SOMMAIRE

1. Configuration côté SSL

Je vérifie que le paquet openssl est déjà installé sur DS2

```
root@DS2: ~#dpkg -l | grep -i openssl
ii  libcurl4t64:amd64            8.14.1-2+deb13u2                amd64        easy-to-use client-side URL transfer libra
ii  openssl                      3.5.4-1~deb13u2                 amd64        Secure Sockets Layer toolkit - cryptograph
ii  openssl-provider-legacy      3.5.4-1~deb13u2                 amd64        Secure Sockets Layer toolkit - cryptograph
ii  ssl-cert                     1.1.3                           all          simple debconf wrapper for OpenSSL
root@DS2: ~#
```

Je vérifie la présence du fichier de configuration

```
root@DS2: ~#cd /etc/ssl
root@DS2: /etc/ssl#ls -l
total 40
drwxr-xr-x 2 root root     20480  5 févr. 15:11 certs
-rw-r--r-- 1 root root     12411 24 janv. 16:50 openssl.cnf
drwx--x--- 2 root ssl-cert  4096  5 févr. 15:11 private
root@DS2: /etc/ssl#
```

Je fais une copie du fichier de configuration

```
root@DS2: /etc/ssl#cp openssl.cnf openssl.cnf.sauv
root@DS2: /etc/ssl#ls -l
total 56
drwxr-xr-x 2 root root     20480  5 févr. 15:11 certs
-rw-r--r-- 1 root root     12411 24 janv. 16:50 openssl.cnf
-rw-r--r-- 1 root root     12411 28 avril 10:33 openssl.cnf.sauv
drwx--x--- 2 root ssl-cert  4096  5 févr. 15:11 private
root@DS2: /etc/ssl#
```

1.1 Création d’une autorité de certification racine

Je créer un environnement du CA

```
root@DS2: /etc/ssl#mkdir /etc/ssl/CA
root@DS2: /etc/ssl#mkdir /etc/ssl/CA/certs /etc/ssl/CA/private /etc/ssl/CA/newcerts
root@DS2: /etc/ssl#ls -l /etc/ssl/CA
total 12
drwxr-xr-x 2 root root 4096 28 avril 10:36 certs
drwxr-xr-x 2 root root 4096 28 avril 10:36 newcerts
drwxr-xr-x 2 root root 4096 28 avril 10:36 private
root@DS2: /etc/ssl#_
```

Je créer les deux fichiers qui se nomment **serial** et **index.txt**

```
root@DS2: /etc/ssl#echo "01" > /etc/ssl/CA/serial
root@DS2: /etc/ssl#touch /etc/ssl/CA/index.txt
root@DS2: /etc/ssl#_
```

Je modifie le fichier de configuration

```
#####################################################################
[ ca ]
default_ca      = CA_default            # The default ca section

#####################################################################
[ CA_default ]

dir             = /etc/ssl/CA           # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/certs/cacert.pem         # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem # The private key

x509_extensions = usr_cert              # The extensions to add to the cert
```

Je remplace usr_cert par v3_req et je décommente copy_extensions

```
####################################################################
[ CA_default ]

dir             = /etc/ssl/CA           # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/certs/cacert.pem        # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem # The private key

x509_extensions = v3_req                # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default            # Subject Name options
cert_opt        = ca_default            # Certificate field options

# Extension copying option: use with caution.
copy_extensions = copy
```

Je génère la clé privé du CA

```
root@DS2: ~#openssl genrsa -out /etc/ssl/CA/private/cakey.pem 2048
root@DS2: ~#
```

Je créer le certificat de l’autorité

```
root@DS2: ~#openssl req -new -x509 -key /etc/ssl/CA/private/cakey.pem -out /etc/ssl/CA/certs/cacert.pem -days 3650
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) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Saint-Raphael
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sio-exupery
Organizational Unit Name (eg, section) []:bts sio
Common Name (e.g. server FQDN or YOUR name) []:DS2.sio-exupery.fr
Email Address []:
root@DS2: ~#
```

Je vérifie la présence des fichiers **cakey.pem** et **cacert.pem**

```
root@DS2: ~#cd /etc/ssl/CA/private/
root@DS2: /etc/ssl/CA/private#ls -l
total 4
-rw------- 1 root root 1704 28 avril 11:00 cakey.pem
root@DS2: /etc/ssl/CA/private#
```

```
root@DS2: ~#cd /etc/ssl/CA/certs/
root@DS2: /etc/ssl/CA/certs#ls -l
total 4
-rw-r--r-- 1 root root 1391 28 avril 11:02 cacert.pem
root@DS2: /etc/ssl/CA/certs#
```

