?? Certbot ???? HTTPS ??

????? Certbot ? Let’s Encrypt?

Let’s Encrypt 是一个由非营利组织 ISRG 提供的免费证书颁发机构， Certbot 则是其官方推荐的自动化工具。它们的核心优势包括：

- 免费：无需支付证书费用。
- 自动化 ： Certbot 提供自动获取和续期证书的功能。
- 开源：社区支持广泛，兼容多种服务器环境。
- 快速：几分钟即可完成配置。

无论你是运行一个个人博客还是小型商业网站， Certbot 都能帮你快速实现 HTTPS。

????

在开始之前，请确保你已准备好以下内容：

1. 一个域名 ：已解析到你的服务器 IP。
2. 服务器环境 ：支持 Linux（如 Ubuntu、CentOS）或类似系统。
3. **Web** 服务器 ：已安装 Nginx 或 Apache。
4. 管理员权限 ：需要 root 或 sudo 权限来执行命令。

本文以 Ubuntu 20.04 和 Nginx 为例，其他环境配置类似，可参考 Certbot 官网。

????

下面是使用 Certbot 获取和配置 HTTPS 证书的完整流程。整个过程可以分为五个步骤：

准备服务器和域名

安装 Certbot

获取 HTTPS 证书

配置 Web 服务器

设置自动续期

?? 1??? Certbot

Certbot 的安装非常简单，推荐使用 snap 安装方式，因为它能确保获取最新版本。

在 Ubuntu 系统上，运行以下命令：

```
sudo snap install core; sudo snap refresh core
sudo snap install --classic certbot
sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

验证安装是否成功：

```
certbot --version
```

输出类似 `certbot 2.x.x` 说明安装完成。

?? 2??? HTTPS ??

Certbot 支持多种验证方式，这里我们使用 `--nginx` 插件（适用于 Nginx 用户），它会自动验证域名并修改 Nginx 配置。如果你是 Apache 用户，可以替换为 `--apache`。

运行以下命令：

```
sudo certbot --nginx -d yourdomain.com -d www.yourdomain.com
sudo certbot --nginx --nginx-server-root=/www/server/nginx/conf -d easytribe.bakeding.site
```

- `-d` 指定需要 HTTPS 的域名，可以多次使用以支持多个子域名。
- Certbot 会通过 HTTP-01 挑战验证域名所有权，确保你的域名指向当前服务器。

执行过程中，Certbot 会提示你输入邮箱（用于续期通知）和同意服务条款。完成后，证书将存储在 `/etc/letsencrypt/live/yourdomain.com/` 目录下。

?? 3??? Web ???

如果你使用 `--nginx` 插件，Certbot 会自动修改 Nginx 配置文件，添加 HTTPS 支持。你可以检查配置文件（通常在 `/etc/nginx/sites-available/`）：

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

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

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

    # 其他配置...
}
```

如果 Certbot 未自动配置，你需要手动添加上述 HTTPS server 块，并重启 Nginx：

```
sudo nginx -t
sudo systemctl reload nginx
```

?? 4??? HTTPS

在浏览器中访问 `https://yourdomain.com`，检查是否加载正常。你也可以使用在线工具（如 SSL Labs 的 SSL Server Test）检查证书状态。

?? 5???????

Let’s Encrypt 证书有效期为 90 天，Certbot 提供自动续期功能。测试自动续期是否正常工作：

```
sudo certbot renew --dry-run
```

如果没有报错，说明续期配置正常。Certbot 默认会通过 cron 或 systemd 定时任务自动续期。你可以查看 systemd 定时任务：

```
sudo systemctl status snap.certbot.renew.service
```

确保服务是启用状态，通常 Certbot 会每天尝试续期。

?????????

1. **“DNS 解析错误”怎么办?**
   确保域名已正确解析到服务器 IP。使用 `dig yourdomain.com` 或 `nslookup` 检查 DNS 状态。
2. **Nginx 配置未自动更新?**
   手动检查 `/etc/letsencrypt/live/yourdomain.com/` 下的证书路径，并更新 Nginx 配置文件。
3. **续期失败?**
   检查服务器是否允许 80 端口访问，Let’s Encrypt 需要通过 HTTP 验证续期。
4. **多域名支持?**
   在获取证书时，添加多个 `-d` 参数，如 `-d yourdomain.com -d www.yourdomain.com -d api.yourdomain.com`。

???

- 备份证书：定期备份 `/etc/letsencrypt/` 目录，避免意外丢失。
- 强制 **HTTPS**：在 Nginx 配置中添加 301 重定向，确保所有 HTTP 流量跳转到 HTTPS。
- 监控续期：可以通过邮件通知或脚本监控续期状态。

??

通过 Certbot 和 Let’s Encrypt，任何人都能轻松为网站启用 HTTPS。整个过程简单高效，从安装到配置只需几分钟，且自动续期功能让维护变得无忧。希望这篇教程能帮你快速上手 HTTPS 配置，让你的网站更安全、更专业！

如果有任何问题，欢迎在评论区交流，或者访问 Certbot 官网 获取更多帮助。使用 Certbot 获取免费 HTTPS 证书：从零开始的 HTTPS 配置指南 - 使用 Let’s Encrypt 免费申请泛域名 SSL 证书，并实现自动续期

Revision #1
Created 2025-12-15 08:33:53 CST by eason
Updated 2025-12-15 08:34:05 CST by eason