Configurer SSL sur NGINX avec Gandi

Procédure

1. Créer un certificat chaine

```
cat makeitsimple.be.crt GandiStandardSSLCA2.pem >
makeitsimple.be.chain.crt
```

2. Créer une clé Diffie-Hellman

```
cd /etc/ssl
openssl dhparam -out dh.pem 4096
```

3. Créer un fichier de configuration modulaire

```
nano /etc/nginx/wildcard_example_com.ssl.conf
```

Et voici un exemple de contenu:

```
ssl_certificate /etc/ssl/certs/makeitsimple.be.chain.crt;
ssl_certificate_key /etc/ssl/private/makeitsimple.be.key;

ssl_session_timeout 24h;
ssl_session_cache shared:SSL:10m;

ssl_dhparam /etc/ssl/dh.pem;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-
AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-
SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-
SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-
GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-
SHA:AES:CAMELLIA:DES-CBC3-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-
SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA';
ssl_prefer_server_ciphers on;

ssl_stapling on;
ssl_stapling_verify on;
ssl_trusted_certificate /etc/ssl/certs/gandi-standardssl-2.chain.pem;
resolver 127.0.0.1;
```

4. Faire un fichier

Sources

- https://jlecour.github.io/ssl-gandi-nginx-debian/
- https://angristan.fr/configurer-https-nginx/

From:
https://wiki.makeitsimple.be/ - **makeITsimple wiki**

Permanent link:
https://wiki.makeitsimple.be/doku.php?id=linux:nginx:ssl&rev=1623609797

Last update: **2021/06/20 09:42**