?? SSL ??????

你要的其实就是 免费 **SSL** 域名证书 ，能直接配到 **Nginx** 上，并且可以 下载到本地（而不是像一些托管服务只给 HTTPS 反代）。
我帮你分成两种方式: 自动申请 （推荐）和 手动申请 （方便离线保存）。

???????Let’s Encrypt + Certbot ??????????

Let’s Encrypt 提供免费 DV 证书，有效期 **90** 天，支持自动续期。

1. ?? Certbot

Ubuntu / Debian:

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

2. ????

假设你的域名是 **example.com**，且已经解析到服务器 IP:

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

Certbot 会自动:

- 验证域名
- 生成 `/etc/letsencrypt/live/example.com/fullchain.pem` 和 `privkey.pem`
- 修改 Nginx 配置加载证书

3. Nginx ????

```
server {
    listen 443 ssl;
    server_name example.com www.example.com;
```

```
    ssl_certificate /etc/letsencrypt/live/example.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/example.com/privkey.pem;

    location / {
        root /var/www/html;
        index index.html;
    }
}
```

4. ????

```
sudo systemctl enable certbot.timer
sudo systemctl start certbot.timer
```

????????????? Nginx ?????

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ **acme.sh**□

1. ?? acme.sh

```
curl https://get.acme.sh | sh
source ~/.bashrc
```

2. ?? DNS ??????????? 80/443 ????

□□□□□□□□□□ API Key□□

```
export Ali_Key="□□□□□AccessKeyId"
export Ali_Secret="□□□□□AccessKeySecret"

acme.sh --issue --dns dns_ali -d example.com -d www.example.com
```

3. ??? Nginx ???????

```
acme.sh --install-cert -d example.com \
--key-file /root/cert/example.com.key \
--fullchain-file /root/cert/example.com.crt \
--reloadcmd "nginx -s reload"
```

生成后 `/root/cert/example.com.key` 和 `/root/cert/example.com.crt` 就可以打包下载了。

??????

- 免费证书一般 **90** 天有效 ，需要续期（ acme.sh 可自动续期）。
- 如果是公司内部测试，可以用自签证书（但浏览器会提示不安全）。
- 申请时 域名必须已解析到你的服务器 ，否则验证失败。

???????80?443 ??????????????????????????SSL ?????

**1. 使用 DNS验证方式申请证书 **
DNS验证方式不需要开放 80或 443端口，而是通过添加 DNS TXT记录来验证域名所有权。

**方法一：使用 acme.sh（推荐） **
1. **安装 acme.sh**
   ```bash
   curl https://get.acme.sh | sh
   ```
2. **申请证书（以阿里云 DNS为例） **
   ```bash
   export Ali_Key="你的 AccessKey"
   export Ali_Secret="你的 AccessSecret"
   acme.sh --issue --dns dns_ali -d example.com -d *.example.com
   ```
3. **证书存储位置 **
   证书默认存放在 `~/.acme.sh/example.com/` 目录下，包含 `fullchain.cer` 和 `example.com.key` 文件。

方法二：使用CertBot
1. **安装CertBot**
   ```bash
   sudo apt install certbot
   ```
2. **手动DNS验证**
   ```bash
   certbot certonly --manual --preferred-challenge dns -d example.com
   ```
   按照提示添加TXT记录`_acme-challenge.example.com`，等待解析生效后继续。

---

2. 使用邮箱验证（适用于ZeroSSL）
如果无法使用DNS验证，可以尝试通过邮箱验证：
1. **在ZeroSSL申请证书**
   - 访问[ZeroSSL](https://zerossl.com/)并选择邮箱验证。
2. **在服务器上搭建Postfix邮件服务**
   - 接收验证邮件（如`admin@example.com`）以完成验证。

---

3. 使用JoySSL等支持非标准端口的CA
某些CA（如JoySSL）支持通过22端口（SSH）进行验证：
1. **访问JoySSL官网**
   - 选择IP或域名证书类型。
2. **通过SSH验证服务器所有权**
   - 提供服务器访问权限，CA通过22端口完成验证。

---

4. 使用acme-redirect（Rust工具）
1. **安装acme-redirect**
   ```bash
   git clone https://github.com/kpcyrd/acme-redirect.git
   cd acme-redirect && cargo build --release
   ```
2. **配置并运行**
   - 修改`/etc/acme-redirect.d/example.com.conf`，启动服务：
   ```bash
   systemctl enable --now acme-redirect
   ```
   - 证书存放在`/var/lib/acme-redirect/live/example.com/`。

---

5. 自动续期
- **acme.sh**: 默认自动续期，无需额外操作。
- **CertBot**: 需手动设置 cron任务:
  ```bash
  30 0 * * 1 certbot renew --manual-auth-hook /path/to/dns-update-script.sh
  ```

总结
方法	适用场景	工具	验证方式
DNS验证	有 DNS管理权限	acme.sh / CertBot	添加 TXT记录
邮箱验证	无 80/443端口	ZeroSSL	邮件接收验证
SSH验证	服务器可 SSH访问	JoySSL	22端口验证
acme-redirect	需临时占用 80端口	acme-redirect	HTTP验证

选择最适合你的方式，确保域名解析正确后即可获取证书。

???? DNS ????????? **NXDOMAIN**????? Let's Encrypt ???? `_acme-challenge.bost.lesrec.cn` ? TXT ???