J’affiche le certificat racine

```
root@DS2: ~#openssl x509 -in /etc/ssl/CA/certs/cacert.pem -text | more_
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0a:96:34:72:be:d9:f7:78:90:c8:58:f0:80:8a:50:82:86:88:25:f5
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FR, ST=France, L=Saint-Raphael, O=sio-exupery, OU=bts sio, CN=DS2.sio-exupery.fr
        Validity
            Not Before: Apr 28 09:02:22 2026 GMT
            Not After : Apr 25 09:02:22 2036 GMT
        Subject: C=FR, ST=France, L=Saint-Raphael, O=sio-exupery, OU=bts sio, CN=DS2.sio-exupery.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:63:01:e6:b9:13:45:f5:f2:ed:95:2b:2f:8c:
                    96:30:c1:6f:ad:62:da:ed:a4:3a:30:2a:09:a8:fa:
                    b6:36:91:68:71:cc:4b:c9:ee:07:71:48:d3:11:fa:
                    25:00:92:15:a2:e2:85:21:5d:19:ad:76:58:77:61:
                    d5:ee:5a:f9:9e:57:0d:09:e5:c4:f1:09:e4:b9:5e:
                    e8:46:87:ce:5c:fa:cc:f6:ed:39:81:50:5d:ac:fc:
                    bf:68:80:bd:5a:d0:39:26:8f:fa:3b:ed:ae:9e:d7:
                    8c:83:b1:c8:ae:0c:7c:68:70:3b:fc:2e:d2:c0:79:
                    08:3a:e5:3a:5d:06:83:17:b4:0f:f5:8a:c5:ad:c2:
                    c5:34:35:ad:62:7b:25:db:e1:55:ba:39:38:26:39:
                    24:f7:af:ec:c0:03:f8:99:9e:23:05:e7:49:64:1a:
                    26:63:96:3f:ea:a9:3c:cd:45:0a:2f:cc:37:db:7c:
                    a8:7f:07:4a:54:50:51:cc:7f:6c:77:27:14:87:57:
                    ed:71:d8:27:c3:0c:9c:47:5c:c3:49:63:16:4e:d5:
                    81:cd:6a:f1:7e:d0:28:a7:04:7f:9e:53:09:14:9b:
                    24:87:25:5c:50:1e:10:47:87:1b:8e:ef:90:d9:01:
                    b9:60:b8:dc:9f:19:af:62:46:2d:af:1e:28:5d:7d:
                    fc:f1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                62:C5:DC:5F:90:F6:70:EB:23:80:88:9B:2E:E2:21:48:74:02:71:38
            X509v3 Authority Key Identifier:
                62:C5:DC:5F:90:F6:70:EB:23:80:88:9B:2E:E2:21:48:74:02:71:38
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        80:25:5d:60:30:9b:e1:a3:15:f8:a3:e2:d2:54:15:55:f2:b6:
        15:92:d8:26:12:da:9e:c4:b8:74:57:4a:da:d8:a8:2b:d7:84:
        2a:29:83:08:00:79:b8:31:24:7d:00:da:bc:bf:42:04:15:0d:
        41:4a:d2:d9:75:6d:7b:b7:b0:5f:2b:9f:dc:88:38:fc:a2:c9:
        3a:b4:2b:48:76:85:2d:3e:89:03:77:25:c7:65:fa:bd:57:3b:
        53:71:ad:99:cb:73:a8:6d:5e:53:92:c5:44:fe:e8:34:1a:4d:
--Plus--
```

```
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUCpY0cr7Z93iQyFjwgIpQgoaIJfUwDQYJKoZIhvcNAQEL
BQAwezELMAkGA1UEBhMCRlIxDzANBgNVBAgMBkZyYW5jZTEWMBQGA1UEBwwNU2Fp
bnQtUmFwaGFlbDEUMBIGA1UECgwLc2lvLWV4dXBlcnkxEDAOBgNVBAsMB2J0cyBz
aW8xGzAZBgNVBAMMEkRTMi5zaW8tZXh1cGVyeS5mcjAeFw0yNjA0MjgwOTAyMjJa
Fw0zNjA0MjUwOTAyMjJaMHsxCzAJBgNVBAYTAkZSMQ8wDQYDVQQIDAZGcmFuY2Ux
FjAUBgNVBAcMDVNhaW50LVJhcGhhZWwxFDASBgNVBAoMC3Npby1leHVwZXJ5MRAw
DgYDVQQLDAdidHMgc2lvMRswGQYDVQQDDBJEUzIuc2lvLWV4dXBlcnkuZnIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvYwHmuRNF9fLtlSsvjJYwwW+t
YtrtpDowKgmo+rY2kWhxzEvJ7gdxSNMR+iUAkhWi4oUhXRmtdlh3YdXuWvmeVw0J
5cTxCeS5XuhGh85c+sz27TmBUF2s/L9ogL1a0Dkmj/o77a6e14yDsciuDHxocDv8
LtLAeQg65TpdBoMXtA/1isWtwsU0Na1ieyXb4VW6OTgmOST3r+zAA/iZniMF50lk
GiZjlj/qqTzNRQovzDfbfKh/B0pUUFHMf2x3JxSHV+1x2CfDDJxHXMNJYxZO1YHN
avF+0CinBH+eUwkUmySHJVxQHhBHhxuO75DZAblguNyfGa9iRi2vHihdffzxAgMB
AAGjUzBRMB0GA1UdDgQWBBRixdxfkPZw6yOAiJsu4iFIdAJxODAfBgNVHSMEGDAW
gBRixdxfkPZw6yOAiJsu4iFIdAJxODAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4IBAQCAJV1gMJvhoxX4o+LSVBVV8rYVktgmEtqexLh0V0ra2Kgr14Qq
KYMIAHm4MSR9ANq8v0IEFQ1BStLZdW17t7BfK5/ciDj8osk6tCtIdoUtPokDdyXH
Zfq9VztTca2Zy3OobV5TksVE/ug0Gk2STp/2r3KsoA4fzE4SkhnKim4i1susoPv5
w74bBPihbNio5VvJ+jVivBruR6UFDG9vQxnkKJNDB6RmPsNbXKCC0jQq2PtC8iyk
uVJ7TkloYaqmMcuCbr4rbUCP3d8Q60rXv/5i6Ji9pRK8kX0qDFSv3VHipxS2LVei
S3/SMYb3EBHSXyLG8quw6cnSSssoGGIa33vP
-----END CERTIFICATE-----
root@DS2: ~#
```

