是 https，但仍提示“不安全”或部分图片不显示	混合内容 ：页面里还引用了 <code>http://</code> 的图片、脚本	第 10.2 节

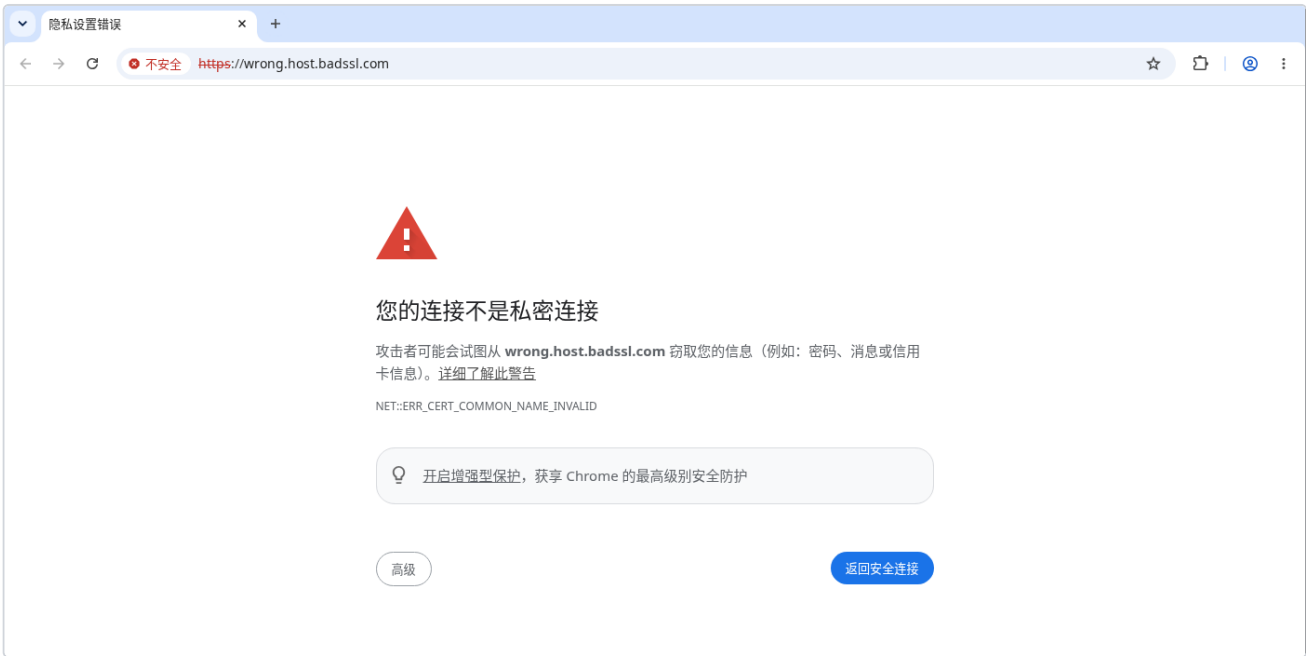
下面三张是真实浏览器（Chrome 154 中文版）里的样子：



真实截图 图 4 没有证书的 http 网站：地址栏显示“不安全”（实验环境演示站点）



真实截图 图 5 证书过期：NET::ERR_CERT_DATE_INVALID（实验环境：用一张已过期的测试证书复现）



真实截图 图 6 证书域名对不上：NET::ERR_CERT_COMMON_NAME_INVALID（公开测试站 wrong.host.badssl.com）

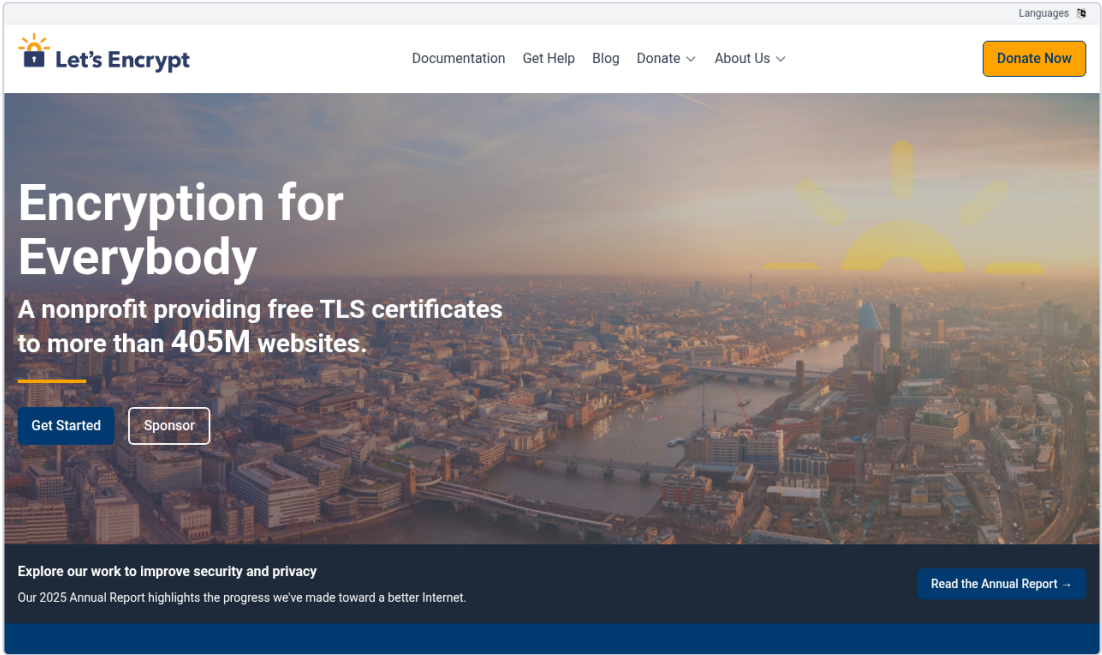
⚠️ 注意

2026 年起，没有 HTTPS 的代价更大了

Google 官方宣布：从 **Chrome 154（2026 年 10 月）** 开始，默认开启“始终使用安全连接”——用户第一次访问一个没有 HTTPS 的公共网站时，Chrome 会先弹出警告、征求同意才打开（来源：Google 安全博客 2025-10-28）。对外贸网站来说，这意味着海外买家可能在看到你的产品之前就被吓走。

1.3 有哪些免费证书

免费证书来源	是什么	有效期	适合谁
Let's Encrypt	非营利机构 ISRG 运营，全球最大的免费 CA	目前 90 天，自动续期	几乎所有托管服务器、宝塔、cPanel
ZeroSSL	商业公司提供的免费档：网页上手动申请免费 3 张 90 天证书；用 ACME 自动化工具申请不限数量	90 天	Let's Encrypt 之外的备选
Cloudflare 通用证书	域名接入 Cloudflare 后自动给访客端发证书，自动续期	由 Cloudflare 管理	路线 D
Cloudflare 源证书 (Origin CA)	只用于“Cloudflare ↔ 你的服务器”这一段，浏览器并不直接信任它	可选 7 天~15 年	路线 D 的源站
宝塔 LiteSSL、cPanel AutoSSL (Sectigo) 等	面板内置的其他免费 DV 证书	约 90 天	路线 B、C



真实截图 图 7 Let's Encrypt 官网首页 (letsencrypt.org, 2026-10-10)

💡 小贴士

名词：ACME、DV

ACME：一套“自动申请和续期证书”的标准协议。Certbot、win-acme、宝塔、cPanel 背后都是它。**DV**（Domain Validation，域名验证）：只验证“你能控制这个域名”的证书。免费证书都是 DV，它和付费证书用的是同样强度的加密（见第 13 章）。

1.4 证书有效期：90 天，而且会越来越短

- Let's Encrypt 现在签发的证书有效期是 **90 天**。
- Let's Encrypt 官方计划（2025-12-02 公告）：**2027-02-10** 起默认改为 **64 天**，**2028-02-16** 起改为 **45 天**。
- 整个行业的规则（CA/浏览器论坛 SC-081 决议）也在收紧：所有公开证书最长有效期 2026-03-15 起 200 天，2027-03-15 起 100 天，2029-03-15 起 47 天。**这意味着：花钱买的“一年证书”以后也不存在了。**
- Let's Encrypt 已于 **2025-06-04** 停止发送证书到期提醒邮件。所以你必须：① 让证书**自动续期**；② 自己设一个**到期监控**（第 10.4 节）。

⚠ 注意 手动续期 = 迟早过期

不要用“每三个月记得登录一次续期”的方式。人一定会忘，而证书过期后网站会整页红色警告。本指南每条路线都会教你确认“自动续期已经开好”。

1.5 开始前你需要准备什么

- 1 **域名控制权**：能登录域名注册商或 DNS 管理后台（阿里云、腾讯云、GoDaddy、Namecheap、Cloudflare.....）。
- 2 **域名已经解析到你的服务器**：即域名的 A 记录（IPv4 地址记录）指向服务器 IP。
- 3 **80 和 443 端口对外开放**：80 是 http 的“门”，证书机构默认通过它来验证你；443 是 https 的“门”。
- 4 **后台管理权限**：SSH（带 sudo 权限）、宝塔、cPanel、Cloudflare、Windows 管理员中的一种。
- 5 （中国大陆服务器）**域名已备案**，见第 3.4 节。

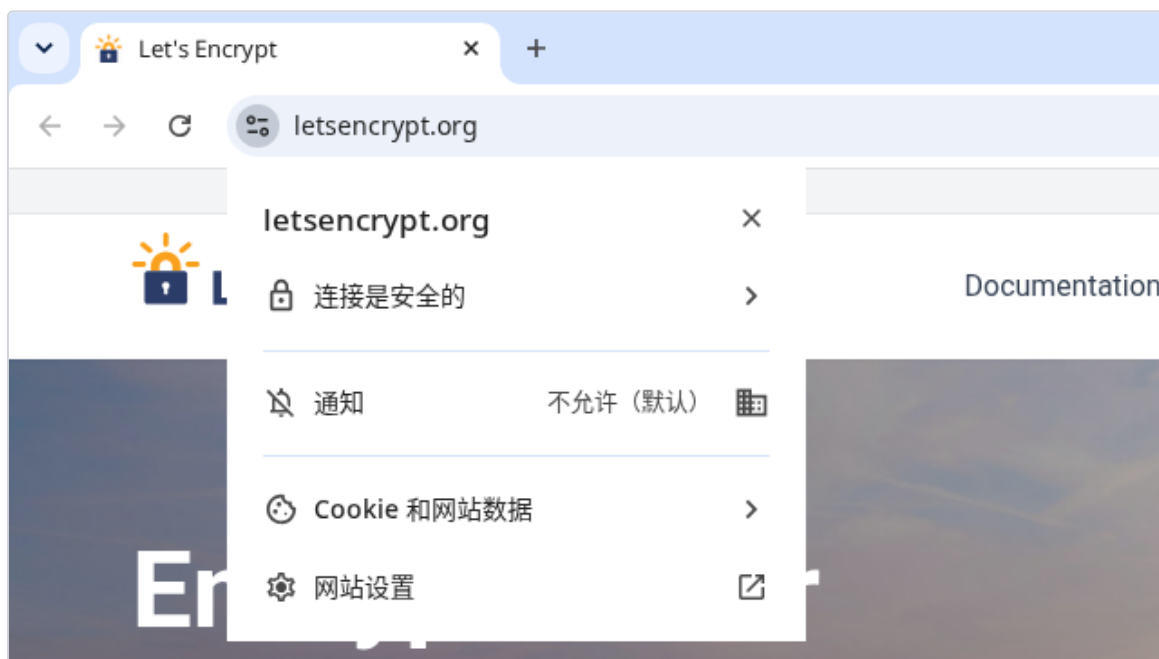
详细的“怎么检查每一项”，在第 3 章预检清单里。

第2章

自查：你的网站现在 HTTPS 正常吗？

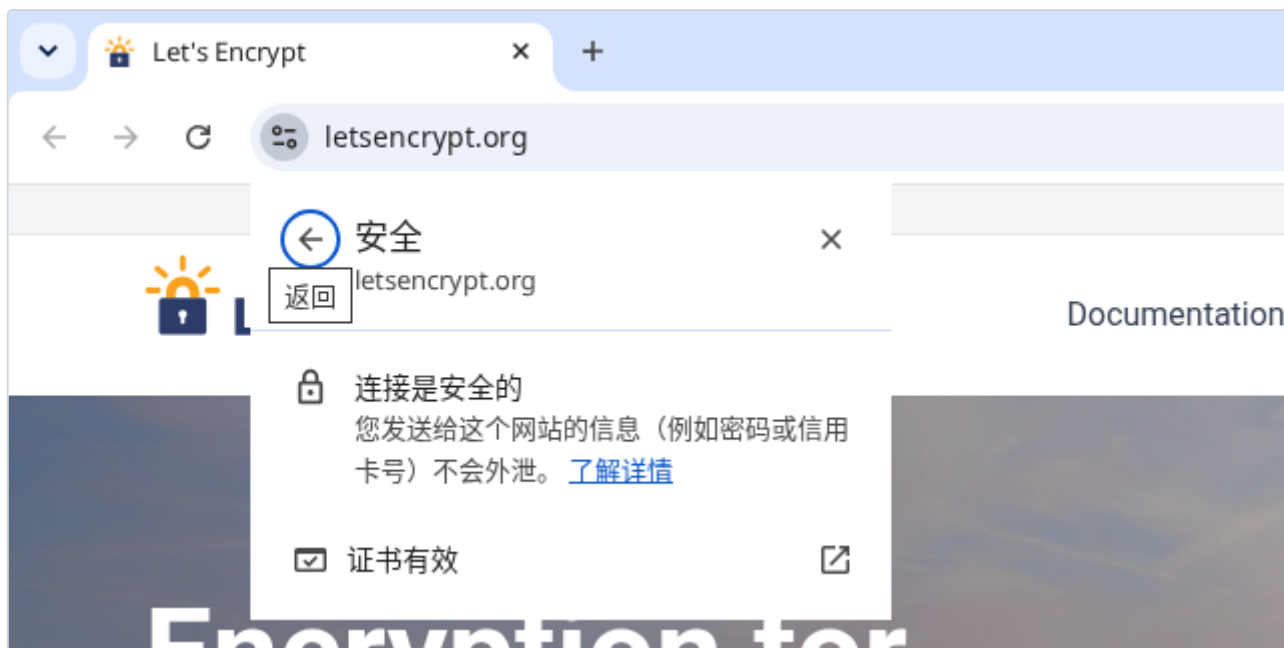
2.1 用 Chrome 浏览器检查（最简单）

- 1 用 Chrome 打开你的网站，网址前面输入 `https://`，例如 `https://www.my-trade-demo.com`。
- 2 看地址栏最左边：
 - 新版 Chrome（117 版以后）不再显示小锁头，而是显示一个“调节”图标（两条横线带小圆点），这是**正常的安全状态**；
 - 如果写着红色或灰色的“**不安全**”，或者整页红色警告，说明有问题。
- 3 点击这个图标，弹出窗口第一行应显示“**连接是安全的**”。



真实截图 图 8 点击地址栏左侧图标后弹出的窗口（letsencrypt.org，2026-10-10）

- 4 点“连接是安全的”，再点“**证书有效**”。



真实截图 图9 点“连接是安全的”后看到“证书有效”

- 5 弹出“证书查看器”。重点看三处：**颁发对象的公用名**（应是你的域名）、**颁发者**（如 Let's Encrypt 的 R12、E8、YE2 等中间证书名）、**有效期的截止日期**。



