Setting up OCSP for NGINX server

Question

How do I set up an OCSP for server-based on NGINX?

Answer

How to enable OCSP Stapling on NGINX:

1. First check that NGINX 1.3.7 or above is installed by running the following command:

```
nginx –v
```

Versions lower than 1.3.7 do not support OCSP stapling, so you should update NGINX before proceeding with the rest of this tutorial.

2. Check whether OCSP stapling is already enabled or not:

- Use openssl command:

```
openssl s_client -connect login.live.com:443 -tls1 -tlsextdebug -status
```

- Scroll down to "OCSP response:"
- If OCSP is enabled, the “OCSP Stapling” is

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

- If OCSP is not enabled, you won’t see any OCSP Response Data:

```
OCSP response: no response sent
```

3. If Step 2 revealed no evidence that OCSP is enabled on your server, it is first worth checking that NGINX can actually connect to our OCSP servers. OCSP servers are at the following locations:

DNS HOSTNAME(S)	Destination IP	Port

OCSP.ComodoCA.com OCSP.usertrust.com	178.255.83.1 or 2a02:1788:2fd::b2ff:5301	Tcp/80

To check connectivity, use the following telnet command:

```
telnet OCSP.ComodoCA.com 80
```

If the test is successful the reply will state

```
Connected to OCSP.ComodoCA.com
```

for at least one of the ‘Destination IP’ addresses in the table above.

If the test is unsuccessful the replies will state

```
Network Unreachable
```

or / and

```
Connection Timed Out
```

Please make the required network changes to allow NGINX to connect to our OCSP servers.
Once complete, re-run the test in Step 2 to establish whether OCSP stapling is already enabled.

4. To enable OCSP stapling, edit the server block configuration file for your site (or nginx.conf if server blocks are not used) using the editor of your choice (example editors include nano or vim):

```
nano /etc/nginx/sites-enabled/my-domain.com-ssl.conf
```

or

```
nano /etc/nginx/nginx.conf
```

If you need to enable OCSP stapling on just one server block, it must be the “default_server”. If you need to enable OCSP stapling on more than one server block, it must be enabled on the "default_server" before it can be enabled on any other server block.

5. Turn on OCSP stapling and enable the server to check OCSP by adding the following lines inside

```
the server block:
ssl_stapling on;
ssl_stapling_verify on;
```

6. Point to a trusted certificate chain file. This must contain the intermediate & root certificates in order

```
ssl_trusted_certificate /etc/nginx/ssl/full_chain.pem
```

Use the example below as a reference configuration:

```
server {
  listen 443 default_server;
  server_name mydomain.com

  # Change this to point to your document root.

  root /srv/www/example.com/public_html;
  index index.html index.htm;

  ssl on;
  ssl_certificate /etc/nginx/ssl/mydomain.com/my_certificate.crt;
  ssl_certificate_key /etc/nginx/ssl/mydomain.com/mydomain.key;

  ssl_stapling on;
  ssl_stapling_verify on;
  ssl_trusted_certificate /etc/nginx/ssl/full_chain.pem

}
```

7. Test your configuration is OK:

```
sudo service nginx configtest
OR
nginx -t
```

8. Restart NGINX if OK:

```
sudo service nginx reload
OR
systemctl restart nginx
```

9. Verify OCSP Stapling is working by repeating Step 2

Revision #2
Created 2026-08-07 14:53:08 UTC by Sarath
Updated 2026-08-07 16:02:08 UTC by Sarath