解决方法
1. 检查 DNS 记录是否已正确添加
- 进入你的 DNS 管理控制台（如阿里云、腾讯云、Cloudflare 等）。
- 添加一条 **TXT 记录**:
  - **主机名**: `_acme-challenge.bost`（或 `_acme-challenge`，取决于你的 DNS 提供商）
  - **记录值**: `a0La5vEuhIg0Omqo7U-vS00_mUG40kjXgOZCKq0y7dw`（CertBot 提供的值）
  - **TTL**: 默认即可（如 600 秒）。

2. 等待 DNS 生效
DNS 记录可能需要 **几分钟到几小时** 才能全球生效。你可以使用以下命令检查是否生效:
```bash
dig TXT _acme-challenge.bost.lesrec.cn +short
```
或:
```bash
nslookup -type=TXT _acme-challenge.bost.lesrec.cn
```

如果返回正确的 TXT 值，说明 DNS 已生效。

3. 重新运行 CertBot
```bash
certbot certonly --manual --preferred-challenge dns -d bost.lesrec.cn
```
再次输入 `Y` 并等待验证。

常见问题排查
1. **DNS 记录格式错误**
   - 确保主机名是 `_acme-challenge.bost`（而不是 `_acme-challenge.bost.lesrec.cn`）。
   - 某些 DNS 提供商（如 Cloudflare）会自动补全域名，你可能只需要输入 `_acme-challenge`。

2. **DNS 缓存问题**
   - 使用 `dig @8.8.8.8 TXT _acme-challenge.bost.lesrec.cn` 检查 Google DNS 是否已更新。
   - 如果本地 DNS 缓存未更新，可以尝试 `systemd-resolve --flush-caches`（Linux）。

3. **CertBot 超时**
   - Let's Encrypt 默认等待 **30 秒**，如果 DNS 传播较慢，可以手动验证后再继续：
   ```bash
   certbot certonly --manual --preferred-challenge dns -d bost.lesrec.cn --manual-auth-hook /path/to/dns-update-script.sh --manual-cleanup-hook /path/to/dns-cleanup-script.sh
   ```

4. **使用 acme.sh 自动 DNS 验证（推荐）**
   - 如果你的 DNS 提供商支持 API（如阿里云、Cloudflare），可以使用 `acme.sh` 自动完成验证：
   ```bash
   export Ali_Key="你的 AccessKey"
   export Ali_Secret="你的 AccessSecret"
   acme.sh --issue --dns dns_ali -d bost.lesrec.cn
   ```

成功后的证书位置
- CertBot 默认存放路径：
  - **证书**：`/etc/letsencrypt/live/bost.lesrec.cn/fullchain.pem`
  - **私钥**：`/etc/letsencrypt/live/bost.lesrec.cn/privkey.pem`

如果仍然失败，请提供 `dig TXT _acme-challenge.bost.lesrec.cn` 的输出，我可以帮你进一步排查！

??????SSL???????

如果你的服务器 **80/443** 端口都不开放，就不能用 Let’s Encrypt 的 HTTP 验证方式，只能用 **DNS** 验证来手动申请 SSL 证书，这样证书签发过程完全不依赖服务器的 Web 端口。

我给你分几种 手动申请免费 **SSL** 的方法（都可以直接下载证书， Nginx 格式 `.crt` + `.key`）：

---

1. ZeroSSL??? DNS ???

- 地址： https://zerossl.com
- 优点：
  - 免费 90 天 DV 证书
  - 可直接生成 `.crt` 和 `.key` 文件
  - 支持手动 DNS 验证
- 步骤：
  1. 注册 ZeroSSL 账号。
  2. 新建证书 → 输入域名 → 选择 **DNS (CNAME)** 验证。
  3. 按提示在域名解析中添加 TXT 或 CNAME 记录。
  4. 验证完成后下载证书（可选 Nginx 格式）。
  5. 上传到服务器 `/etc/nginx/ssl`，配置 Nginx：

```
ssl_certificate /etc/nginx/ssl/example.com.crt;
ssl_certificate_key /etc/nginx/ssl/example.com.key;
```

---

2. Buypass Go SSL??? 180 ????

- 地址： https://www.buypass.com/ssl/resources/go-ssl
- 优点：
  - 免费半年有效期
  - 支持 ACME 协议，可离线生成
  - DNS 验证支持
- 步骤：
  1. 使用 acme.sh 或 Certbot，设置验证方式为 `--dns`。
  2. 生成证书并保存 `.crt`、`.key`。

---

3. Let’s Encrypt + acme.sh?DNS ????????

如果你不想依赖网页操作，可以用 acme.sh，本地生成后把证书上传到服务器。

?? acme.sh

```
curl https://get.acme.sh | sh
source ~/.bashrc
```

????????? DNS ???

```
export Ali_Key="你的阿里云AccessKeyId"
export Ali_Secret="你的阿里云AccessKeySecret"

acme.sh --issue --dns dns_ali -d example.com -d www.example.com
```

??? Nginx ?????????

```
acme.sh --install-cert -d example.com \
--key-file ./example.com.key \
--fullchain-file ./example.com.crt
```

生成的 `.crt` 和 `.key` 就可以直接配到 Nginx。

---

4. SSL.com??? 90 ??????

- 地址：https://www.ssl.com/certificates/free
- 手动上传 CSR，选择 DNS 验证，审核后下载证书。

□ □□

- 你这种 不开 **80/443** 的情况，最佳方案是 **acme.sh + DNS** 验证 或 **ZeroSSL** 手动签发 。
- DNS 验证是通过添加 TXT/CNAME 记录证明域名所有权，不依赖服务器端口，非常适合内网或防火墙环境。

如果你需要，我可以帮你做一个本地一键脚本，用 `acme.sh` 自动生成 **Nginx** 格式证书，全程只需要你填一次域名和 DNS API Key，90 天后也能自动续期，不用手动去 ZeroSSL。这样你连网页都不用开，全程命令行离线可操作。

你要我帮你写这个脚本吗？这样申请下来直接就是 `.crt` + `.key`。

Revision #6
Created 13 August 2025 00:45:13 by Admin
Updated 13 August 2025 02:00:13 by Admin