真实截图 图10 Chrome 证书查看器：颁发对象、颁发者、有效期

💡 小贴士 一定要测这四种网址

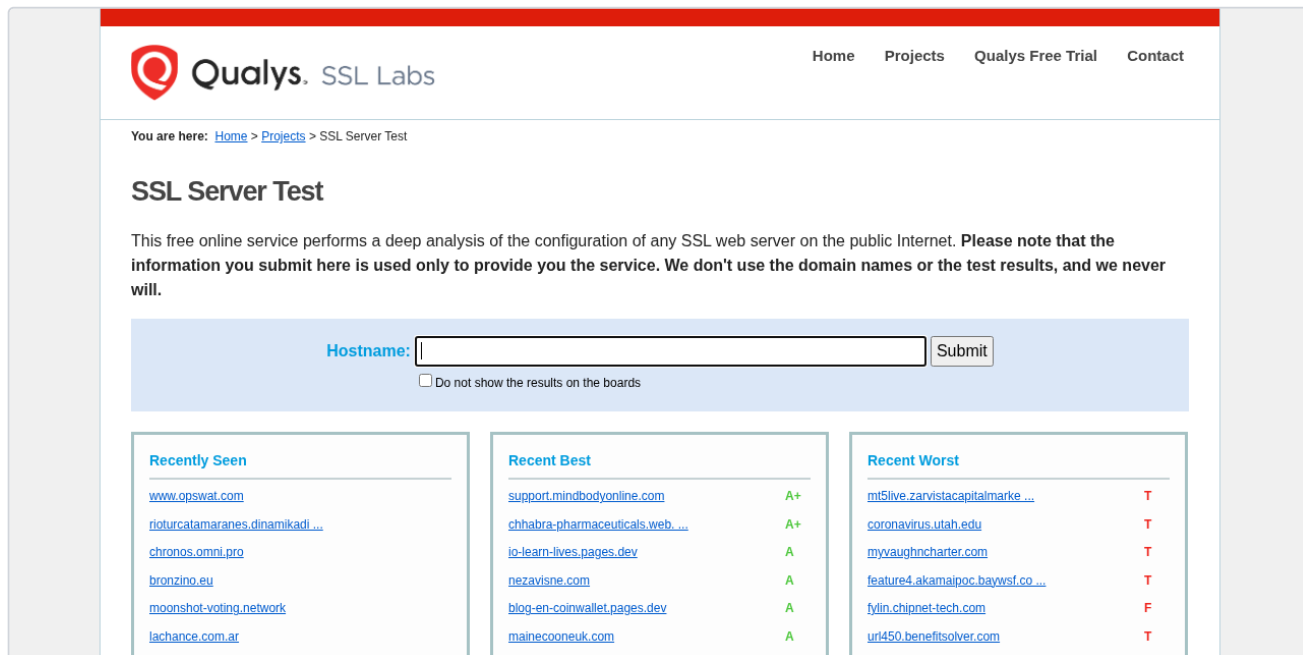
<https://你的域名>、<https://www.你的域名>、<http://你的域名>、<http://www.你的域名>。前两个应该都正常，后两个应该自动跳转到 https。手机上也打开一次（手机浏览器对证书链问题更敏感）。

2.2 用 SSL Labs 在线检测（最全面）

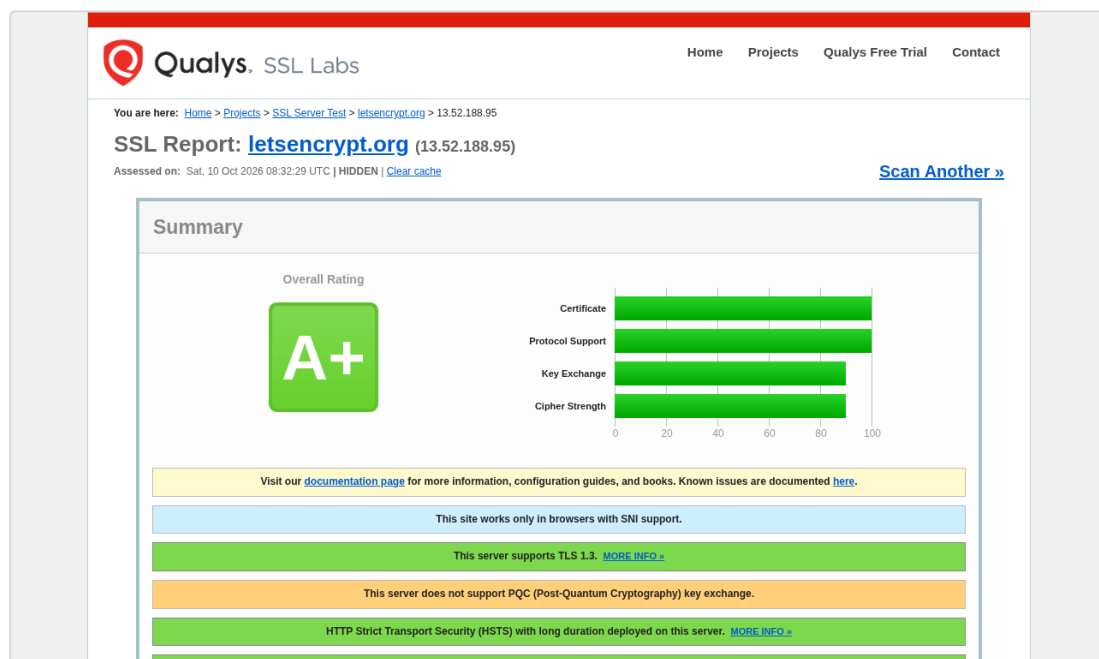
SSL Labs 是 Qualys 公司提供的免费在线检测工具，不用注册。

- 1 打开 <https://www.ssllabs.com/ssltest/>。

- 2 在 **Hostname** 框里输入你的域名（不带 https://），点 **Submit**。
- 3 如果不想让结果出现在公开榜单，勾选 “Do not show the results on the boards”。
- 4 等 1~3 分钟，看总评分：**A 或 A+** 就很好；**B** 也能用；出现 **T**（证书不受信任）或 **F** 必须处理。



真实截图 图 11 SSL Labs 检测首页



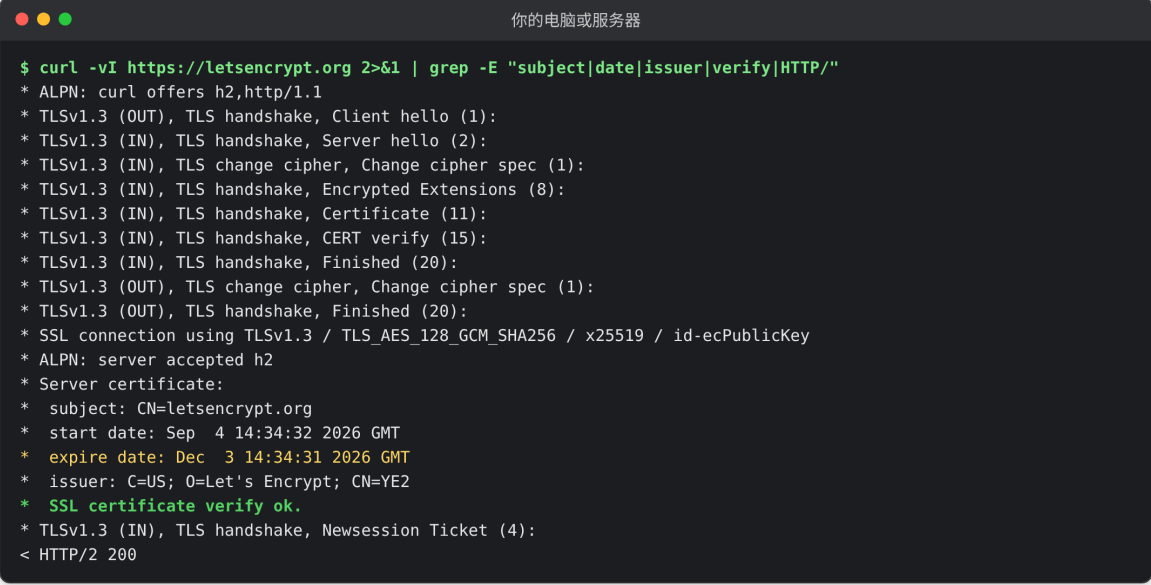
真实截图 图 12 SSL Labs 检测结果示例：letsencrypt.org 获得 A+（2026-10-10）

2.3 用命令检查（给愿意多走一步的人）

BASH

```
curl -vI https://letsencrypt.org 2>&1 | grep -E "subject|date|issuer|verify|HTTP/"
```

逐段解释：`curl` 是一个“命令行浏览器”；`-v` 显示详细过程（包括证书信息）；`-I` 只取响应头；`2>&1 | grep ...` 只把我们关心的几行（证书主体、起止日期、颁发者、校验结果）筛出来。把 `letsencrypt.org` 换成你的域名即可。



```
$ curl -vI https://letsencrypt.org 2>&1 | grep -E "subject|date|issuer|verify|HTTP/"
* ALPN: curl offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_128_GCM_SHA256 / x25519 / id-ecPublicKey
* ALPN: server accepted h2
* Server certificate:
*  subject: CN=letsencrypt.org
*  start date: Sep  4 14:34:32 2026 GMT
*  expire date: Dec  3 14:34:31 2026 GMT
*  issuer: C=US; O=Let's Encrypt; CN=YE2
*  SSL certificate verify ok.
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
< HTTP/2 200
```

真实运行输出 用 curl 查看真实网站的证书（2026-10-10 实测）

真实命令输出 图 13 curl 查看证书：subject（颁发给谁）、start/expire date（起止日期）、issuer（谁颁发的）、verify ok（校验通过）

```
BASH
echo | openssl s_client -connect letsencrypt.org:443 -servername letsencrypt.org 2>/dev/null \
| openssl x509 -noout -subject -issuer -dates
```

逐段解释：`openssl s_client` 像浏览器一样连接网站的 443 端口并取回证书；`-servername` 告诉服务器你要的是哪个域名（一台服务器常有多个网站）；第二个 `openssl x509` 把证书内容翻译成人能看懂的字；`notAfter` 就是到期时间（GMT 时间，北京时间要加 8 小时）。



```
$ echo | openssl s_client -connect letsencrypt.org:443 -servername letsencrypt.org 2>/dev/null \
| openssl x509 -noout -subject -issuer -dates
subject=CN=letsencrypt.org
issuer=C=US, O=Let's Encrypt, CN=YE2
notBefore=Sep  4 14:34:32 2026 GMT
notAfter=Dec  3 14:34:31 2026 GMT

$ curl -sI https://expired.badssl.com
curl: (60) SSL certificate problem: certificate has expired
```

真实运行输出 上：正常证书；下：过期证书的报错（2026-10-10 实测）

真实命令输出 图 14 openssl 查看到期日；下方是访问过期证书网站时 curl 的报错

说明 自查结果怎么用

全部正常：恭喜，直接跳到第 10.3 节确认自动续期即可。有问题：继续读第 3 章，做完预检再进入你的路线章节。

第3章

动手前的准备：预检清单

很多人失败，不是因为不会装证书，而是因为前提条件没满足。下面 7 项检查全部是“只看不改”，放心做。

3.1 预检清单（打勾再开始）

#	检查项	怎么查	合格标准	不合格怎么办
1	域名 A 记录指向服务器	nslookup 你的域名，或 dns.google 查 type=A	显示的 IP = 你的服务器公网 IP（云控制台里能看到）	到 DNS 后台把 A 记录改成服务器 IP，等 10 分钟~24 小时生效
2	www 也解析了	nslookup www.你的域名	同上（或是指向主域名的 CNAME）	补一条 www 的 A 记录或 CNAME 记录
3	没有错误的 AAAA 记录	dns.google 查 type=AAAA	没有结果，或是服务器真实的 IPv6 地址	删除指向旧服务器的 AAAA（IPv6）记录——这是验证失败的隐形杀手
4	80 端口外网可达	在另一台电脑/手机流量下打开 http://你的域名	能打开网页（哪怕是默认欢迎页、403 页）	见 3.2 节放行端口
5	443 端口开放	curl -vI https://你的域名	能看到 TLS 握手过程（即使证书报错）	见 3.2 节
6	没有 CAA 记录阻挡	dns.google 查 type=CAA	没有结果，或包含 letsencrypt.org	让 DNS 管理员加一条允许 letsencrypt.org 的 CAA 记录或删除旧记录
7	中国大陆服务器已备案	问建站公司 / 云控制台备案页	已备案，或服务器在境外	见 3.4 节

💡 小贴士 名词：A 记录、CNAME、CAA

A 记录：“域名 → IPv4 地址”的对应关系。**AAAA 记录：**“域名 → IPv6 地址”。**CNAME：**“这个域名 = 另一个域名”的别名。**CAA 记录：**规定“只有哪些证书机构可以给我的域名发证书”的白名单；没有这条记录就代表谁都可以。

3.2 放行 80 / 443 端口：两道门都要开

云服务器的端口有两道门：云厂商控制台里的“安全组”（像小区大门），和服务器系统里的“防火墙”（像家门）。两道都要放行 TCP 80 和 443。

第一道门：云安全组（在网页控制台点）

- 登录云控制台，找到你的服务器实例。
 - 阿里云 ECS：实例详情 → 安全组 → 配置规则 → 入方向 → 手动添加；
 - 腾讯云 CVM：实例 → 安全组 → 修改规则 → 入站规则 → 添加规则；轻量应用服务器：实例 → 防火墙 → 添加规则；
 - AWS EC2：实例 → Security → 点安全组 → Edit inbound rules → Add rule（类型选 HTTP、HTTPS）。
- 添加两条规则：协议 TCP，端口 80，来源 0.0.0.0/0；协议 TCP，端口 443，来源 0.0.0.0/0。
- 保存。一般立即生效。



示意图 图 15 云安全组添加 80/443 入方向规则（以阿里云 ECS 为例，菜单名称以实际控制台为准）

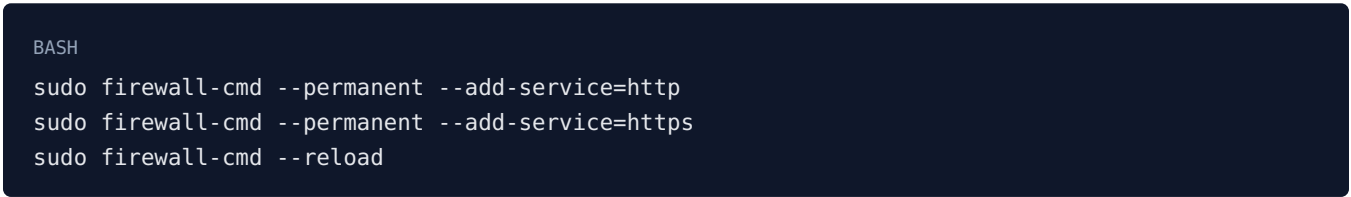
第二道门：系统防火墙（用命令）



命令清单 图 16 Ubuntu/Debian 用 ufw，CentOS/Rocky 用 firewalld



逐行解释：第 1 行查看 ufw 防火墙状态，如果显示 `Status: inactive`（未启用），说明这道门本来就开着，后两行可以不做；第 2、3 行分别放行 80 和 443。CentOS / Rocky / AlmaLinux 用：



`--permanent` 表示重启后依然有效，`--reload` 让设置马上生效，看到 `success` 即可。

⚠ 注意 别把 22 端口对全世界敞开

SSH 用的 22 端口，建议在安全组里只允许你办公室的 IP 访问。放行 80/443 是必须的，放行 22 给所有人不是。

3.3 DNS 生效需要时间

改了 DNS 记录或 NS 后，全世界的 DNS 服务器需要时间“同步”，通常几分钟到几小时，最长可达 48 小时。判断是否生效：用 `dns.google` 查（它查的是全球公共 DNS 的结果），看到新的 IP 再申请证书，可以避免“验证失败”。

