

Letsencrypt

Debian 9

```
apt update  
apt install certbot
```

Generate Strong Dh (Diffie-Hellman) Group

```
openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
```

Obtaining a Let's Encrypt SSL certificate Webroot way

```
mkdir -p /var/lib/letsencrypt/.well-known  
chgrp www-data /var/lib/letsencrypt  
chmod g+s /var/lib/letsencrypt
```

To avoid duplicates and to support multiple vhosts, create config files:

</etc/apache2/conf-available/letsencrypt.conf>

```
Alias /.well-known/acme-challenge/ "/var/lib/letsencrypt/.well-known/acme-challenge/"  
<Directory "/var/lib/letsencrypt/">"  
    AllowOverride None  
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec  
    Require method GET POST OPTIONS  
</Directory>
```

</etc/apache2/conf-available/ssl-params.conf>

```
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH  
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1  
SSLHonorCipherOrder On  
Header always set Strict-Transport-Security "max-age=63072000;  
includeSubDomains; preload"  
Header always set X-Frame-Options SAMEORIGIN  
Header always set X-Content-Type-Options nosniff  
# Requires Apache >= 2.4  
SSLCompression off  
SSLUseStapling on  
SSLStaplingCache "shmc:logs/stapling-cache(150000)"  
# Requires Apache >= 2.4.11  
SSLSessionTickets Off  
  
SSLOpenSSLConfCmd DHParameters "/etc/ssl/certs/dhparam.pem"
```

Enable mod_ssl and mod_headers in apache:

```
a2enmod ssl  
a2enmod headers
```

Also enable http2 module

```
a2enmod http2
```

Enable SSL config

```
a2enconf letsencrypt  
a2enconf ssl-params
```

Reload apache config

```
systemctl reload apache2
```

Now use certbot with the webroot plugin to obtain the Letsencrypt certificate files

```
certbot certonly --agree-tos --email admin@example.com --webroot -w  
/var/lib/letsencrypt/ -d example.com -d www.example.com
```

Adjust/create virtualhost file for the domain and enforce https, redirect www to non-www if desired:

</etc/apache2/sites-available/example.com.conf>

```
<VirtualHost *:80>  
    ServerName example.com  
    ServerAlias www.example.com  
  
    Redirect permanent / https://example.com/  
</VirtualHost>  
  
<VirtualHost *:443>  
    ServerName example.com  
    ServerAlias www.example.com  
  
    Protocols h2 http/1.1  
  
    <If "%{HTTP_HOST} == 'www.example.com'">  
        Redirect permanent / https://example.com/  
    </If>  
  
    DocumentRoot /var/www/example.com/public_html  
    ErrorLog ${APACHE_LOG_DIR}/example.com-error.log  
    CustomLog ${APACHE_LOG_DIR}/example.com-access.log combined  
  
    SSLEngine On  
    SSLCertificateFile /etc/letsencrypt/live/example.com/fullchain.pem
```

```
SSLCertificateKeyFile /etc/letsencrypt/live/example.com/privkey.pem  
# Other Apache Configuration  
</VirtualHost>
```

check configuration, then reload config

```
apachectl configtest  
systemctl reload apache2
```

To auto-renew the cert:

</etc/cron.d/certbot>

```
0 */12 * * * root test -x /usr/bin/certbot -a \! -d /run/systemd/system  
&& perl -e 'sleep int(rand(3600))' && certbot -q renew --renew-hook  
"systemctl reload apache2"
```

Test renewal process

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

<https://linuxize.com/post/secure-apache-with-let-s-encrypt-on-debian-9/>

From:
<http://wuff.dyndns.org/> - **Wulf's Various Things**



Permanent link:
<http://wuff.dyndns.org/doku.php?id=linux:letsencrypt>

Last update: **2023/05/29 11:55**