1.2 Création des clés et du certificat du serveur Web

Je génère une paire de clés publique et privé pour le serveur Web

```
root@DS2: ~#openssl genrsa -out /etc/ssl/private/web.key 2048
root@DS2: ~#
```

Je génère une demande de signature de certification

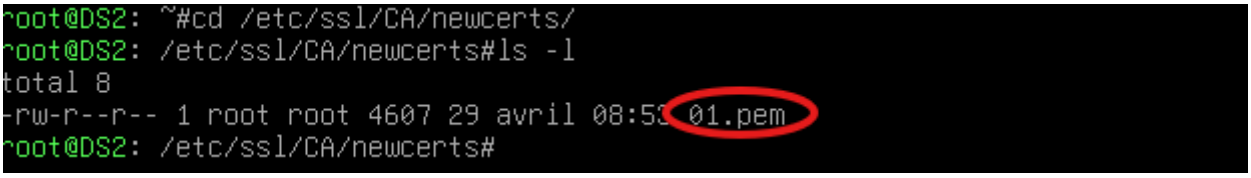
```
root@DS2: ~#openssl req -new -key /etc/ssl/private/web.key -out /etc/ssl/certs/webds2.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields 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) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Saint-Raphael
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sio-exupery
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:secu.sio-exupery.fr
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@DS2: ~#_
```

Je signe le certificat en tant qu'autorité de certification (Je n'ai pas pu prendre la capture d'écran lorsqu'il demande si je veux signer le certificat)

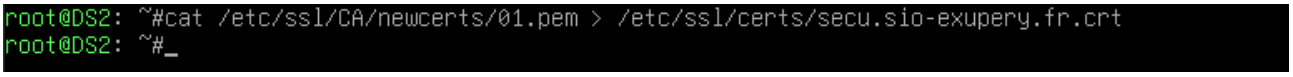
```
root@DS2: ~#openssl ca -in /etc/ssl/certs/webds2.csr -config /etc/ssl/openssl.cnf
Using configuration from /etc/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
ERROR:There is already a certificate for /C=FR/ST=France/O=sio-exupery/CN=secu.sio-exupery.fr
The matching entry has the following details
Type          :Valid
Expires on    :270429065301Z
Serial Number :01
File name     :unknown
Subject Name  :/C=FR/ST=France/O=sio-exupery/CN=secu.sio-exupery.fr
root@DS2: ~#
```

J’affiche le contenu des fichiers index.txt et serial

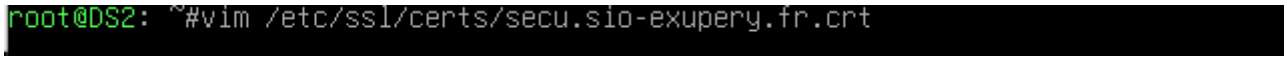
Je vérifie la présence du certificat SSL qui se nomme 01.pem



