

Compte rendu TP PKI Noa Fontaine :

Tout d'abord il faut installer Nginx et faire le nécessaire pour avoir notre serveur web fonctionnel sans certificat SSL. Voici les étapes à suivre pour mettre en place le serveur WEB.

- Tout d'abord il faut installer nginx avec la commande suivante :

`dnf install -y nginx`

(Ne pas oublier de faire un `dnf update` juste avant)

```
[root@SRVWEB ~]# dnf install -y nginx
```

Ensuite on active le services Nginx :

`Systemctl start nginx`

`Systemctl enable --now nginx`

```
[root@SRVWEB ~]# systemctl start nginx
[root@SRVWEB ~]# systemctlctl enable --now nginx
-bash: systemctlctl: command not found
[root@SRVWEB ~]# systemctl enable --now nginx
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /lib/systemd/system/nginx.service.
[root@SRVWEB ~]#
```

On ouvre les ports du firewall port 80 et port 443 en tcp et en permanent grâce aux commandes suivantes :

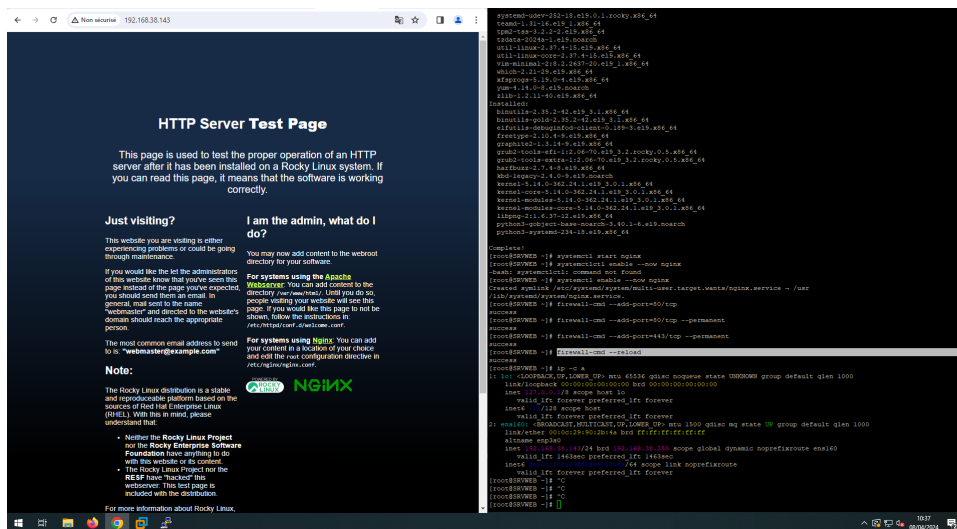
`firewall-cmd --add-port=80/tcp --permanent`

`firewall-cmd --add-port=443/tcp --permanent`

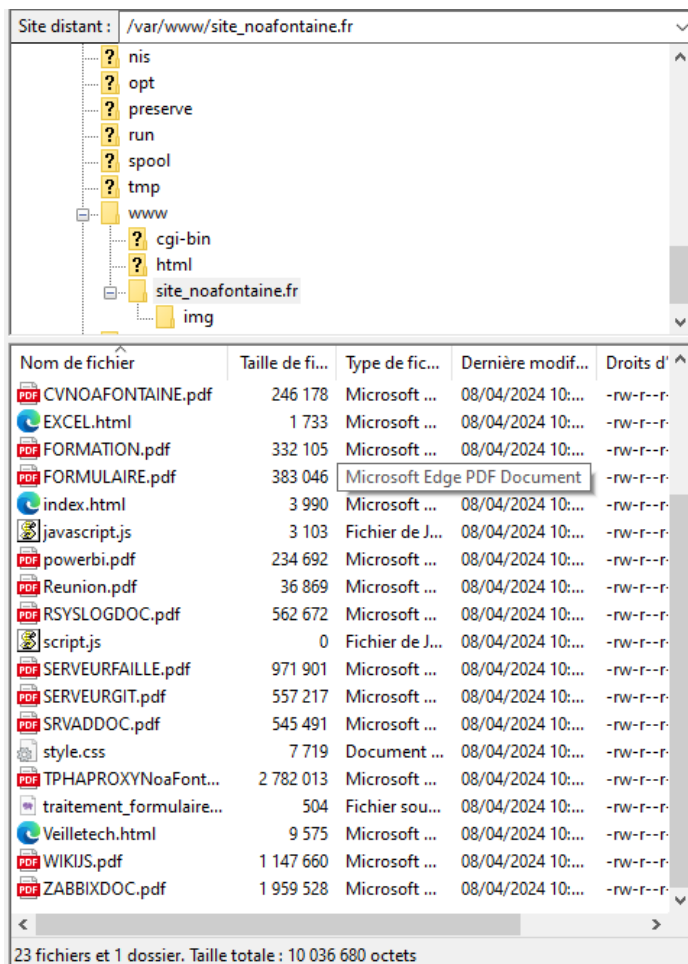
`firewall-cmd --reload`

```
[root@SRVWEB ~]# firewall-cmd --add-port=80/tcp --permanent
success
[root@SRVWEB ~]# firewall-cmd --add-port=443/tcp --permanent
success
[root@SRVWEB ~]# firewall-cmd --reload
success
[root@SRVWEB ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:90:2b:4a brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.38.143/24 brd 192.168.38.255 scope global dynamic noprefixroute ens160
        valid_lft 1463sec preferred_lft 1463sec
    inet6 fe80::20c:29ff:fe90:2b4a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@SRVWEB ~]#
```