3.4 中国大陆服务器与 ICP 备案（简要说明）

- 按国内规定，域名解析到**中国大陆服务器**、对外提供网站服务，必须先完成**ICP 备案**。以阿里云为例，其官方帮助文档写明：未在阿里云备案的域名解析到阿里云中国内地服务器，**会被监测系统识别并阻断网站访问**。其他云厂商请咨询其客服。
- 被阻断时，Let's Encrypt 的 HTTP 验证也到不了你的网站，表现为“验证失败 / 连接超时 / 返回备案提示页”。
- 用 DNS 验证可以拿到证书，但**网站本身依然会被阻断**——证书解决不了备案问题，也不要尝试绕过。
- **服务器在境外（含香港）则不需要 ICP 备案**。外贸网站主要面向海外客户，很多公司本来就用境外服务器。
- 备案只和“服务器在哪里”有关，和“证书是哪家的”无关。

i 说明 本节为简要说明

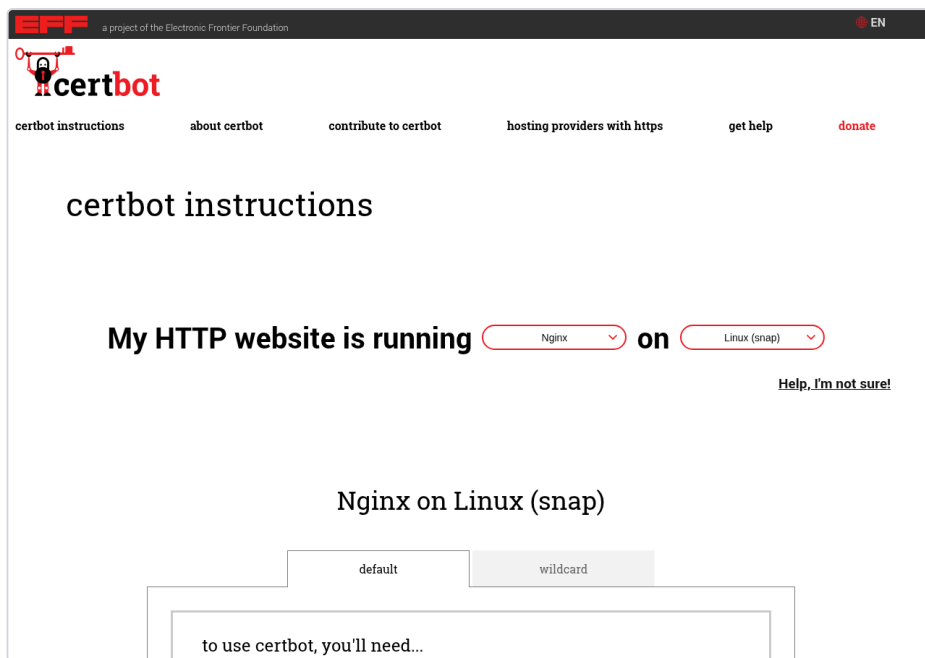
备案的具体流程、时限以工信部和你的云厂商最新规定为准。本指南只说明它与证书验证的关系。

第4章

路线 A: Linux 云服务器 + Certbot (Nginx / Apache)

适合: 你或技术人员能用 SSH 登录 Linux 服务器 (有 sudo 权限)，网站跑在 Nginx 或 Apache 上。**用时:** 15~30 分钟。

Certbot 是 EFF (电子前哨基金会, 美国非营利组织) 开发的免费工具, 能自动申请 Let's Encrypt 证书、自动改好 Nginx/Apache 配置、自动续期。官方安装向导: <https://certbot.eff.org/instructions>。



真实截图 图 17 Certbot 官方安装向导 (选择 Nginx + Linux (snap))

4.1 第 0 步: 登录服务器

- 1 Windows 用户: 打开“Windows 终端”或“PowerShell” (Windows 10/11 自带 ssh 命令); Mac 用户: 打开“终端”。也可以用云厂商网页控制台里的“远程连接 / Workbench / VNC”。
- 2 输入 (把 IP 换成你的服务器 IP, 把 `root` 换成你的用户名):

```
BASH
ssh root@47.xx.xx.xx
```

- 3 第一次连接会问 `Are you sure you want to continue connecting (yes/no)?`, 输入 `yes` 回车。
- 4 输入密码 (输入时屏幕不会显示任何字符, 这是正常的), 回车。
- 5 看到类似 `root@server:~#` 或 `ubuntu@server:~$` 的提示符, 说明登录成功。

💡 小贴士 先确认系统和网页软件

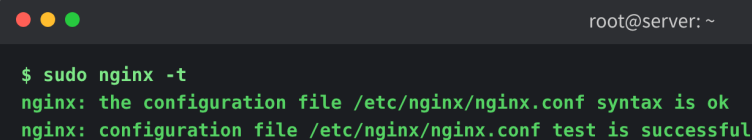
输入 `cat /etc/os-release` 看系统 (Ubuntu / Debian / CentOS / Rocky)。输入 `nginx -v` 和 `apache2 -v` (CentOS 上是 `httpd -v`) 看用的是哪个网页软件——哪个能显示版本号就是哪个。

4.2 第 1 步：备份配置并确认网站能用 http 打开

```
BASH
sudo cp -a /etc/nginx /root/nginx-backup-$(date +%F)
sudo nginx -t
curl -sI http://example.com | head -1
```

逐行解释：

- 1 把整个 Nginx 配置目录复制一份到 `/root/`，文件夹名带今天日期（出问题时可以原样恢复）。Apache 换成 `sudo cp -a /etc/apache2 /root/apache2-backup-$(date +%F)`（CentOS 是 `/etc/httpd`）。
- 2 检查当前配置语法。应看到 `syntax is ok` 和 `test is successful`。
- 3 确认网站 http 能访问，应看到 `HTTP/1.1 200 OK`（或 301/403）。



```
root@server: ~
$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

真实运行输出 改完 Nginx 配置后，先用 `nginx -t` 检查语法（真实输出）

真实命令输出 图 18 nginx -t 检查通过

⚠ 注意 配置里要写对域名

Certbot 靠配置文件里的 `server_name` (Nginx) 或 `ServerName` / `ServerAlias` (Apache) 找到你的网站。用 `grep -R "server_name" /etc/nginx/` 看一眼，必须包含你要申请的域名，例如 `server_name example.com www.example.com;`。

4.3 第 2 步：安装 Certbot

方法一（官方推荐）：snap 安装

```
BASH
sudo apt-get remove certbot
sudo snap install --classic certbot
sudo ln -s /snap/bin/certbot /usr/local/bin/certbot
```

逐行解释：

- 1 先删掉系统里可能存在的旧版 certbot（没有装过会提示“未安装”，没关系）。
- 2 用 snap（Ubuntu 自带的软件商店）安装最新版 Certbot。`--classic` 是官方要求的参数。
- 3 建一个“快捷方式”，让你在任何地方都能直接输入 `certbot`。如果提示 `File exists`，说明已经有了，忽略即可。

说明 Debian 上先装 snapd

Ubuntu 默认带 snap。Debian 需要先运行 `sudo apt update && sudo apt install snapd`，然后 `sudo snap install core`，再执行上面的命令。

方法二：用系统软件源 (apt / dnf) 安装

```
BASH
sudo apt update
sudo apt install certbot python3-certbot-nginx
```

Apache 用户把第二行换成 `sudo apt install certbot python3-certbot-apache`。系统源的版本可能比 snap 旧一些，但同样能用、同样自带自动续期。本指南的实验环境 (Debian 13) 用的就是这种方式，装上的是 Certbot 4.0.0。

CentOS / RHEL / Rocky / AlmaLinux

```
BASH
sudo dnf install epel-release
sudo dnf install certbot python3-certbot-nginx
```

逐段解释：第 1 行启用 EPEL (Fedora 社区维护的扩展软件源，certbot 在这里面)；第 2 行安装 Certbot 和 Nginx 插件。Apache (在这些系统里叫 httpd) 用户安装 `python3-certbot-apache mod_ssl`。老的 CentOS 7 用 `yum` 代替 `dnf` (CentOS 7 已停止维护，建议尽早升级系统)。

4.4 第 3 步：一条命令申请并安装证书 (Nginx)

```
BASH
sudo certbot --nginx -d example.com -d www.example.com
```

逐段解释：`--nginx` 表示“用 Nginx 插件：自动验证 + 自动改配置”；每个 `-d` 后面跟一个域名，根域名和 `www` 都要写 (把 `example.com` 换成你的域名)。

第一次运行会问你几个问题：

- 1 `Enter email address`：填一个常用邮箱 (用于重要通知；Let's Encrypt 已不再发到期提醒)。
- 2 `Please read the Terms of Service ... (Y)es/(N)o`：输入 `Y` 同意服务条款。
- 3 `Would you be willing ... to share your email address with the EFF`：是否订阅 EFF 新闻，`Y` 或 `N` 都可以。
- 4 等待十几秒，看到下面这样的输出就成功了：

```
root@server: ~ (实验环境 Debian 13 / Certbot 4.0.0)

$ sudo certbot --nginx -d example.com -d www.example.com \
  --email admin@example.com --agree-tos --no-eff-email
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Account registered.
Requesting a certificate for example.com and www.example.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/example.com/fullchain.pem
Key is saved at: /etc/letsencrypt/live/example.com/privkey.pem
This certificate expires on 2027-01-08.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for example.com to /etc/nginx/sites-enabled/example.com
Successfully deployed certificate for www.example.com to /etc/nginx/sites-enabled/example.com
Congratulations! You have successfully enabled HTTPS on https://example.com and https://www.example.com

- - - - -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
 * Donating to EFF: https://eff.org/donate-le
- - - - -
```

真实运行输出 在本地测试 CA (Let's Encrypt 官方测试服务器 Pebble) 上真实运行; 实验时另加了 --server 参数指向测试 CA, 你在正式环境不需要加。

真实命令输出 图 19 certbot --nginx 成功申请并部署证书

你应该看到的关键字:

- **Successfully received certificate.**: 证书拿到了;
- **This certificate expires on ...**: 到期日 (约 90 天后);
- **Certbot has set up a scheduled task to automatically renew**: 自动续期已安排;
- **Congratulations! You have successfully enabled HTTPS**: 已经部署到 Nginx。

Certbot 自动改了你的 Nginx 配置: 加了 443 端口和证书路径, 并把 80 端口的访问 **301 跳转**到 https。带 **# managed by Certbot** 的行就是它加的:

```
root@server: ~

$ sudo cat /etc/nginx/sites-enabled/example.com
server {
    server_name example.com www.example.com;
    root /var/www/example.com;
    index index.html;

    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/example.com/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/example.com/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}

server {
    if ($host = www.example.com) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    if ($host = example.com) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    listen 80;
    server_name example.com www.example.com;
    return 404; # managed by Certbot
}
```

真实运行输出 Certbot 自动改写后的 Nginx 配置 (真实文件内容)。带 “# managed by Certbot” 的行都是它加的。

真实命令输出 图 20 Certbot 修改后的 Nginx 配置文件

💡 小贴士 想自己改配置?

用 `sudo certbot certonly --nginx -d example.com -d www.example.com` 只申请证书、不改配置。证书在 `/etc/letsencrypt/live/example.com/fullchain.pem`，私钥在 `/etc/letsencrypt/live/example.com/privkey.pem`，在 Nginx 里分别填到 `ssl_certificate` 和 `ssl_certificate_key`。私钥文件不要发给任何人。

4.5 Apache 用户

```
BASH
sudo certbot --apache -d example.com -d www.example.com
```

和 Nginx 完全一样，只是把 `--nginx` 换成 `--apache`。Certbot 会新建一个 `-le-ssl.conf` 结尾的配置文件，并加好跳转。完成后检查：

```
BASH
sudo apachectl configtest
```

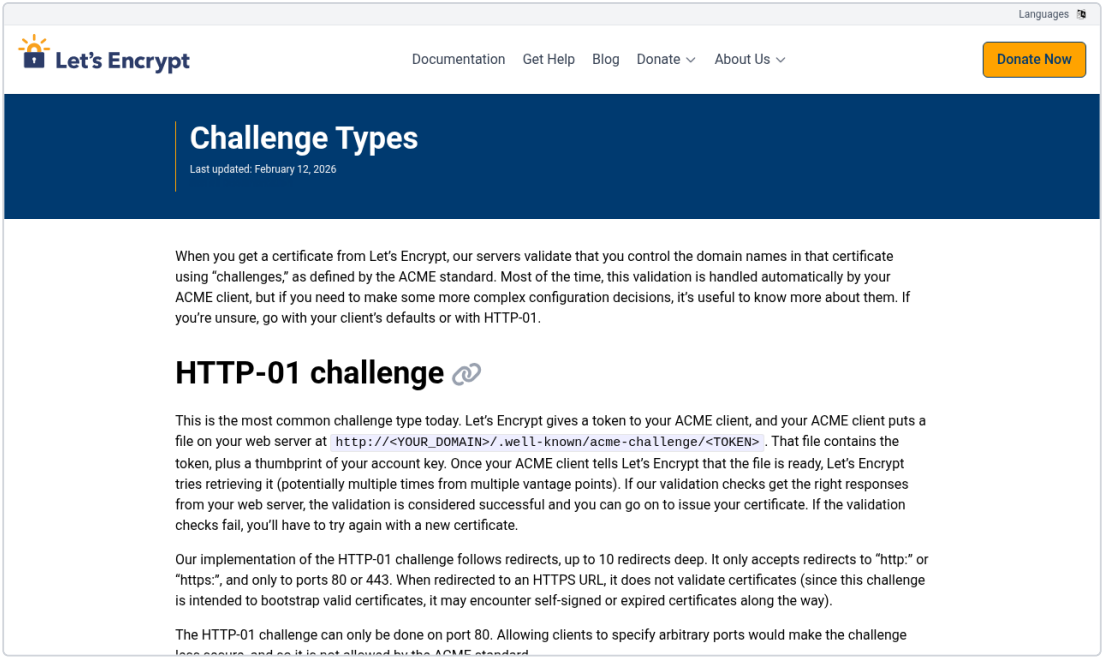
应看到 `Syntax OK`。CentOS 上如果报 `mod_ssl` 相关错误，先 `sudo dnf install mod_ssl` 再重试。

4.6 没法用插件时：webroot 方式

如果你的网站是 Docker、Node.js 等特殊架构，Certbot 插件识别不了，可以用 **webroot**（网站根目录）方式：

