

Apache: включаем OCSP и HSTS

OCSP

Включается глобально — нужно раскомментировать строки:

```
# ee /usr/local/etc/apache24/extra/httpd-ssl.conf

# Enable stapling for all SSL-enabled servers:
SSLUseStapling On
SSLStaplingCache "shmcb:/var/run/ssl_stapling(32768)"
SSLStaplingStandardCacheTimeout 3600
```

или для каждого виртуального хоста индивидуально в файле `./extra/httpd-vhosts.conf` или в файлах `./Includes/`:

```
<VirtualHost _default_:443>
# General setup for the virtual host
DocumentRoot "/usr/local/www/apache24/data"
ServerName mail.domen.ua:443
ServerAdmin postmaster@domen.ua
ErrorLog "/var/log/httpd-error.log"
TransferLog "/var/log/httpd-access.log"

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

...
SSLUseStapling On
SSLStaplingCache "shmcb:/var/run/ssl_stapling(32768)"
...
</VirtualHost>
```

Проверяем на сайтах www.ssllabs.com, www.digicert.com или в консоли:

```
% openssl s_client -connect mail.imp.kiev.ua:443 -tls1 -
tlsextdebug -status
```

OCSP response:

=====

OCSP Response Data:

OCSP Response Status: **successful** (0x0)

Response Type: **Basic OCSP Response**

Version: 1 (0x0)

Responder Id: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3

Produced At: Jul 22 22:37:00 2019 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 7EED44DAAB3FCF8A220646C16A09AD71085D

Issuer Key Hash:

A84A6A63047DDDBAE6D139B7D44DAEFF3A8ECA1

Serial Number: 03F102AA63047DDDBAE6DA7043D44DA589

Cert Status: **good**

This Update: Jul 22 22:00:00 2019 GMT

Next Update: Jul 29 22:00:00 2019 GMT

HSTS

Добавляем строку в extra/httpd-vhosts.conf

```
<VirtualHost *:443>
```

```
...
```

```
## HSTS
```

```
Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains;"
```

```
</VirtualHost>
```

При этом должна быть настроена переадресация с http на https:

ee extra/httpd-vhosts.conf

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

```
ServerName mail.domen.ua
```

```
RewriteEngine On
```

```
RewriteCond %{HTTPS} off
```

```
RewriteRule (.*?) https://%{HTTP_HOST}%{REQUEST_URI}
```

```
</VirtualHost>
```

Проверяем на сайте www.ssllabs.com.