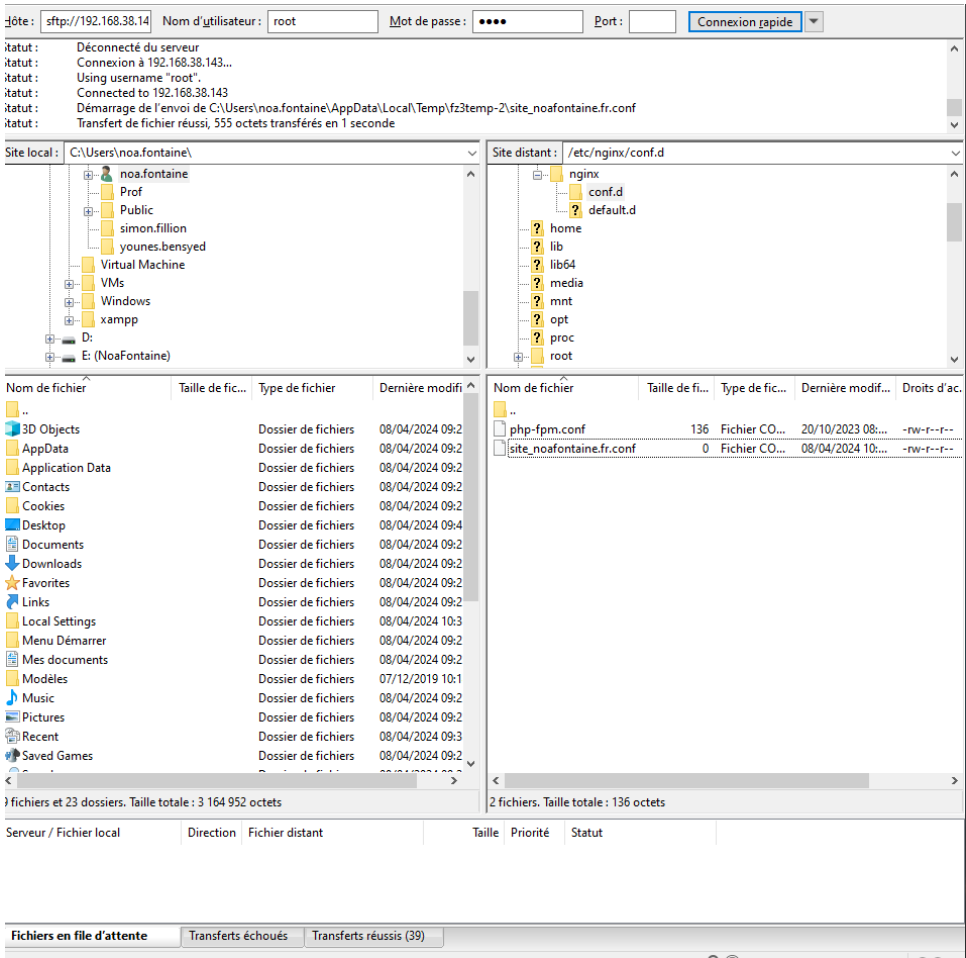
On peut voir que nginx est présent



J'ouvre Filezilla pour transférer mon site internet dans la machine virtuelle. J'ai mis mon PortFolio dans le répertoire /var/www/site-noafontaine.fr