Je créer le certificat SSL qui se nomme secu.sio-exupery.fr.crt



Je consulte le certificat à l’aide de la commande VIM



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FR, ST=France, L=Saint-Raphael, O=sio-exupery, OU=bts sio, CN=DS2.sio-exupery.fr
        Validity
            Not Before: Apr 29 06:53:01 2026 GMT
            Not After : Apr 29 06:53:01 2027 GMT
        Subject: C=FR, ST=France, O=sio-exupery, CN=secu.sio-exupery.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:f5:2a:b3:54:e1:57:1c:0d:d3:be:6a:76:b5:
                    9f:e4:f4:05:43:94:6a:30:f6:61:9e:f0:b5:46:ab:
                    01:20:dc:b2:94:cf:06:32:17:36:44:cc:26:96:a9:
                    61:89:31:c1:a8:4d:a0:80:38:46:27:ec:4a:d9:00:
                    c6:bc:41:20:df:ab:ea:48:d3:bf:8d:0e:5e:a3:04:
                    07:f7:c3:33:4a:ba:82:27:3b:ab:ee:19:a0:22:0f:
                    8f:a3:17:38:40:f6:33:f5:e5:26:57:d1:4b:94:09:
                    d2:c6:df:02:74:d3:8a:dc:f2:5a:09:df:6e:c1:6b:
                    8a:f7:c1:42:eb:2b:14:55:13:21:0e:f6:a4:d4:b6:
                    9f:58:1e:ba:6b:f7:05:7a:43:b5:04:dd:22:fa:e5:
                    b8:c5:c1:24:29:12:c9:51:73:f0:53:16:cb:85:28:
                    5b:ae:3b:fc:9b:63:17:ea:0a:7f:d3:cc:7f:7b:45:
                    b0:7e:bd:f6:c4:fc:ed:88:0d:60:39:cd:0b:b0:4b:
                    64:ea:f7:00:00:e5:da:6b:36:9b:09:b7:2d:c5:f1:
                    f2:f3:07:9a:95:fb:6e:6e:18:8c:08:80:e4:d4:ea:
                    01:7a:48:c9:17:bc:26:b9:b7:2e:8f:bb:41:9d:5b:
                    d4:72:72:a4:6e:5d:61:9f:99:09:e0:68:6c:5b:e0:
                    55:33
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:secu.sio-exupery.fr
            X509v3 Subject Key Identifier:
                EA:2E:43:CB:7A:4F:18:88:FD:AB:04:43:E0:88:84:0C:F7:0D:23:16
            X509v3 Authority Key Identifier:
                EA:B5:47:B8:B3:70:9D:B4:E3:71:01:B7:60:09:FC:27:0E:BC:52:DF
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        0d:6b:e2:b6:77:57:6a:c5:51:9c:17:21:ce:5a:ff:63:7f:a7:
        40:00:5c:c4:ca:6d:9a:a8:31:18:e1:11:d9:4e:26:68:e9:25:
        5b:99:ab:c3:1d:4e:72:2e:91:02:2d:be:9f:f2:2b:d9:2e:26:
"/etc/ssl/certs/secu.sio-exupery.fr.crt" 84L, 4607B
```

2. Configuration côté Apache

J’active le module **SSL**

```
root@DS2: ~#a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@DS2: ~#
```

Je redémarre le service apache2

```
root@DS2: ~#systemctl reload apache2
root@DS2: ~#
```

Je vérifie la présence du fichier ssl.conf

```
root@DS2: ~#ls -l /etc/apache2/mods-enabled/ | tail -5
lrwxrwxrwx 1 root root 36 29 avril 09:12 socache_shmcb.load -> ../mods-available/socache_shmcb.load
lrwxrwxrwx 1 root root 26 29 avril 09:12 ssl.conf -> ../mods-available/ssl.conf
lrwxrwxrwx 1 root root 26 29 avril 09:12 ssl.load -> ../mods-available/ssl.load
lrwxrwxrwx 1 root root 29  5 févr. 15:12 status.conf -> ../mods-available/status.conf
lrwxrwxrwx 1 root root 29  5 févr. 15:12 status.load -> ../mods-available/status.load
root@DS2: ~#_
```

Dans le fichier **ssl.conf** j'ajoute les lignes **SSLCertificateFile** et **SSLCertificateKeyFile** pour que le serveur Apache puisse disposer de sa clé privé et de son certificat

```
  GNU nano 8.4                                        /etc/apache2/mods-enabled/ssl.conf *
#   Allow insecure renegotiation with clients which do not yet support the
#   secure renegotiation protocol. Default: Off
#SSLInsecureRenegotiation on

#   Whether to forbid non-SNI clients to access name based virtual hosts.
#   Default: Off
#SSLStrictSNIVHostCheck On

# Warning: Session Tickets require regular restarting of the server!
# Make sure you do this (e.g. via logrotate) before changing this setting!
SSLSessionTickets off

SSLCertificateFile /etc/ssl/certs/secu.sio-exupery.fr.crt
SSLCertificateKeyFile /etc/ssl/private/web.key
```

Je vérifie le contenu du fichier **ports.conf** afin de s'assurer qu'après avoir activé le module SSL, le service Apache écoute également sur le port 443

```
root@DS2: ~#cat /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
root@DS2: ~#
```

Je modifie le contenu du fichier **sites-sio.conf** pour les hôtes virtuels

```
 GNU nano 8.4                                    /etc/apache2/sites-enabled/sites-sio.conf
<VirtualHost 192.168.2.9:443>

        ServerName secu.sio-exupery.fr:443
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/secu
        ErrorLog /var/www/html/secu/logs/error.log
        CustomLog /var/www/html/secu/logs/access.log combined
        SSLEngine on
        LogLevel info