```
BASH
sudo certbot certonly --webroot -w /var/www/html -d example.com -d www.example.com
```

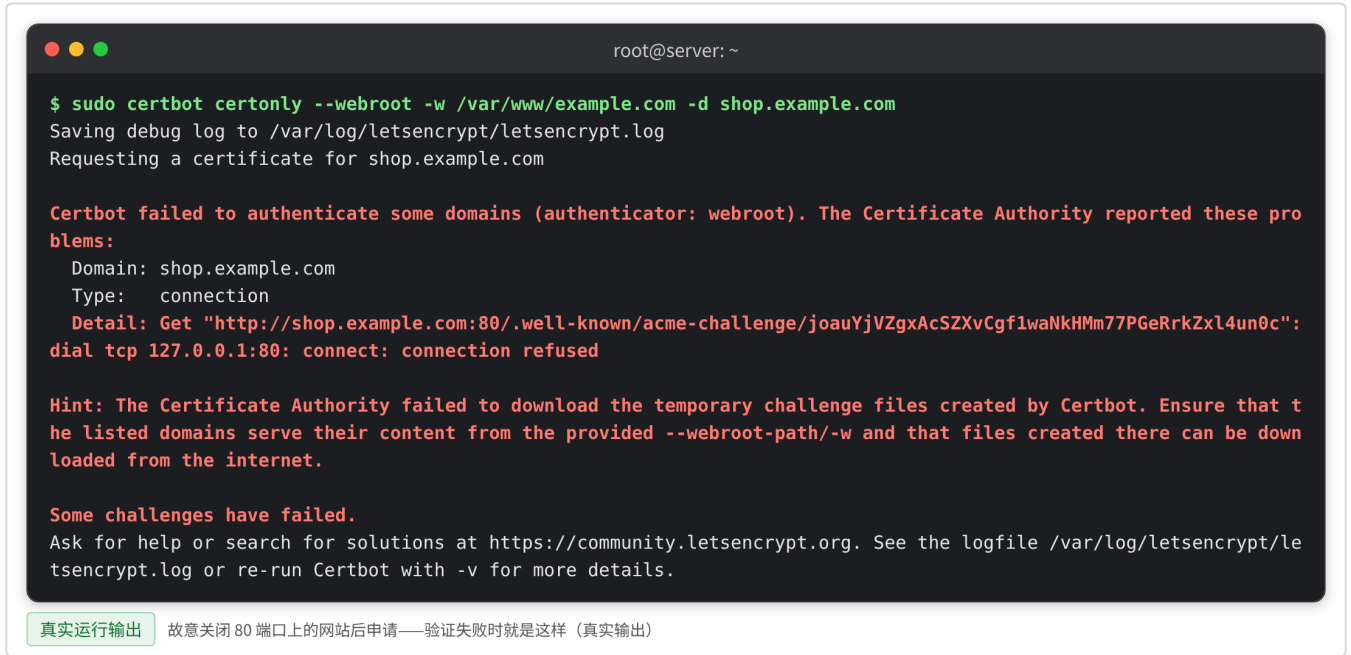
`-w` 后面填网站文件所在目录。Certbot 会在其中的 `.well-known/acme-challenge/` 放一个临时文件，Let's Encrypt 通过 `http://你的域名/.well-known/acme-challenge/...` 读取它来确认你控制该域名。拿到证书后需要手动配置到网页软件里。



真实截图 图 21 Let's Encrypt 官方文档“验证方式（Challenge Types）”页面，介绍 HTTP-01 与 DNS-01

4.7 验证失败长什么样

下面是实验中故意关掉 80 端口上的网站后申请证书的真实输出。看到 `Type: connection` 和 `connection refused / Timeout`，就是 Let's Encrypt 连不上你的 80 端口：



真实运行输出 故意关闭 80 端口上的网站后申请——验证失败时就是这样（真实输出）

真实命令输出 图 22 验证失败：Let's Encrypt 无法访问 80 端口

输出里的关键词	意思	怎么办
<code>Type: connection</code> + <code>Timeout</code>	80 端口被安全组/防火墙挡住	第 3.2 节
<code>Type: connection</code> + <code>connection refused</code>	服务器没有程序在 80 端口上运行	启动 Nginx/Apache: <code>sudo systemctl start nginx</code>
<code>Type: dns</code> + <code>NXDOMAIN</code>	域名没有解析	第 3.1 节第 1~2 项

输出里的关键词	意思	怎么办
Type: unauthorized + 404	访问到的不是这台服务器，或网站有重写/跳转规则	检查 A/AAAA 记录、伪静态规则
too many failed authorizations	失败次数太多被暂时限制（同一域名每小时 5 次）	等一小时，先排查再试，可加 <code>--dry-run</code> 测试

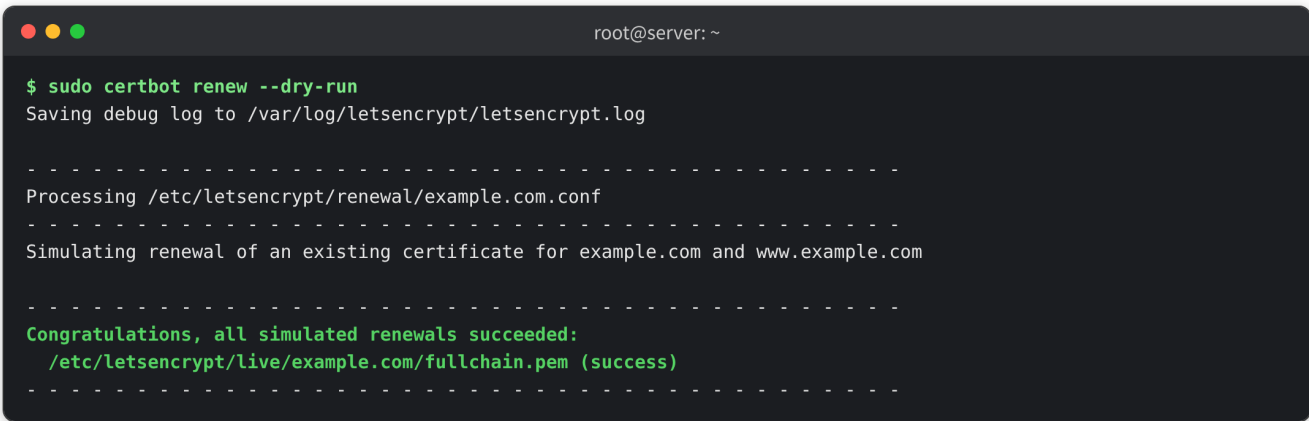
⚠ 注意 别反复狂试

Let's Encrypt 有频率限制：同一组域名 7 天内最多签发 5 次；同一个域名验证失败每小时最多 5 次。排查问题时，在命令后加 `--dry-run`（只演练、不真正签发）或 `--test-cert`（用测试服务器）。

4.8 第 4 步：确认自动续期