Maintenant j'ai créé un fichier conf pour mon PortFolio. Voici son contenu. Il se situe dans /etc/nginx/conf.d



```
site_noafontaine.fr.conf - Bloc-notes
Fichier Edition Format Affichage Aide
server { listen 80;

listen [::]:80;

root /var/www/site_noafontaine.fr/;
index index.html index.htm index.nginx-debian.html sign-up.php;

server_name noafontaine.fr ; location ~* \.php$ {

fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
} fastcgi_param SCRIPT_NAME $fastcgi_script_name;

access_log /var/log/nginx/access_noafontaine.fr.log; error_log /var/log/nginx/error_noafontaine.fr.log; location / {
try_files $uri $uri/ =404; }}
```

server { listen 80;

listen [::]:80;

```

root /var/www/site_noafontaine.fr/;

index index.html index.htm index.nginx-debian.html sign-up.php;

server_name noafontaine.fr ; location ~* \.php$ {

fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;

} fastcgi_param SCRIPT_NAME $fastcgi_script_name;

access_log /var/log/nginx/access_noafontaine.fr.log; error_log
/var/log/nginx/error_noafontaine.fr.log; location / {

try_files $uri $uri/ =404; }}

```

Voici le résultat :



Maintenant intéressons-nous au certificat. Sur SRVAC il faut créer notre clé privée

```
[root@SRVAC key]# openssl genrsa -aes256 -out CA.key
```

On crée un fichier CSR pour le certificat racine

```
[root@SRVAC key]# openssl req -new -nodes -key CA.key -out CA.csr -sha256
[Enter pass phrase for CA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
[Country Name (2 letter code) [XX]:FR
[State or Province Name (full name) []:LILLE
[Locality Name (eg, city) [Default City]:LILLE
[Organization Name (eg, company) [Default Company Ltd]:LILLE
[Organizational Unit Name (eg, section) []:LILLE
[Common Name (eg, your name or your server's hostname) []:SRVWEB
[Email Address []:LILLE

Please enter the following 'extra' attributes
to be sent with your certificate request
[A challenge password []:root
[An optional company name []:LILLE
[root@SRVAC key]#
```

Il faut ensuite signer le fichier csr avec notre clé privée

```
[root@SRVAC key]# openssl x509 -req -days 365 -in CA.csr -out CA.crt -signkey CA.key
```

On crée un fichier de configuration pour signer nos demandes (dans le même répertoire que notre clé privée et de notre certificat).

```
[ req ]
default_bits = 2048
distinguished_name = req_distinguished_name
string_mask = utf8only
default_md = sha512
```

```
[root@SRVWEB ~]# openssl genrsa -out customCA-site_noafontaine.fr.key
```

```
[root@SRVWEB ~]# openssl req -new -nodes -out noafontaine.fr.csr -newkey rsa:4096 -keyout customCA-noafontaine.fr.key -subj '/CN=noafontaine.fr/C=FR/ST=LILLE/L=LILLE/O=LILLE'
```

Puis je vais générer un fichier `demo.fr.v3.ext` avec les différents noms de mon serveur WEB et son IP je l'ai ensuite renommé `noafontaine.fr.v3.ext`.

```

[[root@SRVAC key]# cat > demo.fr.v3.ext << EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = noafontaine.fr
DNS.2 = www.noafontaine.fr
IP.1 = 192.168.161.153
EOF
[[root@SRVAC key]# █

```

On va pouvoir lire notre CSR depuis notre CA

```

[[root@SRVAC key]# openssl req -text -noout -verify -in noafontaine.fr.csr | grep
Subject
Certificate request self-signature verify OK
    Subject: CN = noafontaine.fr, C = FR, ST = LILLE, L = LILLE, O = LILLE
    Subject Public Key Info:
[[root@SRVAC key]# █

```

Depuis notre CA, nous signons le CSR et générons le certificat. Il faudra le transmettre à notre serveur WEB

```

[[root@SRVAC key]# openssl x509 -req -in noafontaine.fr.csr -CA CA.crt -CAkey CA.
key -CAcreateserial -out noafontaine.fr.crt -days 730 -sha256 -extfile noafontai
ne.fr.v3.ext
Certificate request self-signature ok
subject=CN = noafontaine.fr, C = FR, ST = LILLE, L = LILLE, O = LILLE
[Enter pass phrase for CA.key:
[[root@SRVAC key]# █