</VirtualHost>
```

Je redémarre le service Apache2

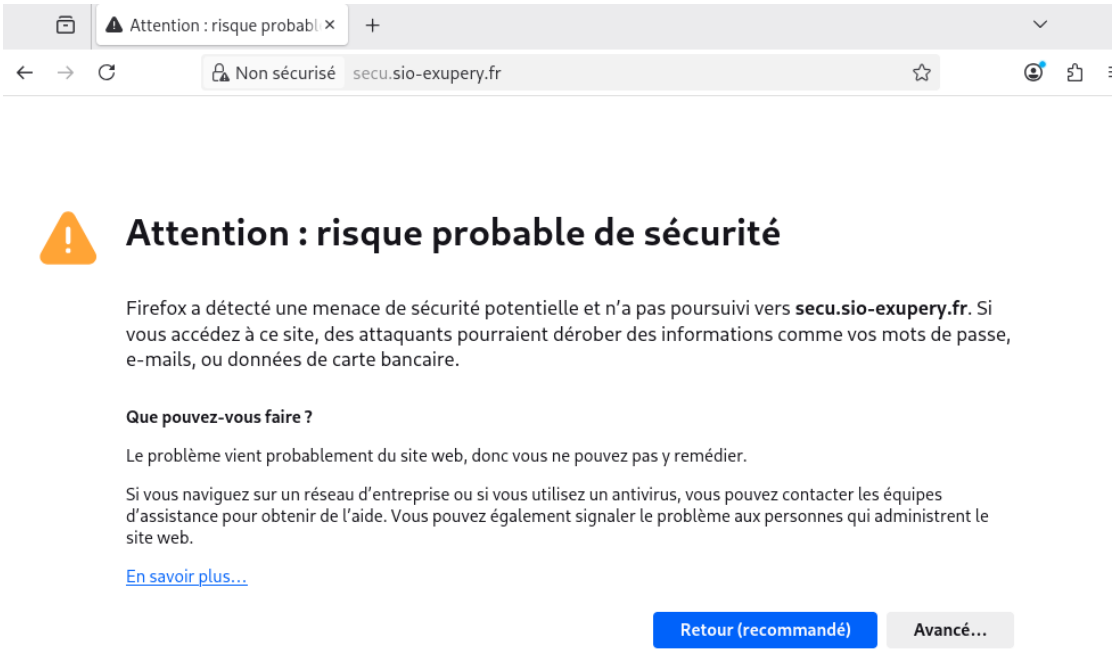
```
root@DS2: ~#systemctl reload apache2
root@DS2: ~#_
```

Je tape la commande ss -lnt pour afficher les connexions TCP

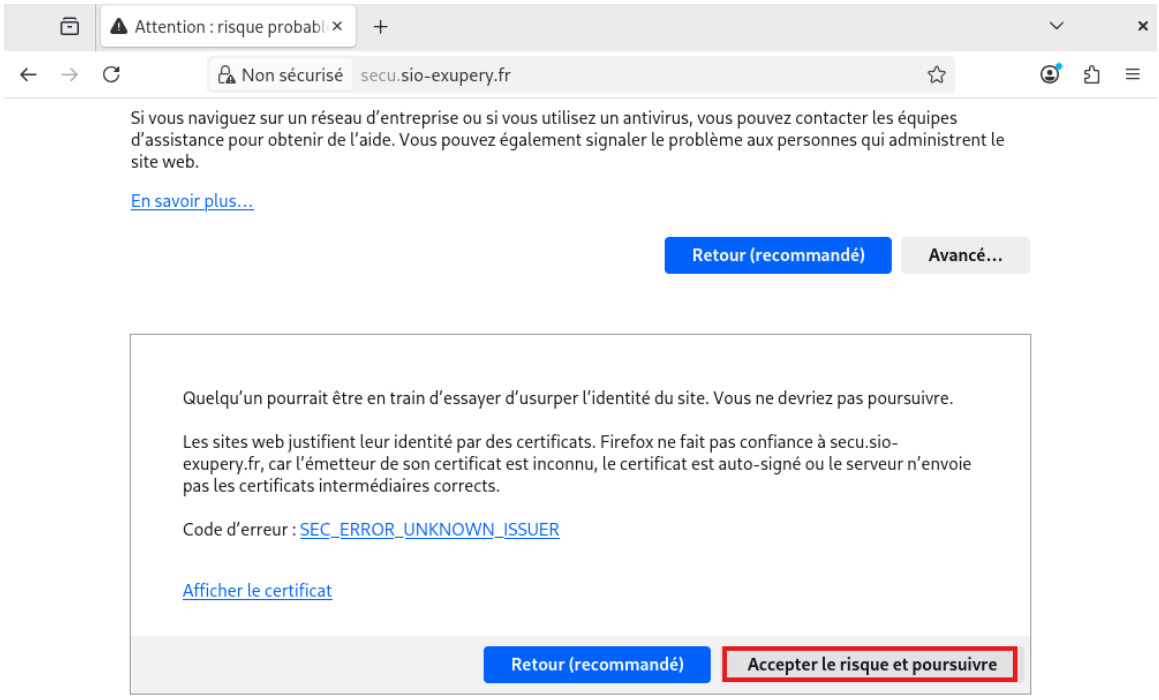
```
root@DS2: ~#ss -lnt
State              Recv-Q             Send-Q                                        Local Address:Port
LISTEN             0                  10                                               127.0.0.1:53
LISTEN             0                  10                                               127.0.0.1:53
LISTEN             0                  128                                                0.0.0.0:22
LISTEN             0                  32                                                 0.0.0.0:21
LISTEN             0                  80                                               127.0.0.1:3306
LISTEN             0                  10                                             192.168.2.1:53
LISTEN             0                  10                                             192.168.2.1:53
LISTEN             0                  5                                                127.0.0.1:953
LISTEN             0                  10                                             192.168.2.9:53
LISTEN             0                  10                                             192.168.2.9:53