```
BASH
sudo certbot renew --dry-run
sudo certbot certificates
```

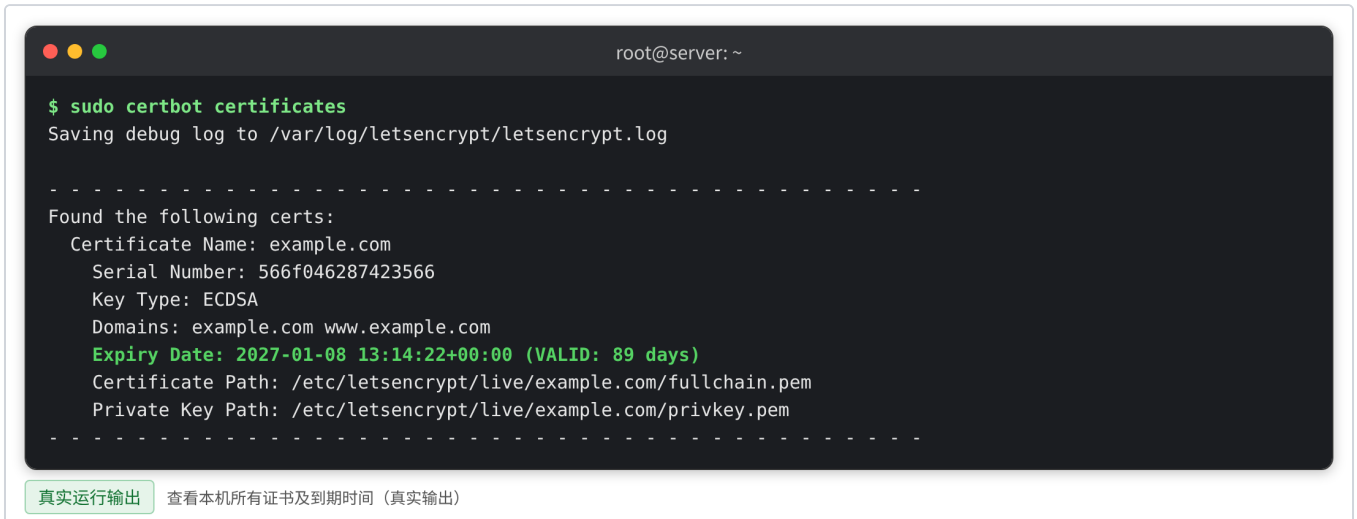
第 1 行“演练续期”：不会真正替换证书，只检查续期流程能不能走通。看到 `Congratulations, all simulated renewals succeeded` 即正常。第 2 行列出本机所有证书和剩余天数。

A terminal window with a dark background and light green text. The prompt is 'root@server: ~'. The command '\$ sudo certbot renew --dry-run' is entered. The output shows 'Saving debug log to /var/log/letsencrypt/letsencrypt.log', followed by a separator line. It then says 'Processing /etc/letsencrypt/renewal/example.com.conf', another separator line, and 'Simulating renewal of an existing certificate for example.com and www.example.com'. After another separator line, it displays 'Congratulations, all simulated renewals succeeded:' and '/etc/letsencrypt/live/example.com/fullchain.pem (success)'. The terminal ends with a final separator line.

真实运行输出

模拟续期成功的样子（真实输出；实验环境指向本地测试 CA）

真实命令输出 图 23 certbot renew --dry-run 演练续期成功



真实命令输出 图 24 certbot certificates 查看证书和剩余天数

Certbot 安装时会自动建好定时任务 (每天两次检查, 到期前约 30 天自动续期)。确认方法:



snap 安装的名字是 `snap.certbot.renew.timer`, apt 安装的是 `certbot.timer` (没有 systemd 的系统则是 `/etc/cron.d/certbot` 定时任务)。



真实命令输出 图 25 apt 版 Certbot 自带的续期定时器和 cron 文件内容

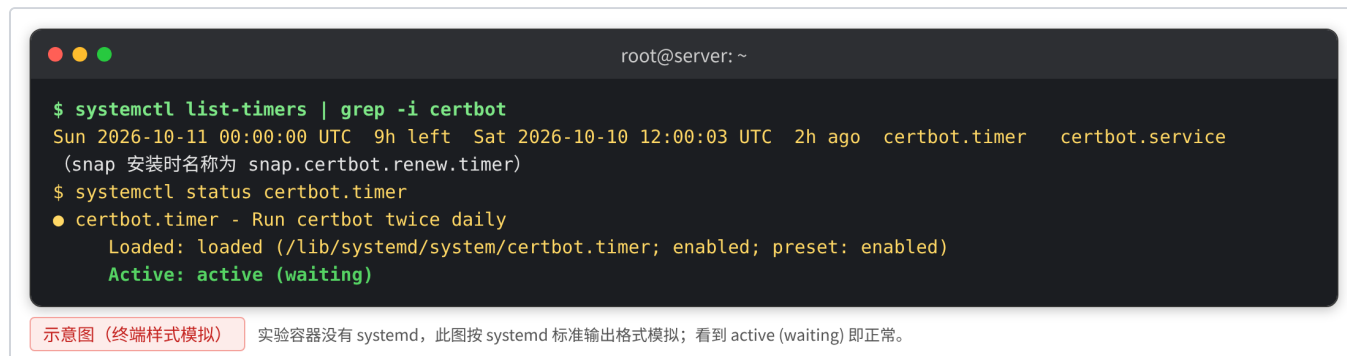


示意图 图 26 systemctl list-timers 的正常输出 (终端样式模拟)

4.9 第 5 步: 打开浏览器验收

- 1 访问 `http://你的域名`, 应自动跳到 `https://`。
- 2 按第 2.1 节查看证书和到期日。
- 3 按第 2.2 节跑一次 SSL Labs。
- 4 用 `curl -I http://你的域名` 确认返回 `301 Moved Permanently` :



真实命令输出 图 27 HTTP 自动 301 跳转到 HTTPS

i 说明 关于本章截图的实验环境

为了给你看“真实的输出”，又不去碰任何真实网站，本章的命令是在一台 Debian 13 实验服务器上运行的，证书由 Let's Encrypt 官方开源的测试 CA 程序 **Pebble** 签发（命令里额外加了 `--server` 指向它）。你在正式服务器上不需要这个参数，输出内容和格式与正式环境一致，只是正式环境的证书由 Let's Encrypt 签发。

第5章

路线 B：宝塔面板

适合： 服务器装了宝塔 Linux 面板（BT Panel，国内常用的服务器管理面板）。**用时：** 5~10 分钟，全程点鼠标。以下菜单名称依据宝塔官方文档（docs.bt.cn，2026-09-30 最新版），不同版本可能略有差异。



真实截图 图 28 宝塔面板官网首页 (bt.cn)

5.1 申请前确认

- 1 域名已解析到这台服务器（第 3.1 节）。
- 2 安全组已放行 80、443（第 3.2 节）。宝塔自带的“安全”页面里也有系统防火墙，确认 80、443 已放行。
- 3 在宝塔里已经建好这个站点，并且“域名管理”里根域名和 www 都已绑定。
- 4 如果站点开了 CDN、反向代理或 301 重定向，先临时关闭——官方文档提示这些会导致验证或续签失败。

5.2 用“文件验证”申请 Let's Encrypt（最常用）

- 1 登录宝塔面板（地址形如 `https://服务器IP:端口/安全入口`，安装时终端里给出）。
- 2 点左侧菜单 **网站**。在网站列表里点你的**站点域名**（或该行右侧的“设置”）。

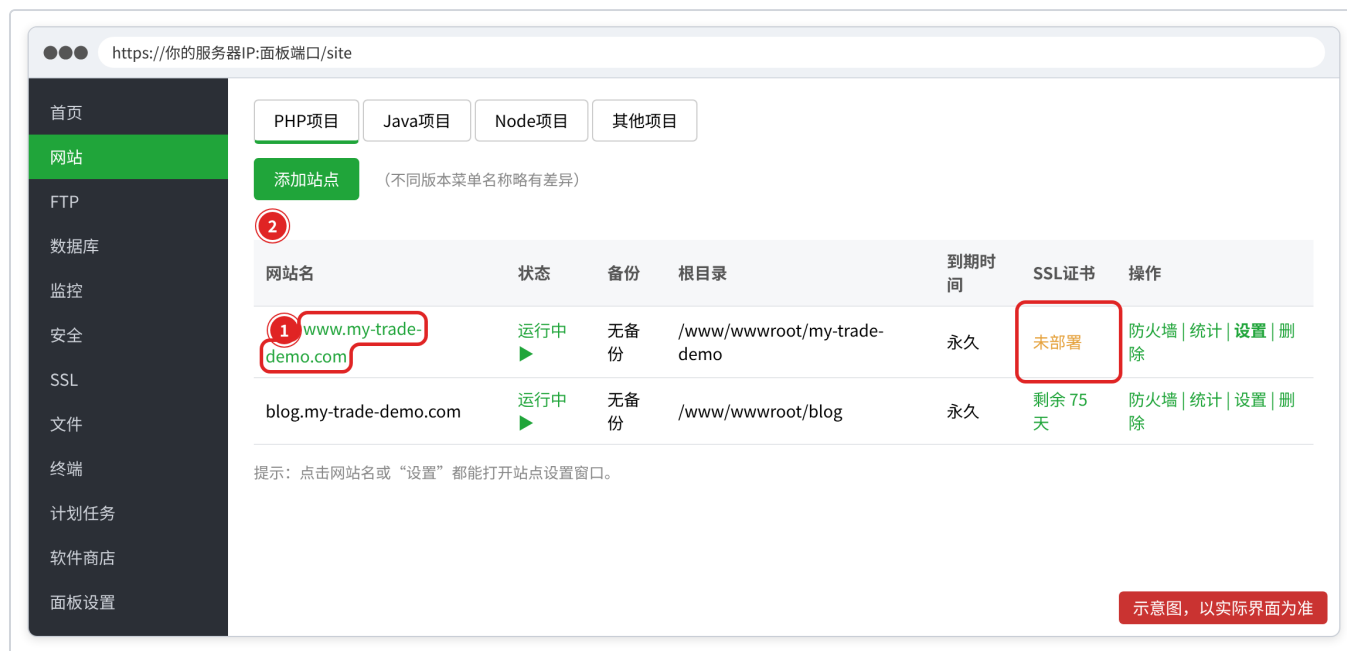


示意图 图 29 宝塔：网站列表，点击站点名或“设置”

- 3 弹出“站点修改”窗口，点左侧的 **SSL**。
- 4 选 **Let's Encrypt** 标签（部分新版本叫“免费证书”）。
- 5 点 **申请证书**。

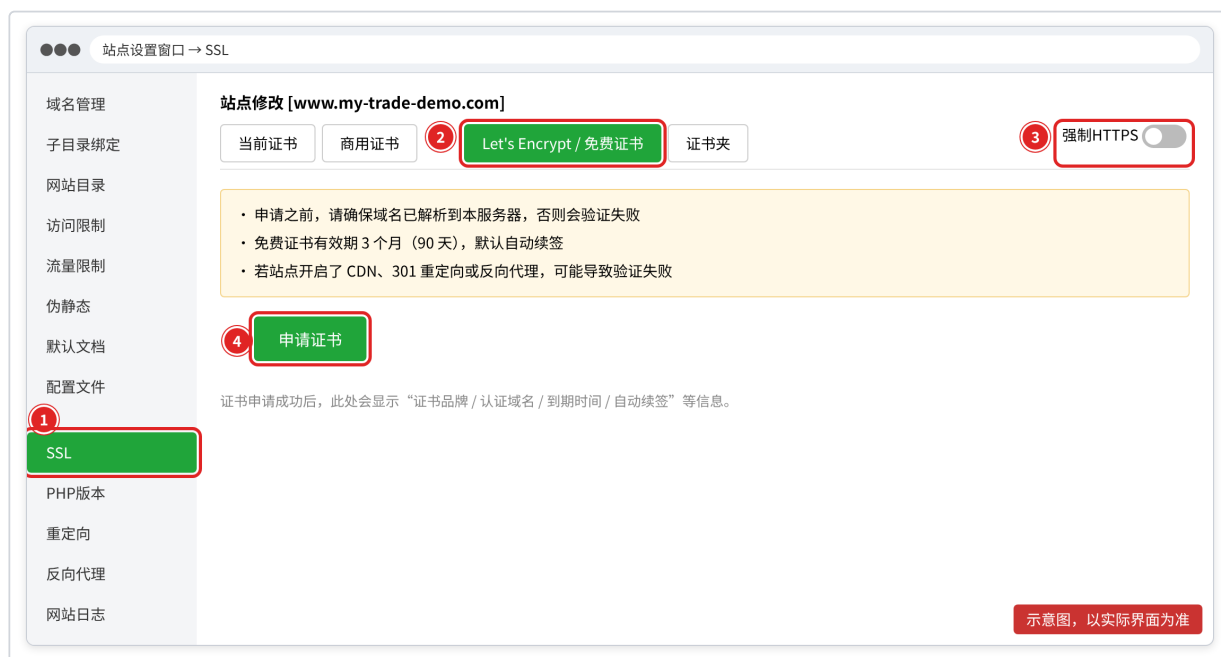


示意图 图 30 宝塔：站点设置 → SSL → Let's Encrypt → 申请证书；右上角是“强制HTTPS”开关

- 6 在弹出的对话框里依次选择：
 - 证书品牌：Let's Encrypt（国际通用）。宝塔也提供 LiteSSL，官方文档称其国内访问更稳定，外贸站两者都可以；
 - 证书算法：RSA2048（兼容性最好，默认推荐）；
 - 验证方式：文件验证；
 - 域名：把根域名和 www 都勾上。
 - 7 点 申请证书，等待几十秒。



示意图 图 31 宝塔：申请证书对话框

- 8 成功后，SSL 页面会显示证书品牌、认证域名、到期时间，状态为已部署。如果需要手动点“保存”，就点一下。

你应该看到：SSL 页显示“剩余 89 天”左右，网站列表的“SSL 证书”一列从“未部署”变成剩余天数。

如果失败：

提示	处理
验证失败 / 无法访问验证文件	检查域名解析、80 端口、是否开了 301/CDN/反向代理
域名未解析 / 解析错误	第 3.1 节，等 DNS 生效后再申请
申请过于频繁	等一小时再试（Let's Encrypt 频率限制）
申请成功但 https 打不开	官方提示：检查安全组是否放行 443 端口

5.3 开启强制 HTTPS

- 1 还在站点设置 → SSL 页面，找到右上角的 **强制 HTTPS** 开关，打开。
- 2 用无痕窗口访问 `http://你的域名`，应自动跳转到 https。

⚠ 注意 开强制 HTTPS 前先检查跳转规则

宝塔官方提示：开启强制 HTTPS 之前，确保站点没有做其他 301 跳转（伪静态规则或 JS 跳转），否则可能出现无限跳转。

5.4 通配符证书：用 DNS 验证

如果你有很多子域名（`shop.`、`m.`、`blog.`），可以申请一张 `*.你的域名` 的 **通配符证书**。通配符证书只能用 **DNS 验证**（证明你能修改域名的 DNS 记录）。

- 1 先到 DNS 服务商（阿里云、腾讯云 DNSPod、Cloudflare 等）后台创建 API 密钥（AccessKey/SecretKey 或 API Token），权限尽量只给“DNS 解析管理”。
- 2 宝塔左侧菜单 **SSL** → **域名管理** → **DNS 接口设置** → **添加 DNS 接口**，选择服务商，填入密钥，点确定。



示意图 图 32 宝塔：SSL → 域名管理 → DNS接口设置 → 添加DNS接口

- 3 回到站点设置 → SSL → Let's Encrypt → 申请证书，验证方式选 **DNS 验证**，选择刚添加的 DNS 接口，勾选域名（含通配符），申请。
- 4 宝塔会自动添加验证用的 TXT 记录、完成验证、签发证书，之后也能自动续签。

💡 小贴士 名词：TXT 记录、通配符

TXT 记录：一条写着任意文字的 DNS 记录，常用来“证明身份”。**通配符证书** `*.example.com`：覆盖所有一级子域名（`www.`、`shop.`），但不包括 `example.com` 本身，也不覆盖 `a.b.example.com`，所以申请时通常同时勾选根域名。

5.5 确认自动续签

宝塔官方文档说明：免费证书有效期 3 个月，**默认自动续签**。建议在到期前一个月左右回到 SSL 页面看一眼剩余天数是否已经刷新；同时按第 10.4 节设置一个外部到期监控，双保险。

第6章

路线 C: cPanel 虚拟主机 (AutoSSL)

适合: 你买的是虚拟主机 (共享主机), 后台叫 cPanel (地址常为 `https://你的域名:2083` 或主机商面板里的“cPanel 登录”按钮)。**用时:** 5 分钟。

cPanel 有一个叫 **AutoSSL** 的功能: 自动给你账户下的所有域名申请免费 DV 证书 (通常来自 Let's Encrypt 或 Sectigo), 并自动续期。很多主机商默认已经开启, 你只需要检查 and 点一下按钮。

6.1 检查并运行 AutoSSL

- 1 登录 cPanel。
- 2 在 **Security (安全)** 区域找到 **SSL/TLS Status** (新版 cPanel 中它也可能是 **SSL/TLS Certificates** 里的一个标签页; 使用新版“Security hub”界面的, 在 **SSL Certificates** 标签里点 **Run AutoSSL**)。顶部搜索框直接输入“SSL”也能找到。
- 3 页面列出你所有的域名和证书状态。
- 4 点 **Run AutoSSL**。页面显示“AutoSSL is in progress...”, 完成后自动刷新。

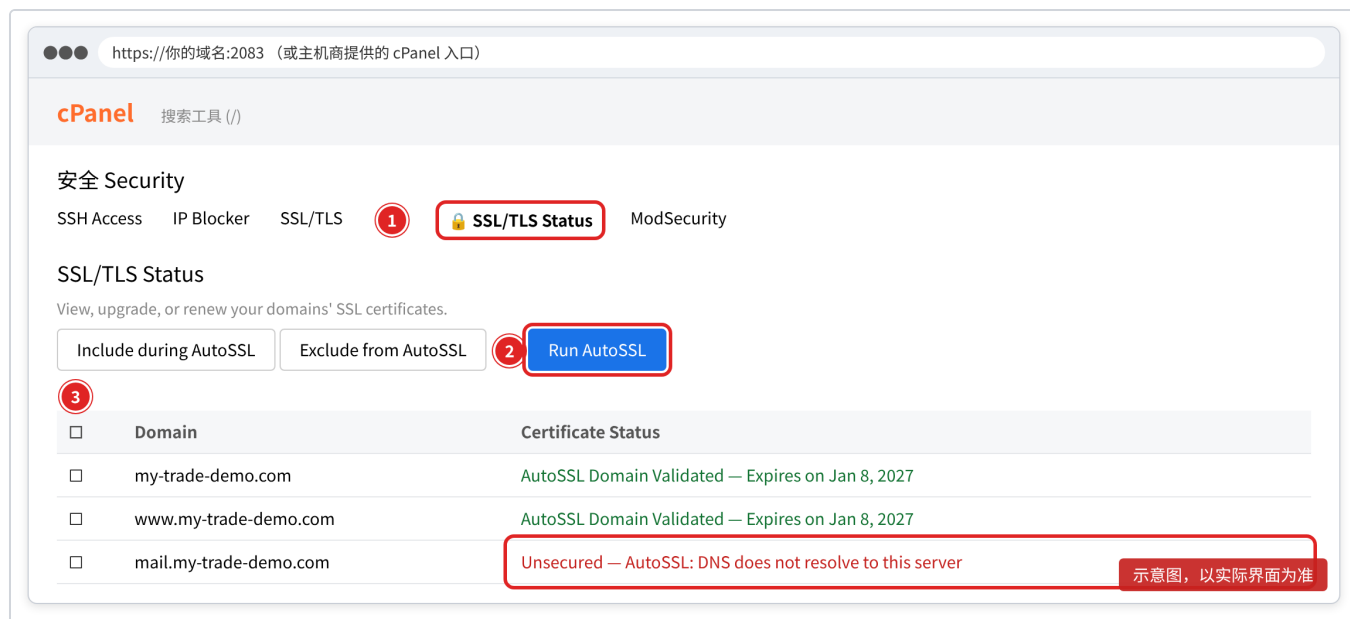


示意图 图 33 cPanel: Security → SSL/TLS Status → Run AutoSSL

