Documentation on Securing a networked system with Public Key Infrastructure in Windows Server 2012 R2

Developed By

Md Ariful Islam (2019-1-60-140)

Syeda Tasfia Tasnim (2019-1-60-137)

Rawnak Jahan Taifa (2019-1-60-134)

Submitted To

Rashedul Amin Tuhin

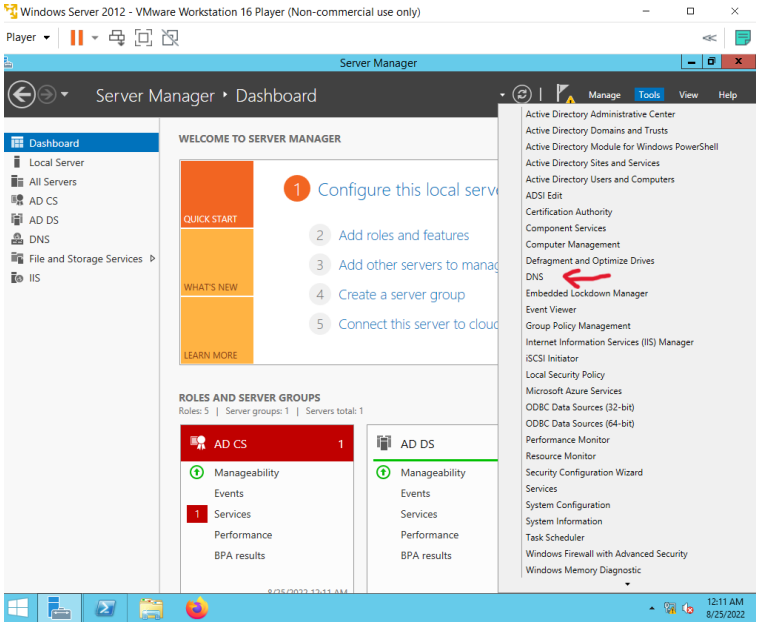
Senior Lecturer

Department of Computer Science and Engineering

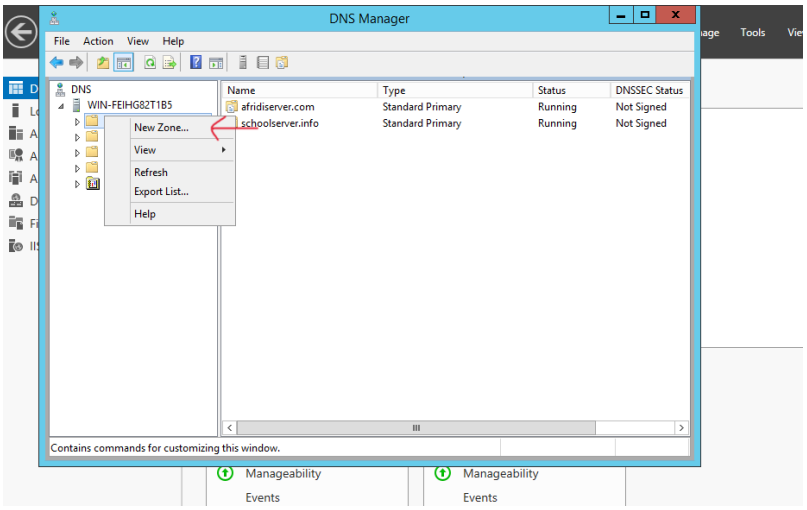
East West University

DNS Configuration

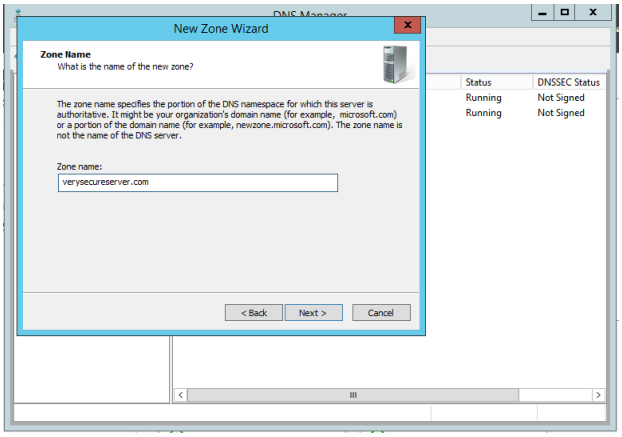
- **Open Windows Server → ‘**
- **Go to DNS**