LISTEN             0                  511                                                    *:80
LISTEN             0                  128                                                 [::]:22
LISTEN             0                  511                                                    *:443
LISTEN             0                  10                                                  [::1]:53
LISTEN             0                  10                                                  [::1]:53
LISTEN             0                  5                                                   [::1]:953
LISTEN             0                  10                                 [fe80::a00:27ff:fe34:6db]%enp0s3:53
LISTEN             0                  10                                 [fe80::a00:27ff:fe34:6db]%enp0s3:53
root@DS2: ~#
```

3. Test du serveur Web sécurisé depuis un client

Depuis la machine DD1 je tape l'URL https://secu.sio-exupery.fr



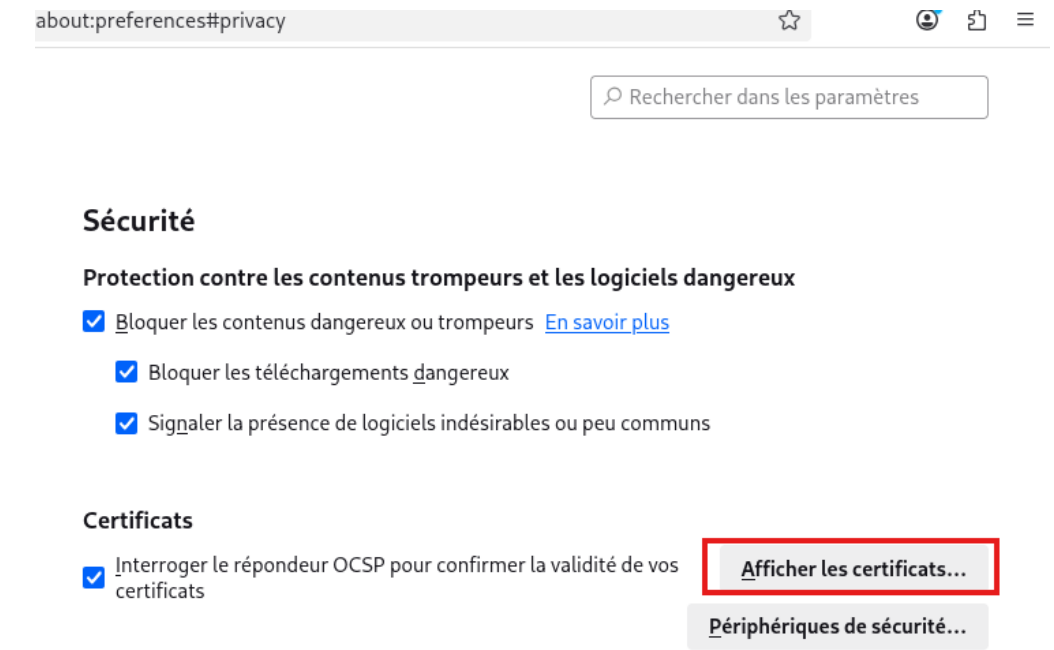
Je clique sur Accepter le risque et continuer

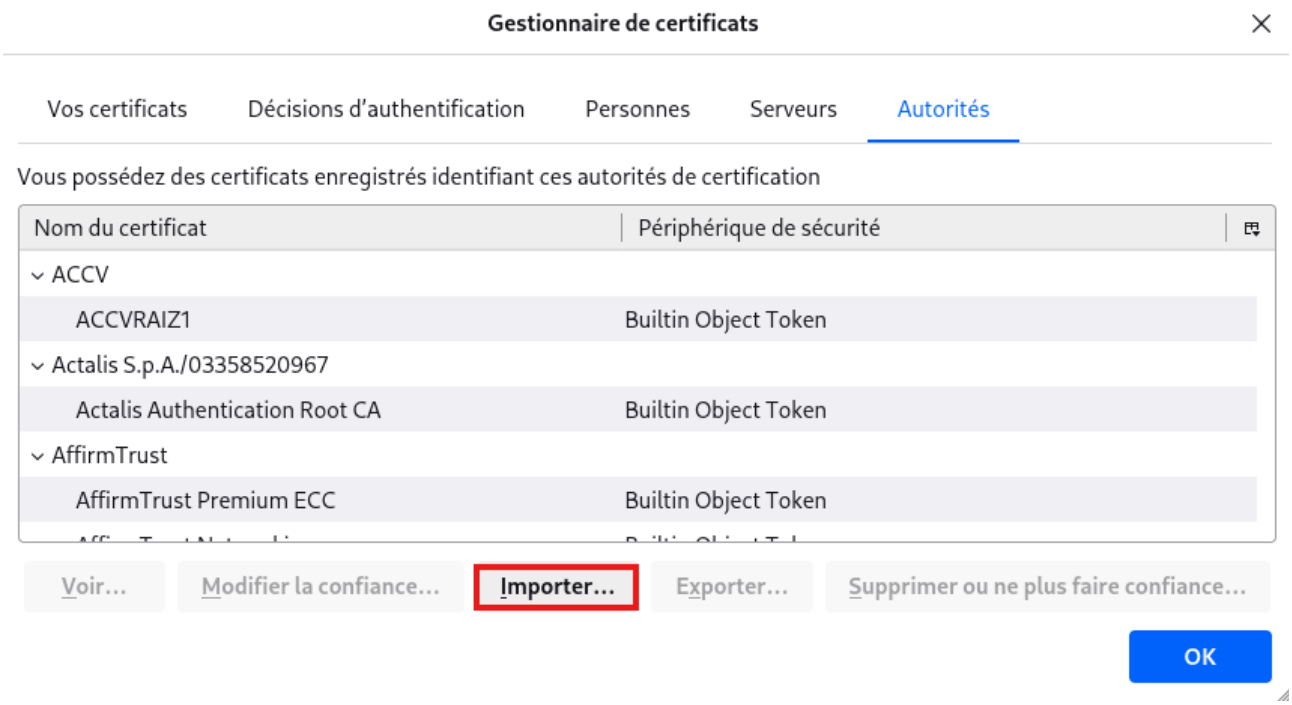


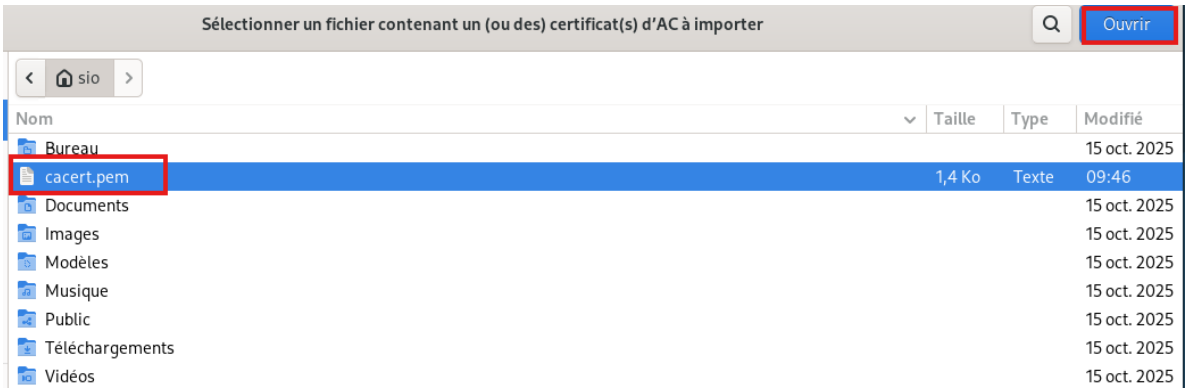
Depuis DD1 je transfert le certificat de l'autorité de certification vers le répertoire personnel de sio

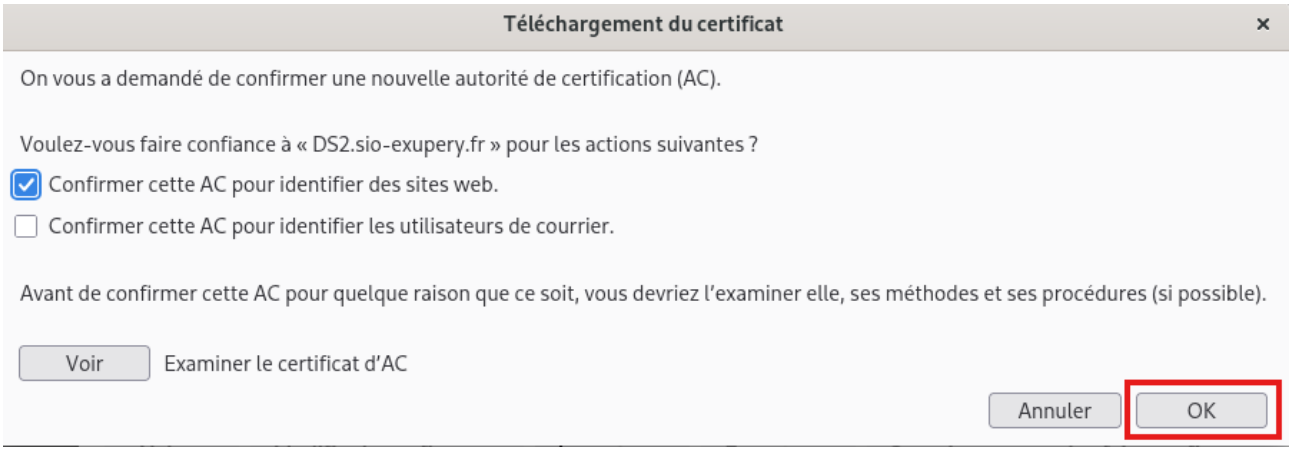
```