- 5 看每个域名的 **Certificate Status**: 显示“AutoSSL Domain Validated”和到期日期即成功。

6.2 看懂失败提示

- 有些子域名 (如 `mail.`、`cpanel.`、`webdisk.`) 没有解析到这台主机, 会显示“DNS does not resolve to this server”之类的错误。如果你不用这些子域名, 可以勾选后点 **Exclude from AutoSSL** (排除), 不影响主站。
- 主域名和 `www` 失败: 检查 DNS 是否指向主机商给你的 IP; 检查域名 CAA 记录 (cPanel 官方文档专门提醒: CAA 记录会限制哪些 CA 能发证书)。
- 找不到 SSL/TLS Status: 说明主机商在后台关闭了这个功能, 直接联系主机商客服, 请他们“为我的账户开启 AutoSSL”。

6.3 开启强制 HTTPS 跳转

- 1 cPanel 首页 → **Domains (域名)** → **Domains**。
- 2 找到你的主域名，把 **Force HTTPS Redirect** 开关打开（cPanel 官方文档：只有已经有有效证书的主域名才能开）。
- 3 如果没有这个开关，联系主机商，或在网站根目录的 `.htaccess` 文件里加跳转规则（WordPress 等程序也可用插件实现）。

说明 AutoSSL 的续期

cPanel 官方文档说明：AutoSSL 证书有效期 90 天，到期前（Let's Encrypt 证书约 29 天内）会自动尝试续期，通常在每晚的系统维护时运行。你不需要手动续期，但仍建议设置第 10.4 节的外部监控。

第7章

路线 D: Cloudflare（没有服务器权限也能做）

适合：① 你只能管理域名、没有服务器权限；② 你想同时获得免费 CDN 加速和防护；③ 域名已经在 Cloudflare。用**时：**30 分钟操作 + 等待 NS 生效（几分钟到 24 小时）。

Cloudflare 是一家全球 CDN（内容分发网络）公司，免费计划就包含 SSL。接入后，访客先连到 Cloudflare，Cloudflare 再去你的服务器（叫“**源站**”，Origin）取内容。因此有**两段路**：访客 ↔ Cloudflare，Cloudflare ↔ 源站。



真实截图 图 34 Cloudflare 免费计划介绍页（cloudflare.com 中文页）

⚠ 注意 先了解：国内访问

Cloudflare 免费计划的节点都在中国大陆境外。外贸站主要面向海外客户，一般影响不大；如果你同时很看重国内客户的访问速度，先小范围测试。

7.1 第 1 步：把域名接入 Cloudflare

- 1 打开 <https://dash.cloudflare.com/sign-up> 注册账号（用公司邮箱，开启两步验证）。
- 2 登录后，点 **添加域 / Add a domain**（按钮名称随版本变化，也可能叫 Onboard a domain），输入你的根域名（不带 www），继续。
- 3 选择 **Free（免费）** 计划。
- 4 Cloudflare 会自动扫描你现有的 DNS 记录。**逐条核对**：网站的 A 记录 / CNAME（@ 和 www）要在；邮箱相关的 MX、TXT（SPF/DKIM）记录一条都不能少，否则企业邮箱会收不到信。网站记录保持“**已代理**”（橙色云朵图标）。



示意图 图 35 Cloudflare：添加域名 → 选免费计划 → 检查 DNS → 获取两个名称服务器

- 5 Cloudflare 给你两个名称服务器（Nameserver），形如 `xxxx.ns.cloudflare.com`、`yyyy.ns.cloudflare.com`（每个账号不同，以页面显示为准）。先把注册商那边原来的 NS 抄下来备用（回滚时要用）。

7.2 第 2 步：到域名注册商修改 NS

- 1 登录你买域名的地方（阿里云、腾讯云、GoDaddy、Namecheap……）。
- 2 找到域名的 **DNS 服务器 / 修改 DNS / Nameservers** 设置：
 - 阿里云：域名控制台 → 域名列表 → 管理 → DNS 管理 → 修改 DNS；
 - 腾讯云：域名注册 → 我的域名 → 管理 → DNS 服务器 → 修改；
 - GoDaddy / Namecheap：Domain → Nameservers → Custom / Change。
- 3 选择“自定义 DNS”，把原来的两个替换成 Cloudflare 给的两个，保存。



示意图 图 36 注册商后台修改 DNS 服务器（各家菜单名称不同，以实际为准）

- 4
- 回到 Cloudflare，点“检查名称服务器 / Check nameservers”。生效后，Cloudflare 会发邮件通知，域名状态变为 **Active（有效）**。通常几分钟到几小时，最长 24~48 小时。

注意 改 NS 是“搬家”

改 NS 之后，域名的**所有** DNS 解析都由 Cloudflare 负责，原来 DNS 后台的设置不再生效。所以第 1 步第 4 项的核对（特别是邮箱 MX 记录）非常重要。

7.3 第 3 步：选择 SSL/TLS 加密模式

Cloudflare 的几种加密模式（两段路分别加不加密）

Flexible 灵活	浏览器	加密	Cloudflare	不加密	你的服务器	源站无需证书；但后半段明文。源站若再强制跳 HTTPS → 无限重定向
Full 完全	浏览器	加密	Cloudflare	加密（不验证）	你的服务器	源站可用自签名证书；能防窃听但防不了冒充
Full (strict)	浏览器	加密	Cloudflare	加密 + 验证	你的服务器	源站要有有效证书（Let's Encrypt 或 Cloudflare 源证书）——推荐

本指南自绘示意图，依据 Cloudflare 官方文档“Encryption modes”

示意图 图 37 Cloudflare 几种加密模式的区别（依据官方文档 Encryption modes）

模式	访客 ↔ Cloudflare	Cloudflare ↔ 源站	源站需要什么	建议
Off	不加密	不加密	—	不要用
Flexible（灵活）	加密	不加密	什么都不用	仅临时过渡；源站再强制 https 会无限跳转
Full（完全）	加密	加密，但不验证证书	任意证书（自签名也行）	过渡用
Full (strict)（完全/严格）	加密	加密并验证证书	有效证书（Let's Encrypt 或 Cloudflare 源证书）	推荐

- 1
- 在 Cloudflare 后台选择你的域名 → 左侧 **SSL/TLS** → **概述（Overview）**。

- 较新的账号默认是 **Automatic SSL/TLS（自动）**：Cloudflare 会扫描你的源站，自动选择它能支持的最安全模式（官方文档说明它不会自动降级）。如果你想自己指定，选 **Custom SSL/TLS（自定义）**。
- 选 **Full (strict)**——前提是源站已经装好有效证书（下一节）。如果源站暂时还没有证书，可以先选 Full，装好后再改成 Full (strict)。

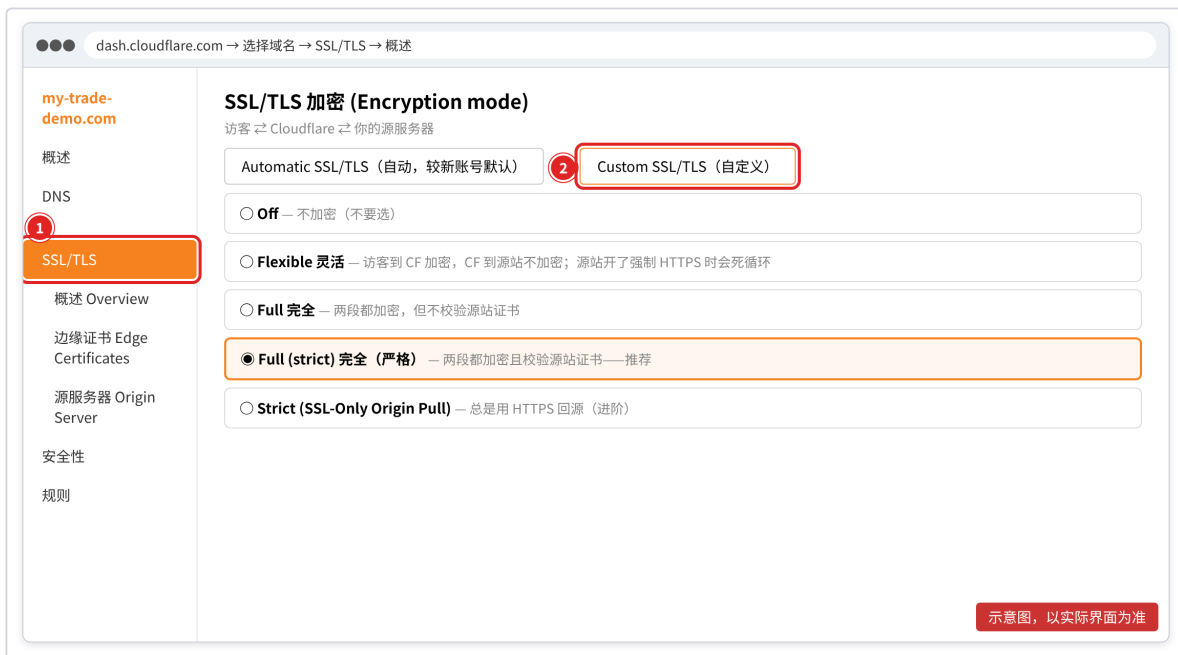
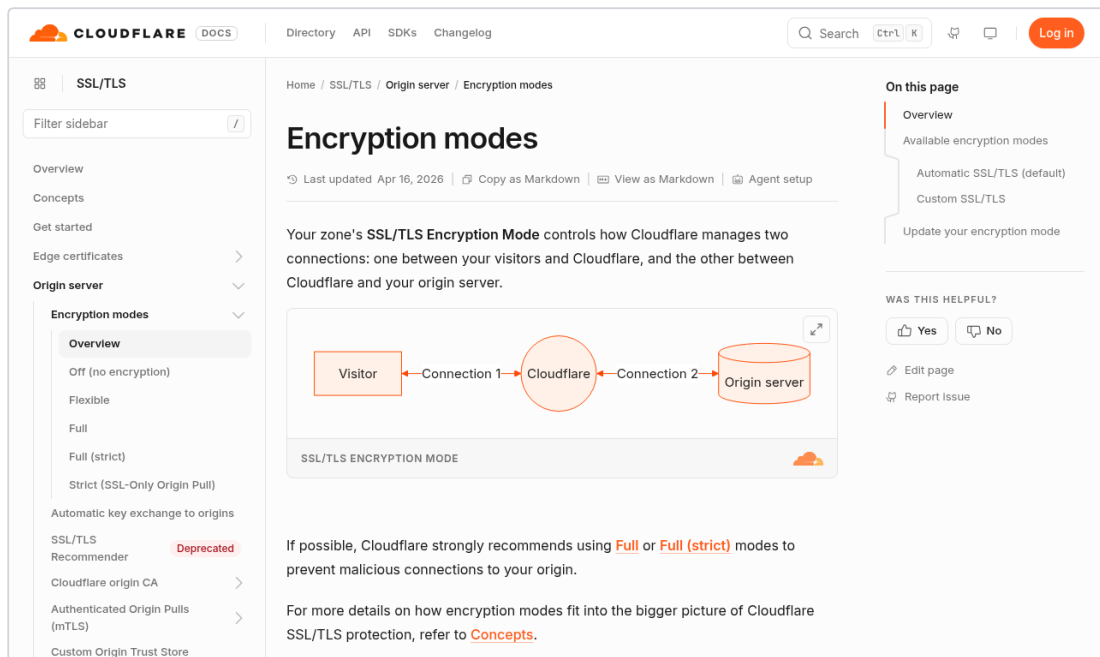


示意图 图 38 Cloudflare: SSL/TLS → 概述 → 选择加密模式



真实截图 图 39 Cloudflare 官方文档“Encryption modes”页面（2026-10-10）

7.4 第 4 步：给源站装证书（二选一）

方式一：源站自己装 Let's Encrypt。 按第 4、5、6 章在服务器 / 宝塔 / cPanel 上装好即可（Cloudflare 代理状态下 HTTP 验证一般也能通过）。优点是：万一以后不用 Cloudflare，网站照样是 https。

方式二：用 Cloudflare 源证书（Origin CA）。 免费、最长 15 年，只给“Cloudflare ↔ 源站”这一段用。

- SSL/TLS → 源服务器（Origin Server）→ 创建证书（Create Certificate）。

- 1 选“使用 Cloudflare 生成私钥和 CSR”，私钥类型 RSA（兼容性最好）或 ECC。
- 2 主机名默认已包含 **你的域名** 和 ***.你的域名**，保持即可。
- 3 有效期选 15 年（或更短）。点 **创建**。
- 4 页面显示两段文本：**源证书**和**私钥**。分别复制，保存为 **origin.pem** 和 **origin.key** 两个文本文件。**私钥离开这个页面后再也看不到。**

dash.cloudflare.com → 选择域名 → SSL/TLS → 源服务器

SSL/TLS › 源服务器 (Origin Server) › 创建证书

1 创建证书 Create Certificate

私钥/CSR

2 ● 使用 Cloudflare 生成私钥和 CSR (私钥类型 RSA / ECC)

主域名

*.my-trade-demo.com my-trade-demo.com

(默认已包含根域名和一级通配符)

有效期

3 15 年 ▼

(可选 7 天 ~ 15 年)

创建

源证书 Origin Certificate (PEM)

-----BEGIN CERTIFICATE-----
MIIE... (复制保存为 origin.pem)
-----END CERTIFICATE-----

私钥 Private Key 离开此页面无法再次查看!

-----BEGIN PRIVATE KEY-----
MIIE... (复制保存为 origin.key)
-----END PRIVATE KEY-----

示意图, 以实际界面为准

示意图 图 40 Cloudflare: SSL/TLS → 源服务器 → 创建证书

- 6 安装到源站：

 - 宝塔：站点设置 → SSL → **当前证书**（或“其他证书”），左边粘贴私钥（KEY），右边粘贴证书（PEM），保存；
 - cPanel：Security → SSL/TLS → Install and Manage SSL for your site，粘贴证书和私钥；
 - Nginx：把两个文件放到 `/etc/ssl/cloudflare/`，配置中写：

