Certificado Auto Assinado - Apache

1. Crie o certificado com o comando:

```
$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/apache-selfsigned.key -out
/etc/ssl/certs/apache-selfsigned.crt
```

Output:

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:New York City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Bouncy
Castles, Inc.
Organizational Unit Name (eg, section) []:Ministry of Water Slides
Common Name (e.g. server FQDN or YOUR name) []:server_IP_address
Email Address []:admin@your_domain.com
```

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

2. Configurando apache para usar SSL. Para isso, abra o arquivo em /etc/apache2/conf-available/ssl-params.conf e insira:

```
#from https://cipherli.st/
#and
https://raymii.org/s/tutorials/Strong_SSL_Security_On_Apache2.html

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder On
# Disable preloading HSTS for now.  You can use the commented out
header line that includes
# the "preload" directive if you understand the implications.
```

```
#Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
# Requires Apache >= 2.4
SSLCompression off
SSLSessionTickets Off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"

SSLOpenSSLConfCmd DHParameters "/etc/ssl/certs/dhparam.pem"
```

3. Faça backup do arquivo /etc/apache2/sites-available/default-ssl.conf com o comando:

```
$ sudo cp /etc/apache2/sites-available/default-ssl.conf
/etc/apache2/sites-available/default-ssl.conf.bak
```

4. Agora, abra o arquivo com o seu editor de texto predileto:

```
$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```

5. Altere as seguintes informações:

```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin your_email@example.com
                ServerName server_domain_or_IP

                DocumentRoot /var/www/html

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                SSLEngine on

                SSLCertificateFile
/etc/ssl/certs/apache-selfsigned.crt
```

```
                SSLCertificateKeyFile
/etc/ssl/private/apache-selfsigned.key

                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>

                BrowserMatch "MSIE [2-6]" \
                               nokeepalive ssl-unclean-shutdown \
                               downgrade-1.0 force-response-1.0

        </VirtualHost>
</IfModule>
```

6. Altere o virtual host para encaminhar para HTTPS automaticamente,com o comando:

```
$ sudo nano /etc/apache2/sites-available/000-default.conf
```

```
<VirtualHost *:80>
        . . .

        Redirect "/" "https://your_domain_or_IP/"

        . . .
</VirtualHost>
```

7. Aplique as configurações no apache com os comandos:

```

$ sudo a2enmod ssl
$ sudo a2enmod headers
$ sudo a2ensite default-ssl
$ sudo a2enconf ssl-params
$ sudo apache2ctl configtest
```

Output:

```
AH00558: apache2: Could not reliably determine the server's fully
```

```
qualified domain name, using 127.0.1.1. Set the 'ServerName' directive
globally to suppress this message
Syntax OK
```

8. Feito isso, inicie com o comando:

```
$ sudo systemctl restart apache2
```

9. Pronto, basta testar!