root@DEB13Desktop:/home/sio# scp root@192.168.2.1:/etc/ssl/CA/certs/cacert.pem /
home/sio
The authenticity of host '192.168.2.1 (192.168.2.1)' can't be established.
ED25519 key fingerprint is SHA256:198ZO5rPJQ7Q9769ZdKu/GI5yS8VnBsOMfL//5BObkE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.1' (ED25519) to the list of known hosts.
root@192.168.2.1's password:
cacert.pem                                    100% 1391   787.0KB/s   00:00
root@DEB13Desktop:/home/sio# ls
Bureau      fichier2.txt  Modèles  Téléchargements
cacert.pem  fichier.txt   Musique  testanonymous.txt
Documents   Images        Public   Vidéos
root@DEB13Desktop:/home/sio#
root@DEB13Desktop:/home/sio#
```

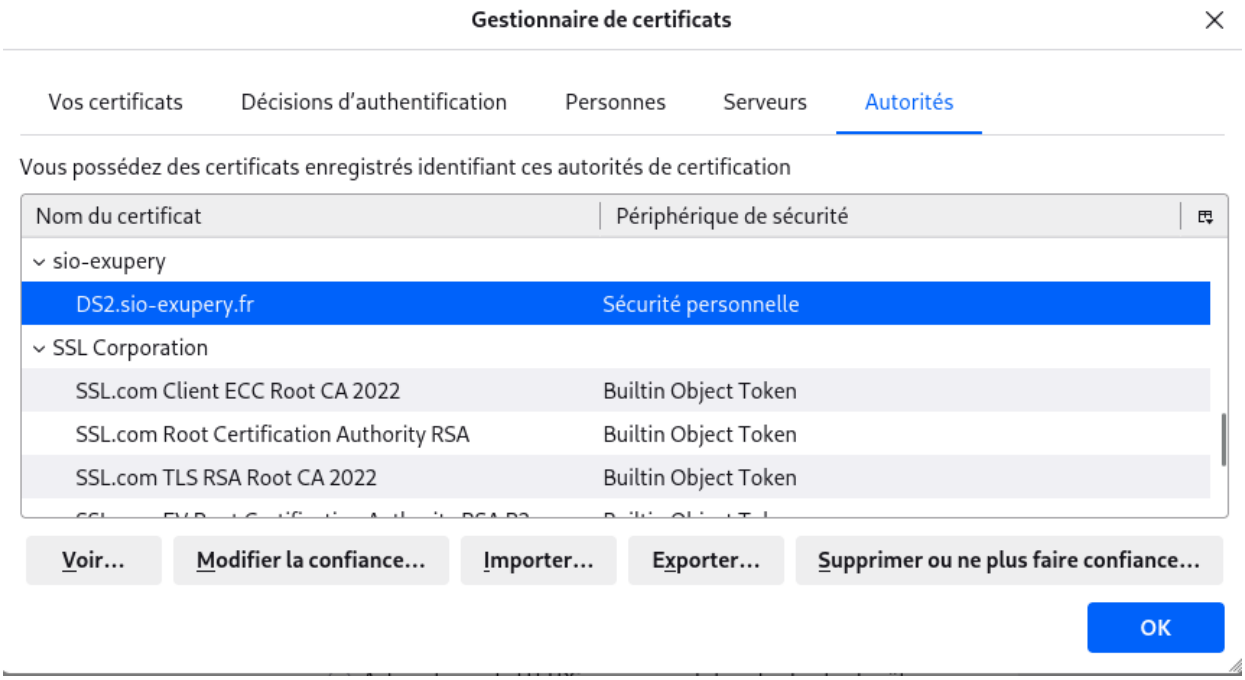
J'importe le certificat dans le magasin de certificats depuis le navigateur Firefox




Gestionnaire de certificats
Vos certificats
Décisions d'authentification
Personnes
Serveurs
Autorités
Vous possédez des certificats enregistrés identifiant ces autorités de certification
Nom du certificat
Périphérique de sécurité
ACCV
ACCVRAIZ1
Builtin Object Token
Actalis S.p.A./03358520967
Actalis Authentication Root CA
Builtin Object Token
AffirmTrust
AffirmTrust Premium ECC
Builtin Object Token
Voir...
Modifier la confiance...
Importer...
Exporter...
Supprimer ou ne plus faire confiance...
OK


Sélectionner un fichier contenant un (ou des) certificat(s) d'AC à importer