```
NGINX
server {
    listen 443 ssl;
    server_name example.com www.example.com;
    ssl_certificate      /etc/ssl/cloudflare/origin.pem;
    ssl_certificate_key  /etc/ssl/cloudflare/origin.key;
    root /var/www/example.com;
}
```

逐行解释：`listen 443 ssl` 监听 https 端口；`server_name` 写你的域名；`ssl_certificate` 指向证书文件；`ssl_certificate_key` 指向私钥文件；`root` 是网站文件目录。改完运行 `sudo nginx -t`，通过后 `sudo systemctl reload nginx`。

⚠ 注意 源证书只能“藏在 Cloudflare 后面”用

浏览器并不信任 Cloudflare 源证书。如果你暂停了 Cloudflare，或把某条 DNS 记录改成“仅 DNS”（灰色云朵），访客会直接看到 `NET::ERR_CERT_AUTHORITY_INVALID` 警告。另外，Cloudflare 官方文档写明：**它不会发送源证书的到期提醒**，请自己记下到期日。

7.5 第 5 步：开启“始终使用 HTTPS”

- 1 SSL/TLS → 边缘证书（Edge Certificates）。
- 2 确认最上方“边缘证书”状态为 **有效（Active）**——这是 Cloudflare 免费发给访客端的证书，自动续期。
- 3 打开 **始终使用 HTTPS（Always Use HTTPS）**：所有 http 访问都 301 跳到 https。
- 4 建议同时打开 **自动 HTTPS 重写（Automatic HTTPS Rewrites）**：能自动修复一部分混合内容。

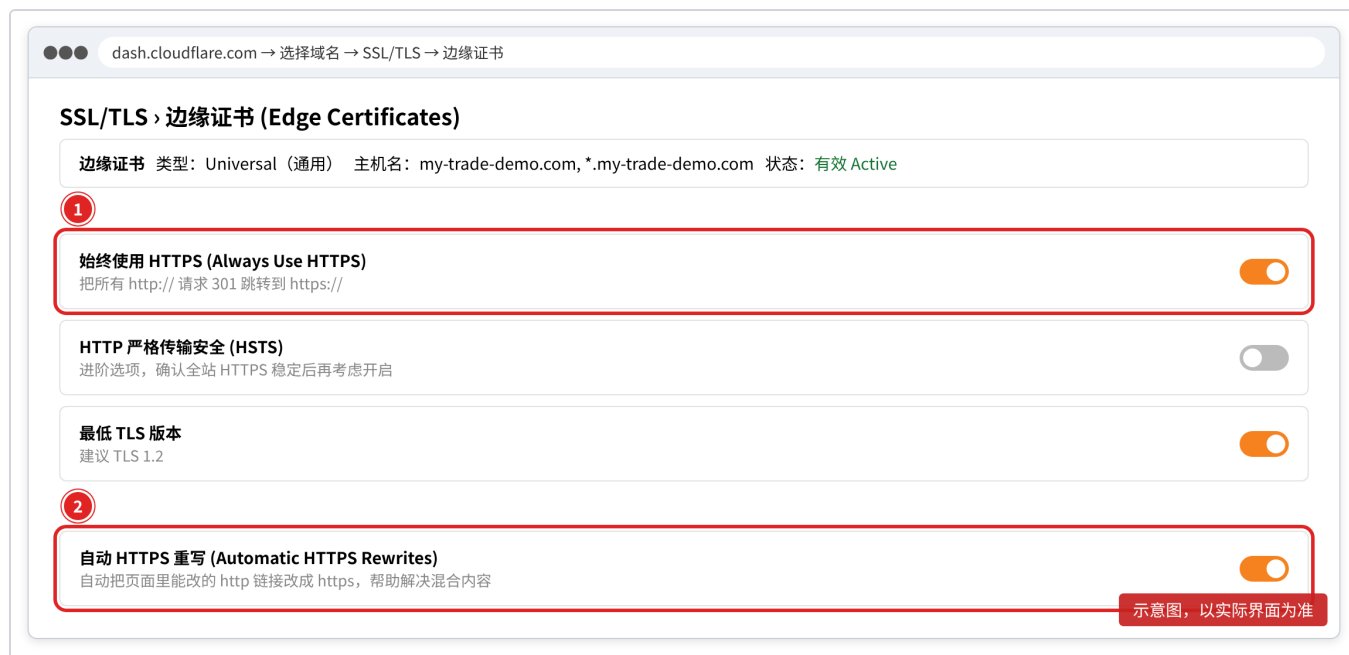


示意图 图 41 Cloudflare: SSL/TLS → 边缘证书 → 始终使用 HTTPS

⚠ 注意 最常见的坑：ERR_TOO_MANY_REDIRECTS

加密模式选了 **Flexible**，而源站（宝塔“强制HTTPS”、Certbot 自动跳转、WordPress 设置）又在把 http 跳到 https：Cloudflare 用 http 回源 → 源站说“去 https” → 访客又来 → Cloudflare 又用 http 回源……无限循环。**解决：把模式改成 Full 或 Full (strict)**。Cloudflare 官方也建议：开了 Always Use HTTPS 就不必在源站再做跳转。

7.6 高级：用 API 自动化（给技术人员或 AI 智能体）

如果让技术人员或 AI 智能体用脚本完成，请创建一个**权限最小**的 API 令牌：Cloudflare 后台右上角头像 → **我的个人资料（My Profile）** → **API 令牌（API Tokens）** → **创建令牌** → 自定义令牌，权限只给：

- Zone → **SSL and Certificates** → Edit（创建源证书）
- Zone → **Zone Settings** → Edit（修改加密模式、始终使用 HTTPS）
- Zone → **DNS** → Read（检查解析记录）

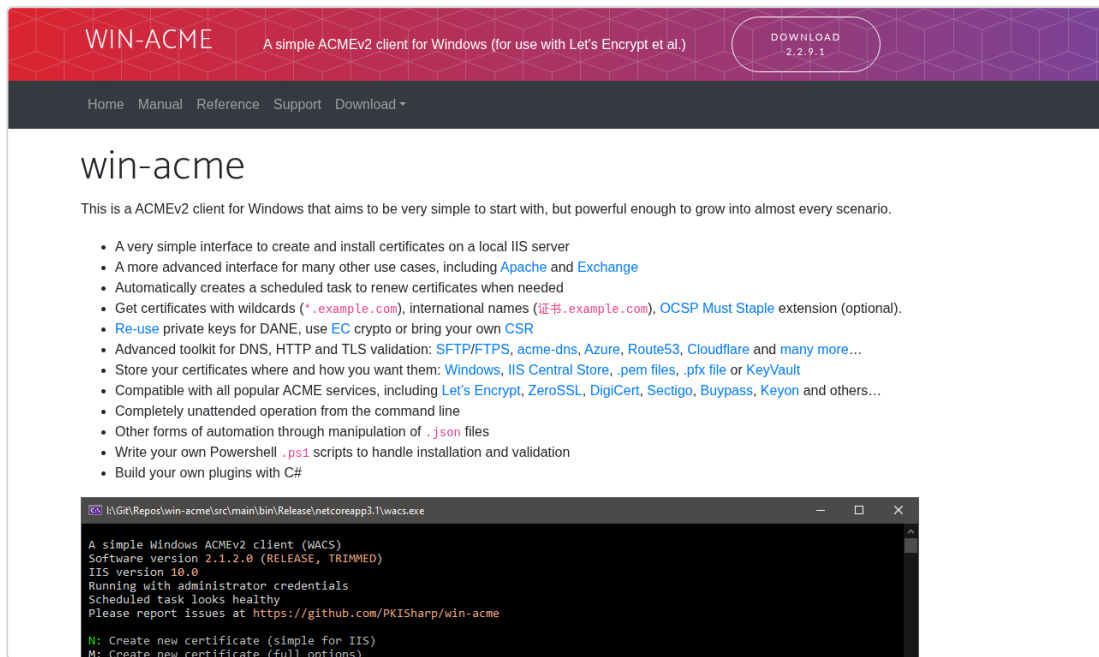
区域资源选“包括 → 特定区域 → 你的域名”，并设置令牌有效期。具体的 API 调用（已对照 Cloudflare 官方 API 文档）见本指南配套的 [SKILL.md](#)，第 11 章也有说明。用完记得在同一页面**撤销令牌**。

第8章

路线 F: Windows 服务器 + IIS (win-acme)

适合: Windows Server，网站用 IIS 搭建，你能用“远程桌面”以管理员身份登录。**用时:** 15 分钟。

win-acme 是 Windows 上最常用的免费 ACME 工具（开源），能自动申请 Let's Encrypt 证书、自动绑定到 IIS、自动创建“计划任务”续期。官网：<https://www.win-acme.com>。



真实截图 图 42 win-acme 官网首页 (win-acme.com)

8.1 准备

- 1 IIS 里网站已经能用 <http://你的域名> 打开，且绑定 (Bindings) 里写了主机名 (根域名和 www 各一条)。
- 2 Windows 防火墙和云安全组放行 80、443。

8.2 下载与运行

- 1 在服务器上用浏览器打开 win-acme 官网，点 Download，下载文件名形如 `win-acme.v2.x.x.xxxx.x64.trimmed.zip` 的版本（官方推荐大多数用户使用的 x64 trimmed 版）。
- 2 解压到一个固定不动的文件夹，官方建议 `C:\Program Files\win-acme`（不要放在桌面或下载文件夹，否则以后续期任务可能找不到程序）。
- 3 右键 `wacs.exe` → 以管理员身份运行。

8.3 按菜单操作

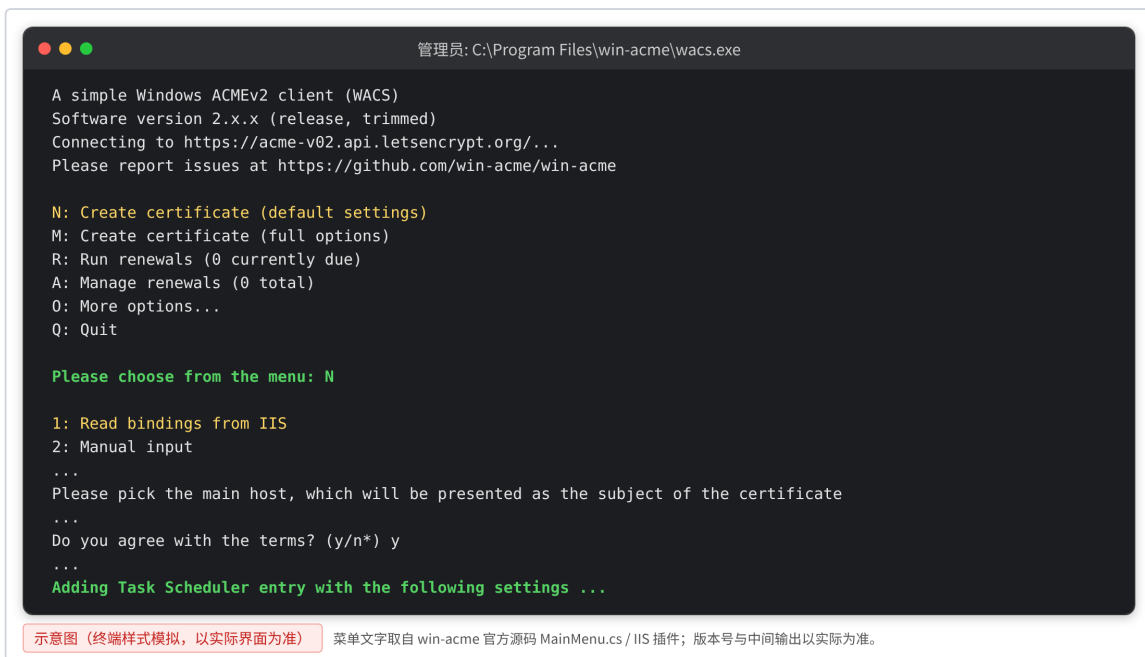


示意图 图 43 win-acme 主菜单与创建流程 (菜单文字取自官方源码, 终端样式模拟)

- 1 主菜单出现后, 输入 **N** (Create certificate (default settings)), 用默认设置创建证书), 回车。
- 2 选择 **Read bindings from IIS** (从 IIS 读取绑定), 然后按提示选择你的网站、选择要包含的域名 (一般全选), 选择主域名。
- 3 第一次使用会让你输入邮箱、同意 Let's Encrypt 服务条款 (输入 **y**)。
- 4 win-acme 自动完成 HTTP 验证 → 下载证书 → 存入 Windows 证书存储 → **自动添加/更新 IIS 的 https 绑定**。
- 5 最后它会创建一个 Windows **计划任务 (Task Scheduler)**, 每天检查并在需要时自动续期。

8.4 验证

- 1 浏览器访问 `https://你的域名`, 按第 2.1 节检查证书。
- 2 再次运行 `wacs.exe`, 选 **A: Manage renewals**, 能看到刚才的续期计划。
- 3 打开“任务计划程序”, 确认有 win-acme 的任务。
- 4 HTTP → HTTPS 跳转: IIS 需要安装“URL 重写 (URL Rewrite)”模块后添加跳转规则, 或交给网站程序处理; 如果用了 Cloudflare, 直接开 Always Use HTTPS。

i 说明 未在实机验证的部分

本章菜单文字依据 win-acme 官方文档与源码核对; 由于本指南的实验环境是 Linux, 未在 Windows Server 上实际运行截图, 界面中的版本号和中间输出以实际为准。

第9章

路线 E：SaaS 建站平台（Shopify / Wix / WordPress.com 等）

好消息：大多数 SaaS 建站平台**自动、免费**提供 SSL 证书，你不需要也不应该另外购买。

平台	官方说法（2026-10 核对）	去哪里看
Shopify	自动为 myshopify.com、在 Shopify 购买的域名以及连接的第三方域名签发免费证书；第三方域名可能需要最多 48 小时	后台 → 设置（Settings）→ 域名（Domains）
Wix	网站和连接的自定义域名默认启用 HTTPS 和免费证书	域名连接后自动生效
WordPress.com	所有托管的域名和子域名自动提供免费 SSL，并自动跳转 https	无需设置
国内外贸 SaaS（Shopline、店匠等）	一般也自动提供，但本指南 未逐一核实	查看平台帮助中心或问客服

9.1 证书一直“待处理 / Pending”怎么办

- 1 按平台的“连接域名”说明，**一字不差**地核对 DNS 记录（通常是一条 A 记录 + 一条 www 的 CNAME）。
- 2 删除指向**旧网站**的 A 记录和 AAAA 记录（一个域名同时指向两个地方，平台验证不了）。
- 3 如果设置过 CAA 记录，确认它允许平台使用的证书机构。
- 4 等待 24~48 小时。仍不行就联系平台客服，并附上第 2 章的自查结果截图。

⚠ 注意 SaaS 平台上没有“装证书”的服务

如果网站在 Shopify/Wix 这类平台上，有人说要收费“帮你安装 SSL”，基本可以判定是不必要的收费——证书由平台负责，第三方也接触不到平台的服务器。

第10章

装好之后：这 6 件事一定要做

10.1 强制 HTTP 跳转到 HTTPS

目的：不管访客输入 `http://` 还是点了旧链接，都自动到 `https`，并告诉搜索引擎“网站搬到 `https` 了”（用 **301 永久跳转**）。

路线	怎么开
A Certbot	<code>--nginx</code> / <code>--apache</code> 默认已自动添加；手动配置时 Nginx 可写 <code>return 301 https://\$host\$request_uri;</code>
B 宝塔	站点设置 → SSL → 强制HTTPS
C cPanel	Domains → Domains → Force HTTPS Redirect
D Cloudflare	SSL/TLS → 边缘证书 → 始终使用 HTTPS（源站不要再重复跳转）
E SaaS	平台自动处理
F IIS	URL Rewrite 规则，或交给程序 / Cloudflare

Nginx 手动写法（只在你没有用 Certbot 自动配置时才需要）：