```

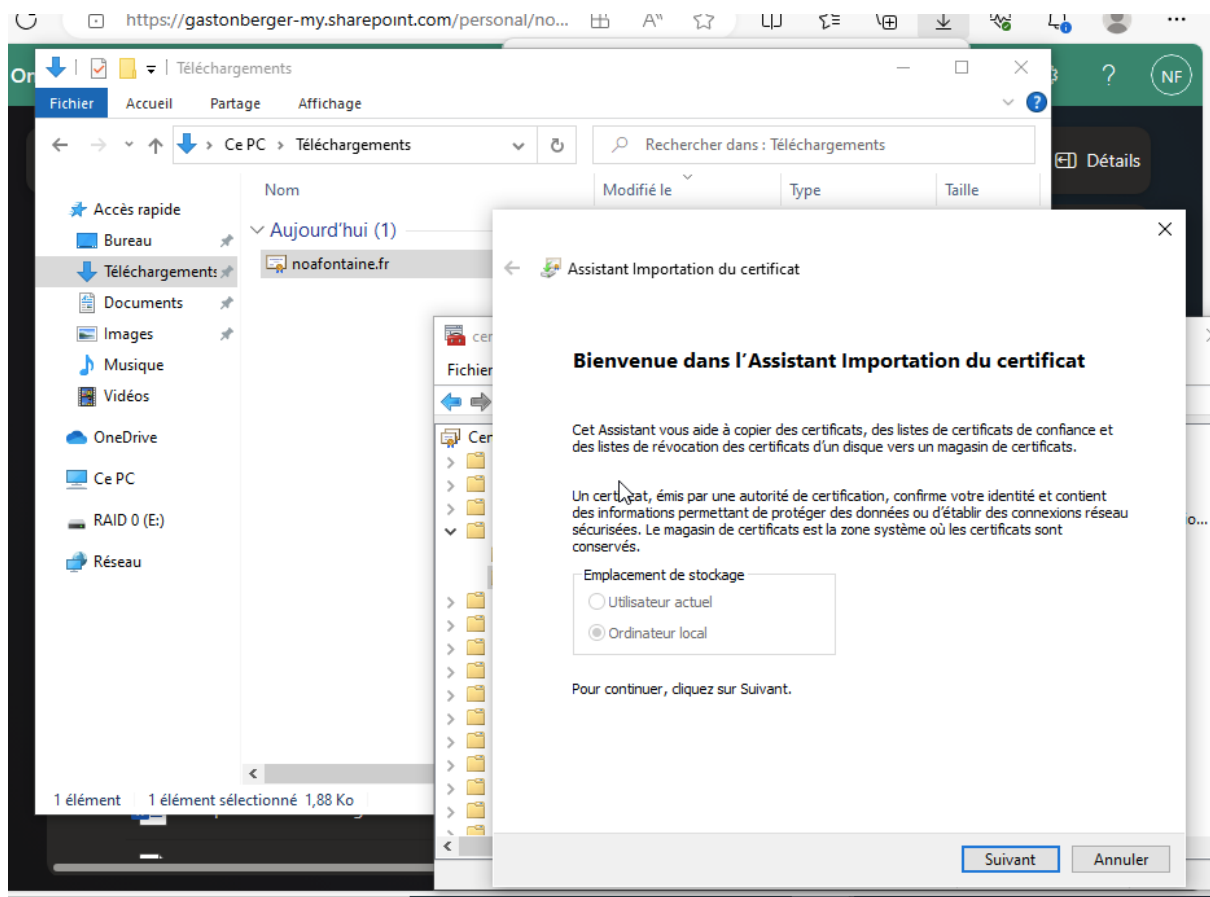
Il reste à configurer Nginx avec le certificat et notre clé privée.

```

GNU nano 5.6.1      site_noafontaine.fr.conf
server {
listen 443 http2 ssl;
server_name noafontaine.fr;
ssl_certificate /etc/nginx/https/noafontaine.fr.crt;
ssl_certificate_key /etc/nginx/https/customCA-noafontaine.fr.key;
root /var/www/site_noafontaine.fr/; index index.html;
}
access_log /var/log/nginx/noafontaineaccess.log;
error_log /var/log/nginx/noafontaineerrorlog;

```

On importe le certificat racine







Fin de l'Assistant Importation du certificat

Le certificat sera importé après avoir cliqué sur Terminer.

Vous avez spécifié les paramètres suivants :

Magasin de certificats sélectionné	Déterminé automatiquement par l'Assistant
Contenu	Certificat
Nom du fichier	C:\Users\Fontaine\Downloads\noafontaine.fr.crt

 Microsoft Windows Hardware ...	Microsoft Root Authority	3
 noafontaine.fr	SRVWEB	1
 Root Agency	Root Agency	0
 www.verisign.com/CPS Incorp....	Class 3 Public Primary Certificatio...	2

Et la clé est mise en place