Ouvrir
sio
Nom
Taille
Type
Modifié
Bureau
15 oct. 2025
cacert.pem
1,4 Ko
Texte
09:46
Documents
15 oct. 2025
Images
15 oct. 2025
Modèles
15 oct. 2025
Musique
15 oct. 2025
Public
15 oct. 2025
Téléchargements
15 oct. 2025
Vidéos
15 oct. 2025


Téléchargement du certificat
On vous a demandé de confirmer une nouvelle autorité de certification (AC).
Voulez-vous faire confiance à « DS2.sio-exupery.fr » pour les actions suivantes ?
Confirmer cette AC pour identifier des sites web.
Confirmer cette AC pour identifier les utilisateurs de courrier.
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).
Voir
Examiner le certificat d'AC
Annuler
OK


Gestionnaire de certificats
Vos certificats
Décisions d'authentification
Personnes
Serveurs
Autorités
Vous possédez des certificats enregistrés identifiant ces autorités de certification
Nom du certificat
Périphérique de sécurité
sio-exupery
DS2.sio-exupery.fr
Sécurité personnelle
SSL Corporation
SSL.com Client ECC Root CA 2022
Builtin Object Token
SSL.com Root Certification Authority RSA
Builtin Object Token
SSL.com TLS RSA Root CA 2022
Builtin Object Token
Voir...
Modifier la confiance...
Importer...
Exporter...
Supprimer ou ne plus faire confiance...
OK

Je re consulte la page https://secu.sio-exupery.fr et le site est bien sécurisé avec le cadenas