```
NGINX
server {
    listen 80;
    server_name example.com www.example.com;
    return 301 https://$host$request_uri;
}
```

逐行解释：监听 80 端口（`http`）；匹配你的域名；把请求以 301 永久跳转到同一地址的 `https` 版本（`$host` 是访客访问的域名，`$request_uri` 是后面的路径和参数）。

 **小贴士 进阶：HSTS 先别急着开**

HSTS（HTTP 严格传输安全）会让浏览器在一段时间内“只认 `https`”。它很安全，但一旦证书出问题，访客连“继续访问”按钮都没有。建议全站 `https` 稳定运行几周后再考虑开启，并从较短的有效期开始。

10.2 修复“混合内容”

混合内容：页面本身是 `https`，但里面的图片、脚本、样式、视频还是用 `http://` 地址加载。浏览器会拦截或自动升级这些资源，严重时显示“不安全”、页面排版错乱、询盘表单失效。

怎么找：

- 1 Chrome 打开网页，按 `F12`（Mac：`Option + Command + I`）打开开发者工具，点 **Console（控制台）**。
- 2 看是否有 **Mixed Content** 字样的黄色/红色提示，它会写出是哪个 `http://` 地址。
- 3 也可以在网页上右键 → 查看网页源代码，`Ctrl + F` 搜索 `http://`。

怎么修：

- 把网站后台设置里的“网站地址”改成 https。WordPress：设置 → 常规 → “WordPress 地址”和“站点地址”都改为 `https://`。
- 把文章、产品详情里写死的 `http://你的域名/...` 图片地址批量替换为 `https://`（WordPress 可用数据库搜索替换类插件，操作前先备份数据库）。
- 第三方资源（在线客服、地图、统计代码）换成它们的 https 版本。
- 用 Cloudflare 的，打开“自动 HTTPS 重写（Automatic HTTPS Rewrites）”。

10.3 确认自动续期真的有效

路线	检查方法	正常的样子
A Certbot	<code>sudo certbot renew --dry-run</code>	<code>Congratulations, all simulated renewals succeeded</code>
A Certbot	<code>systemctl list-timers grep -i certbot</code>	能看到 <code>certbot.timer</code> 或 <code>snap.certbot.renew.timer</code> 及下次运行时间
B 宝塔	站点设置 → SSL	显示自动续签已开启、剩余天数正常
C cPanel	SSL/TLS Status	状态为 AutoSSL Domain Validated，到期前会自动更新
D Cloudflare	SSL/TLS → 边缘证书	边缘证书状态 Active（Cloudflare 自动续）；源证书记下到期日
F win-acme	<code>wacs.exe</code> → A: Manage renewals；任务计划程序	有续期计划和计划任务

 **小贴士** 续期后网页软件要重新加载

Certbot 的 `--nginx` / `--apache` 插件续期后会自动重新加载网页软件。如果你用的是 `certonly --webroot` 方式，需要在续期后重载，可以在 `/etc/letsencrypt/renewal-hooks/deploy/` 目录放一个脚本，内容为 `systemctl reload nginx`，并用 `chmod +x` 让它可执行。

10.4 设置证书到期监控（强烈建议）

Let's Encrypt 已停止发送到期提醒邮件（2025-06-04 起），所以要自己设一个“闹钟”：

- 1 **Red Sift Certificates Lite**（原 Hardenize）：Let's Encrypt 官方推荐的替代方案，免费监控最多 250 张证书，到期前发邮件提醒。需要你自己用公司邮箱注册。
- 2 **网站可用性监控服务**：不少服务的免费套餐也带“SSL 证书到期提醒”，但功能和免费额度经常调整，以各家官网当前说明为准（本指南未逐一核实）。
- 3 **最简单的土办法**：在手机日历里，按证书到期日提前 20 天设一个提醒，提醒内容写“检查网站证书是否已自动续期”。

10.5 更新 Google Search Console 和站点地图

- 1 打开 `https://search.google.com/search-console`，登录管理网站的 Google 账号。

- 2 推荐添加“**网域 (Domain)**”类型资源（输入不带 https 的域名，用 DNS TXT 记录验证）——它同时覆盖 http/https 和所有子域名。若之前只添加过 `http://` 的“网址前缀”资源，请再添加一个 `https://` 开头的网址前缀资源。
- 3 在 **站点地图 (Sitemaps)** 里提交 https 版本的 sitemap 地址，例如 `https://www.你的域名/sitemap.xml`。
- 4 确认网站程序生成的 sitemap、canonical（规范网址）标签、内链都已经是 https。
- 5 只换协议（http → https）、不换域名时，做好 301 跳转即可，不需要使用“更改地址”工具（该工具用于更换域名）。



示意图 图 44 Google Search Console：添加网域资源并提交 https 站点地图

10.6 最后跑一次 SSL Labs

按第 2.2 节检测，目标 **A 或 A+**。常见扣分项与处理：

- “Chain issues / Incomplete”（证书链不完整）：Nginx 要用 `fullchain.pem` 而不是 `cert.pem`；宝塔/cPanel 粘贴证书时要包含中间证书。
- 支持旧协议 TLS 1.0/1.1：在 Nginx 配置里只保留 `ssl_protocols TLSv1.2 TLSv1.3`；（Certbot 自带的 `options-ssl-nginx.conf` 已是合理设置）。
- 评级 T：证书不受信任——多半是用了自签名证书或在源站直接暴露了 Cloudflare 源证书。

第11章

让你的智能体帮你部署

现在很多人会用 AI 智能体（能对话、有的还能直接在电脑或服务器上运行命令的 AI 助手）。本指南的网页版提供“**一键复制给智能体**”按钮：点一下，就把整套部署流程和安全规则复制下来，粘贴给你的智能体，它会一步步问你、带你做，甚至在你授权后直接执行命令。

**让你的 AI 智能体帮你部署**

点下面的按钮，把本文的“部署流程 + 安全规则”一次性复制，粘贴给你常用的 AI 智能体即可。记得把 <你的域名> 换成自己的域名。**不要把密码、密钥发给智能体。**

**一键复制给智能体****下载 SKILL.md****Markdown 版**提示词语言： ☒ 中文 ☐ English[▶ 查看将要复制的提示词](#)

复制的内容只是文字说明，不包含任何账号信息；智能体每次改动前都会先征求你的同意。

真实截图

图 45 网页上的“一键复制给智能体”组件（在 Chrome 中实际渲染测试）

11.1 怎么用（5 步）

- 1 在文章顶点 **一键复制给智能体**。屏幕下方出现“已复制”提示。想先看看复制了什么，点“查看将要复制的提示词”。
- 2 打开你常用的 AI 智能体，新建一个对话，按 **Ctrl + V**（Mac：**Command + V**）粘贴。
- 3 把提示词里的 **<你的域名>** 改成你的域名，发送。
- 4 智能体会先**问你问题**（网站放在哪里、账号在谁手里……），按它的问题如实回答；不知道的就说“不知道”，它会教你怎么查。
- 5 每当它要**改动东西**（装软件、改配置、改 DNS、改 Cloudflare 设置）时，它会先告诉你你要做什么、怎么撤销，你确认“继续”后再做。最后它会给你一张总结表：证书到期日、自动续期方式、回滚方法、你还需要做的事。

**小贴士 能运行命令的智能体更省事**

如果你的智能体能连到服务器终端（例如带终端的编程助手），它可以直接帮你执行检查和部署命令；普通聊天型 AI 则会告诉你“复制哪条命令、粘贴到哪里、应该看到什么”，你照做并把输出（去掉敏感信息）发回给它。技术人员还可以下载 **SKILL.md**（一个可安装的“技能文件”），让支持 Agent Skill 的智能体按标准流程工作。



真实截图 图 46 点击按钮后页面底部出现“已复制”提示（无头 Chrome 测试截图）

11.2 安全须知（一定要看）

⚠ 注意 这 6 条，智能体和你都要遵守

1. **密码、私钥、API 令牌不要发到对话里。** 需要输入时，自己在服务器终端或面板输入框里输入。万一发了，事后立刻去修改密码 / 撤销令牌。
2. **任何改动都要先确认。** 智能体说“我要执行……”时，看清楚再回复“继续”。看不懂就问“这一步会改什么？出错了怎么恢复？”
3. **先备份再改。** 确认它备份了配置（或你自己在面板里截图保存原设置）。
4. **Cloudflare API 令牌要“最小权限、单一域名、有过期时间”，用完撤销。**
5. **不要因为智能体（或任何人）的建议去购买“金融级证书”。** 免费证书完全够用（第 13 章）。
6. **让它在结束时告诉你回滚方法，并自己保存一份总结。**

11.3 给网站管理员：这个按钮怎么做

本指南附带了一个完整的“智能体就绪”内容包（文件夹 `agent/`）：

文件	作用
<code>ssl-deploy-skill/SKILL.md</code>	可安装的 Agent Skill：访谈 → 预检 → 各路线部署 → Cloudflare API 自动化 → 验证 → 续期 → 回滚，以及安全规则
<code>agent-prompt.md</code> (及 <code>.zh.txt</code> / <code>.en.txt</code>)	中英文自包含提示词，就是按钮复制的内容
<code>agent-copy-button.html</code>	网页组件：纯原生 JS/CSS，无第三方依赖；支持 navigator.clipboard 和 textarea 兜底、“已复制”提示、展开查看、下载 SKILL.md
<code>site/llms.txt</code> 、 <code>site/howto.jsonld</code>	机器可读入口：llms.txt 条目、schema.org HowTo 结构化数据

文件	作用
README.md	以后每篇文章照做的模板：一个 Markdown 双胞胎页面 + 一段智能体提示词 + 一个按钮

组件已在无头 Chrome 154 中测试：复制到剪贴板的文字与提示词文件逐字一致（中英文均测试），非 HTTPS 页面下自动走兼容方式复制成功，“已复制”提示正常出现。

第12章

故障排查表

#	症状	原因	解决办法
1	Certbot / 宝塔提示验证失败，含 <code>Timeout</code> / <code>connection</code>	80 端口被云安全组或系统防火墙挡住	第 3.2 节两道门都放行 80；用手机流量访问 <code>http://域名</code> 测试
2	验证失败，含 <code>connection refused</code>	网页软件没运行或没监听 80	<code>sudo systemctl start nginx</code> （或 <code>apache2/httpd</code> ）；宝塔里启动 Nginx
3	验证失败，含 <code>NXDOMAIN</code> / <code>DNS problem</code>	域名没解析或 DNS 尚未生效	第 3.1、3.3 节；用 <code>dns.google</code> 确认后再申请
4	验证失败， <code>unauthorized</code> / <code>404</code> / 返回了别的网站内容	A 或 AAAA 记录指向旧服务器；伪静态/跳转规则拦截了 <code>/.well-known/acme-challenge/</code> ；CDN 缓存	删除旧 AAAA 记录；临时关闭 301/CDN；检查网站根目录是否正确
5	申请提示 <code>CAA record</code> 不允许	CAA 记录未包含 <code>letsencrypt.org</code>	DNS 里添加 <code>0 issue "letsencrypt.org"</code> 的 CAA 记录或删除旧的
6	<code>too many certificates</code> / <code>too many failed authorizations</code>	触发 Let's Encrypt 频率限制	等待（失败限制约 1 小时，重复签发限制 7 天内逐步恢复）；排查时用 <code>--dry-run</code>
7	浏览器 <code>ERR_TOO_MANY_REDIRECTS</code> （重定向次数过多）	Cloudflare 用 Flexible，源站又强制 https；或多处重复跳转	Cloudflare 改 Full / Full (strict)；只保留一处跳转
8	Cloudflare 显示 Error 526 (Invalid SSL certificate)	Full (strict) 模式下源站证书无效/过期/域名不符	源站装有效证书（Let's Encrypt 或源证书），或暂时改为 Full
9	Cloudflare 显示 Error 525 (SSL handshake failed) / 521	源站 443 未开启 SSL / 源站宕机或拦截了 Cloudflare	源站配置 443；放行 Cloudflare IP；检查网页软件状态
10	<code>NET::ERR_CERT_COMMON_NAME_INVALID</code> （名称不符）	证书没包含当前访问的域名（如少了 <code>www</code> ）；访问到了另一个站点的证书	重新申请时把根域名和 <code>www</code> 都加上；宝塔里给每个站点单独部署
11	<code>NET::ERR_CERT_DATE_INVALID</code> （日期无效）	证书已过期；偶尔是访客电脑时间错误	立即续期（Certbot： <code>sudo certbot renew</code> ；宝塔/cPanel：重新申请/Run AutoSSL），再查自动续期为什么失效
12	<code>NET::ERR_CERT_AUTHORITY_INVALID</code>	自签名证书、测试证书；Cloudflare 源证书被直接访问（灰色云朵或暂停了 CF）	换成 Let's Encrypt 证书；DNS 记录恢复橙色云朵
13	地址是 https，但仍提示 “不安全”/部分图片不显示	混合内容	第 10.2 节
14	手机打不开或提示证书不可信，电脑正常	证书链不完整（只装了域名证书，没装中间证书）	Nginx 用 <code>fullchain.pem</code> ；面板粘贴时包含完整证书链；SSL Labs 查 Chain issues

#	症状	原因	解决办法
15	证书到期没自动续	定时任务没运行；续期时 80 端口被关；后来开了 CDN/301；改过网页配置	<code>sudo certbot renew --dry-run</code> 看报错；宝塔查看续签日志；按 1~4 行排查
16	中国大陆服务器，访问显示“网站未备案”提示或验证一直失败	域名未 ICP 备案（或未在当前云厂商接入备案），访问被云厂商阻断	完成备案 / 接入备案；或把网站迁到境外服务器（第 3.4 节）
17	改完 Nginx 配置后网站全挂	配置语法错误	<code>sudo nginx -t</code> 查看错误行；用备份恢复： <code>sudo cp -a /root/nginx-backup-日期/. /etc/nginx/</code> 后 <code>sudo systemctl reload nginx</code>
18	SaaS 平台证书一直 Pending	DNS 记录不对、旧记录冲突、CAA 限制	第 9.1 节

第13章

常见问题（FAQ）

Q1：免费证书和 2500 元的“金融级证书”到底有什么区别？

加密强度没有区别。所有公开受信任的证书用的是同样的 TLS 协议和加密算法；浏览器只认“有效 / 无效”。证书按审核了什么分三类：

DV / OV / EV 三种证书：加密强度一样，区别只在“审核了什么”

类型	审核内容	价格	浏览器地址栏显示	加密强度
DV 域名验证	只证明你控制这个域名	免费（Let's Encrypt 等）~ 几百元	安全图标	相同 (同样的 TLS 协议与算法)
OV 组织验证	+ 核实公司真实存在	通常每年数百至数千元	同 DV，需点开证书详情才能看到公司名	
EV 扩展验证	+ 更严格的企业资料审核	通常每年数千元起	同 DV（2019 年起主流浏览器不再显示绿色公司名地址栏）	

本指南自绘示意图；价格为市场大致区间，仅供参考

示意图 图 47 DV / OV / EV 对比

- DV（域名验证）：只验证你控制这个域名。免费证书都是 DV。
- OV（组织验证）：额外核实公司真实存在，证书里写有公司名，但访客要点开证书详情才看得到。
- EV（扩展验证）：审核更严格。过去浏览器会在地址栏显示绿色公司名，但 **Chrome 等主流浏览器 2019 年起已取消这种显示**，现在 EV 在地址栏的样子和 DV 一样。
- 市面上没有“金融级证书”这个技术标准，它是营销说法。

Q2：那什么时候值得买付费的 OV/EV 证书？

- 客户、合作银行、招标文件或合规审计**明确要求**证书里有公司信息；
- 某些老旧系统、内网设备或特殊客户端需要特定的证书链/根证书兼容（宝塔官方文档也提到 Let's Encrypt 更换根证书后，部分老旧设备可能提示不可信）；
- 你需要证书机构提供的**人工技术支持**或保险赔付条款；
- 无法使用自动化工具、需要较长有效期的场景——但注意行业规则正在把所有证书的有效期缩短（2026 年起最长 200 天，2029 年起 47 天），付费证书也要频繁更换。

对普通外贸展示站、询盘站、独立站来说，免费 DV 证书完全足够。

Q3：什么是通配符证书？我需要吗？

`*.example.com` 可以覆盖 `www.example.com`、`shop.example.com` 等所有一级子域名，但不覆盖 `example.com` 本身，也不覆盖 `a.b.example.com`。Let's Encrypt 免费支持通配符，但必须用 **DNS 验证**（宝塔第 5.4 节；Certbot 需要 DNS 插件；Cloudflare 边缘证书默认已包含 `*, 域名`）。子域名不多时，直接把每个子域名都写进同一张证书更简单。

Q4：一张证书能包含多个域名吗？

可以。Certbot 写多个 `-d`；宝塔勾选多个域名；cPanel AutoSSL 自动包含账户下的域名。Let's Encrypt 一张证书最多可包含 100 个域名。不同的根域名（例如 `brand-a.com` 和 `brand-b.com`）也可以放在一张证书里，但一般建议每个网站各用一张，互不影响。

Q5：证书装好后，网站会变慢吗？

几乎感觉不到。现代 TLS 1.3 的握手很快，而且 https 才能使用 HTTP/2、HTTP/3 等更快的协议。

Q6：换服务器 / 换建站公司，证书怎么办？

在新服务器上重新申请即可（免费、几分钟），不需要“迁移证书”。切换 DNS 前先在新服务器上准备好网站，DNS 生效后立即申请证书。

Q7：我能把证书私钥发给建站公司吗？

尽量不要。私钥等于网站的“公章”。正确做法是让他们在服务器上直接申请，私钥从生成到使用都不离开服务器。

Q8：为什么我的 Chrome 里没有小锁头了？

Chrome 从 117 版起把地址栏的小锁换成了“调节”图标，表示“查看网站信息和权限”，**这不代表不安全**。真正的不安全会明确写出“不安全”字样或出现整页红色警告。

Q9：Let's Encrypt 是什么来头，可靠吗？

由非营利组织 ISRG（互联网安全研究小组）运营，自 2015 年起签发证书，官网称已为超过 7 亿个网站提供免费证书，所有主流浏览器和操作系统都信任它。

第14章

一页速查表（建议打印）

步骤	做什么	关键命令 / 菜单	成功标志
① 选路线	按第 0.3 节 6 道题	NS 含 cloudflare → D；有宝塔 → B；cPanel → C；IIS → F；SaaS → E；其余 → A	知道去哪一章
② 预检	解析、端口、CAA、备案	dns.google 查 A/AAAA/CAA；手机流量打开 <code>http://域名</code>	7 项全部打勾
③ 部署 A	Linux + Certbot	<code>sudo snap install --classic certbot</code> → <code>sudo certbot --nginx -d 域名 -d www.域名</code>	<code>Congratulations! ... enabled HTTPS</code>
③ 部署 B	宝塔	网站 → 站点 → SSL → Let's Encrypt → 申请证书 → 强制 HTTPS	显示剩余约 89 天
③ 部署 C	cPanel	Security → SSL/TLS Status → Run AutoSSL；Domains → Force HTTPS Redirect	AutoSSL Domain Validated
③ 部署 D	Cloudflare	改 NS → SSL/TLS 概述 Full (strict) → 边缘证书 Always Use HTTPS	边缘证书 Active
③ 部署 E	SaaS	连接域名，等待自动签发	后台显示 SSL 已启用
③ 部署 F	IIS	管理员运行 <code>wacs.exe</code> → N → Read bindings from IIS	IIS 出现 https 绑定
④ 跳转	http → https	见第 10.1 节表格	<code>curl -I http://域名</code> 返回 301
⑤ 混合内容	F12 → Console 查 Mixed Content	网站地址改 https；替换 http 链接	控制台无 Mixed Content
⑥ 续期	演练续期	<code>sudo certbot renew --dry-run</code>	<code>all simulated renewals succeeded</code>
⑦ 监控	到期提醒	Red Sift Certificates Lite / 日历提醒	收到确认邮件
⑧ 验收	全面检测	ssllabs.com/ssltest；电脑+手机；带/不带 www	A / A+
⑨ SEO	Search Console	添加网域资源，提交 https sitemap	站点地图状态“成功”

 **注意 三句话记住**

证书是免费的；自动续期必须确认；密码和私钥不给任何人（包括 AI）。

附录

参考资料、图片说明与未核实事项

A. 参考资料（均于 2026-10-10 访问核对）

- 1 Certbot 官方安装说明（Nginx / snap）：<https://certbot.eff.org/instructions?ws=nginx&os=snap>
- 2 Let's Encrypt：证书有效期缩短至 45 天公告（2025-12-02）：<https://letsencrypt.org/2025/12/02/from-90-to-45>
- 3 Let's Encrypt：到期提醒邮件服务已结束（2025-06-26）：<https://letsencrypt.org/2025/06/26/expiration-notification-service-has-ended.html>
- 4 Let's Encrypt 频率限制：<https://letsencrypt.org/docs/rate-limits/>
- 5 Let's Encrypt 验证方式（HTTP-01 / DNS-01）：<https://letsencrypt.org/docs/challenge-types/>
- 6 CA/Browser Forum 决议 SC-081v3（证书有效期时间表）：<https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/>
- 7 Google 安全博客《HTTPS by default》（Chrome 154 默认开启“始终使用安全连接”）：<https://security.googleblog.com/2025/10/https-by-default.html>
- 8 Cloudflare 加密模式：<https://developers.cloudflare.com/ssl/origin-configuration/ssl-modes/>
- 9 Cloudflare Origin CA：<https://developers.cloudflare.com/ssl/origin-configuration/origin-ca/>
- 10 Cloudflare Always Use HTTPS：<https://developers.cloudflare.com/ssl/edge-certificates/additional-options/always-use-https/>
- 11 Cloudflare API：编辑区域设置 <https://developers.cloudflare.com/api/resources/zones/subresources/settings/methods/edit/>；创建 Origin CA 证书 https://developers.cloudflare.com/api/resources/origin_ca_certificates/methods/create/；验证令牌 <https://developers.cloudflare.com/api/resources/user/subresources/tokens/methods/verify/>
- 12 宝塔面板官方文档：网站 SSL 证书部署 <https://docs.bt.cn/user-guide/site/php/site-config/ssl/>；SSL 域名与 DNS 接口管理 <https://docs.bt.cn/user-guide/ssl/domain/>
- 13 cPanel 文档：SSL/TLS Status <https://docs.cpanel.net/cpanel/security/ssl-tls-status/>；Guide to SSL <https://docs.cpanel.net/knowledge-base/security/guide-to-ssl/>；Domains（Force HTTPS Redirect）<https://docs.cpanel.net/cpanel/domains/domains/>
- 14 win-acme 入门：<https://www.win-acme.com/manual/getting-started>；菜单文字来源：GitHub win-acme 源码 MainMenu.cs
- 15 阿里云帮助中心：备案域名注意事项（未备案域名解析至中国内地服务器）：<https://help.aliyun.com/zh/icp-filing/basic-icp-service/support/for-the-record-domain-faq>
- 16 ZeroSSL 价格与 ACME：<https://zerossl.com/pricing>；<https://zerossl.com/documentation/acme>
- 17 Shopify / Wix / WordPress.com 官方帮助中心关于 SSL 的说明
- 18 Pebble（Let's Encrypt 官方测试 CA）：<https://github.com/letsencrypt/pebble>

B. 图片类型一览

- **真实截图**（Chrome 154 实际浏览器或无头浏览器截取）：Let's Encrypt 首页、Certbot 安装向导、宝塔官网、Cloudflare 免费计划页与官方文档页、win-acme 官网、SSL Labs 首页与 letsencrypt.org 检测结果、dns.google 查询结果、Chrome 站点信息弹窗与证书查看器（letsencrypt.org）、wrong.host.badssl.com 警告页、实验环境中的“不安全”页面 / 过期证书页 / 不受信任证书页、“一键复制给智能体”组件。
- **真实命令输出**（实验服务器 Debian 13 上真实运行，用终端样式排版）：certbot --nginx、Nginx 配置、certbot certificates、renew --dry-run、验证失败、nginx -t、301 跳转、certbot 定时器文件；curl / openssl 查看真实网站证书。
- **示意图**（本指南自绘，菜单名称依据官方文档）：路线流程图、HTTP/HTTPS 原理图、Cloudflare 加密模式图、DV/OV/EV 对比、宝塔 4 张、cPanel 1 张、Cloudflare 4 张、注册商改 NS、云安全组、Google Search Console、win-acme 菜单、systemctl 定时器输出。

C. 未能实机核实 / 需以实际为准的内容

- 宝塔、cPanel、Cloudflare 后台、云厂商控制台、Google Search Console：无法登录真实后台，界面为依据官方文档绘制的示意图；不同版本按钮位置、颜色、中文译名可能不同。
- Cloudflare 后台中文菜单译名（如“边缘证书”“源服务器”）按常见译法书写，英文名称以官方文档为准。
- win-acme 未在 Windows Server 上实际运行；菜单文字取自官方源码。
- systemd 定时器的输出为模拟（实验容器无 systemd）；定时器文件内容为真实文件。
- 国内外贸 SaaS 平台（Shopline、店匠等）的 SSL 细节未逐一核实。
- 各网站监控服务的免费额度和功能会变化，未逐一核实。
- 付费 OV/EV 证书价格为市场大致区间，仅供参考。
- 备案相关规定以工信部和各云厂商最新要求为准。