黑客派

一键式申请 SSL 证书，让网站获得 SSL A+ 评级

作者：jianwi

原文链接：https://hacpai.com/article/1538637833079

来源网站：黑客派

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

<blockquote>
【原创】
 本文作者：Denghui.Zhou，欢交流讨论。
 原文链接：https://jianwi.com/articles/os/ssl/quickstart.html
 版权声明：原创不易，转载请注明出处谢谢！
</blockquote>
<h4 id="1-申请Let-s-Encrypt永久免费SSL证书">1、申请 Let's Encrypt 永久免费 SSL 证书</h4>

完全卸载

<pre><code class="language-go highlight-chroma">acme.sh --uninstall
rm -rf /srv/acme/package /srv/acme/config
</code></pre>

重新安装

<pre><code class="highlight-chroma">export LE_WORKING_DIR=/srv/acme/package
export LE_CONFIG_HOME=/srv/acme/config
export CERT_HOME=/srv/acme/certs
curl https://get.acme.sh | sh
source $LE_WORKING_DIR/acme.sh.env
</code></pre>

设置自动更新

<pre><code class="highlight-chroma">$LE_WORKING_DIR/acme.sh \
--accountemail "demo@domain.com" \
--useragent "SSL证书服务" \
--upgrade --auto-upgrade
</code></pre>
如果要关闭自动更新，请执行下面命令
<pre><code class="highlight-chroma">$LE_WORKING_DIR/acme.sh --upgrade --auto-upgrade 0
</code></pre>

自动申请证书
 腾讯云托管的域名，需要获取 DNSPod 的 DNS API 口令

<pre><code class="highlight-chroma">export DP_Id="<DP_Id>"
export DP_Key="<DP_Key>"
$LE_WORKING_DIR/acme.sh --issue --dns dns_dp -d domain.com -d *.domain.com
</code></pre>
阿里云托管的域名，需要获取 DNS 的 Access Token
<pre><code class="highlight-chroma">export Ali_Key="<Ali_Key>"

export Ali_Secret="<Ali_Secret>"
$LE_WORKING_DIR/acme.sh --issue --dns dns_ali -d domain.com -d *.domain.com
</code></pre>

强制更新证书

<pre><code class="highlight-chroma">$LE_WORKING_DIR/acme.sh --renew --force -d domain.com
</code></pre>

部署证书
 部署证书，并配置当证书更新时，自动重载 Nginx，使 Nginx 的 SSL 服务更新证书并生效

<pre><code class="highlight-chroma">export SSL_NGINX_HOME=/etc/ssl/nginx/certs/domain.com
mkdir -p $SSL_NGINX_HOME
$LE_WORKING_DIR/acme.sh --installcert -d domain.com \
--cert-file $SSL_NGINX_HOME/cert.cer \
--key-file $SSL_NGINX_HOME/private.key \
--ca-file $SSL_NGINX_HOME/ca.cer \
--fullchain-file $SSL_NGINX_HOME/fullchain.cer \
--reloadcmd "systemctl force-reload nginx"
</code></pre>

申请到的 SSL 证书基本信息如下图：
 <img src="https://static.hacpai.com/images/img-loading.svg" alt="SSL 证书信息图" data-src="/assets/os/ssl/img/2.png">
SSL 证书颁发机构和路径如下图：
 <img src="https://static.hacpai.com/images/img-loading.svg" alt="SSL 证书路径图" data-src="/assets/os/ssl/img/3.png">
SSL 证书支持泛域名，证书详细信息如下图：
 <img src="https://static.hacpai.com/images/img-loading.svg" alt="SSL 证书详细信息图" data-src="/assets/os/ssl/img/4.png">

<h4 id="2-配置Nginx-SSL-获得更安全的HTTPS网站">2、配置 Nginx SSL，获得更安全的 HTTPS 网站</h4>
作者查阅了 Nginx 文档以及 SSL 配置说明，经多次测试，整理了一份安全性最高的 Nginx 站点 SSL 配置模板，模板下载地址如下：
 Nginx 的 SSL 站点配置模板
使用前需要生成 nginx 的 ssl_dhparam 证书，并升级 Nginx 版本到最新版本，否则部分参数不持。
<pre><code class="highlight-chroma">openssl dhparam -out /etc/nginx/dhparam.pem 4096
</code></pre>
按上述模板配置好 HTTPS 站点，让网站轻松获得 SSL Labs 的 A+ 评级，如下图：
<img src="https://static.hacpai.com/images/img-loading.svg" alt="SSL Labs 网站安全测等级图" data-src="/assets/os/ssl/img/1.png">