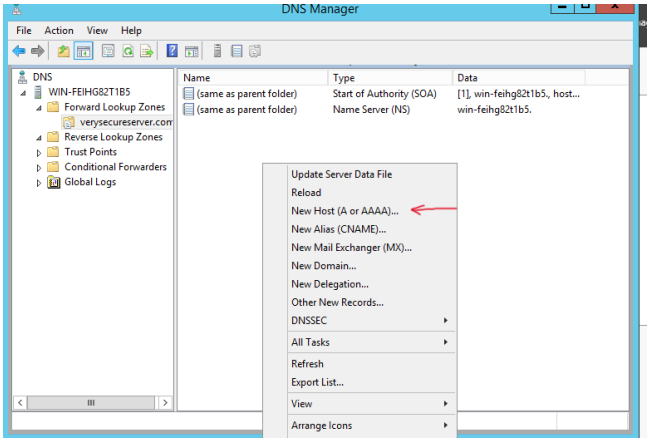
- **Create New Zone in Forward lookup zone**

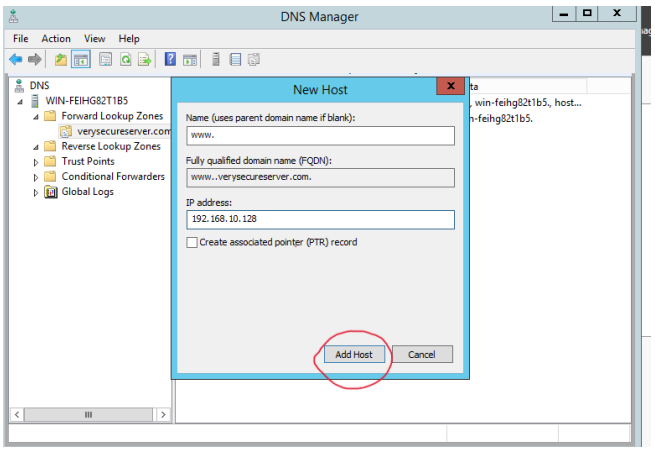


- **Enter server name and click next →**

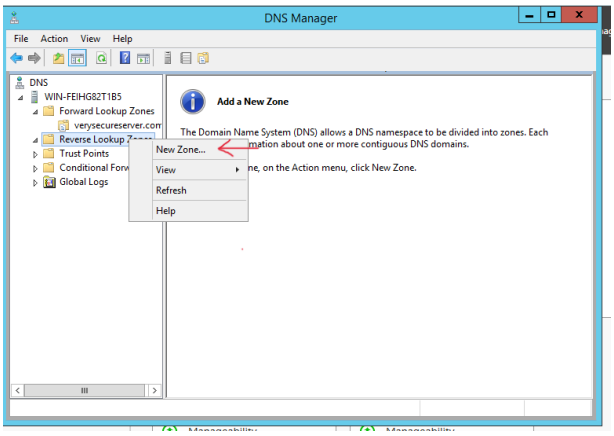


- **Create a new host under server zone**

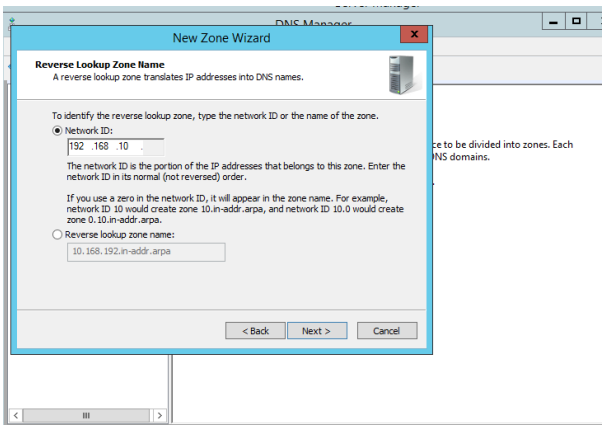




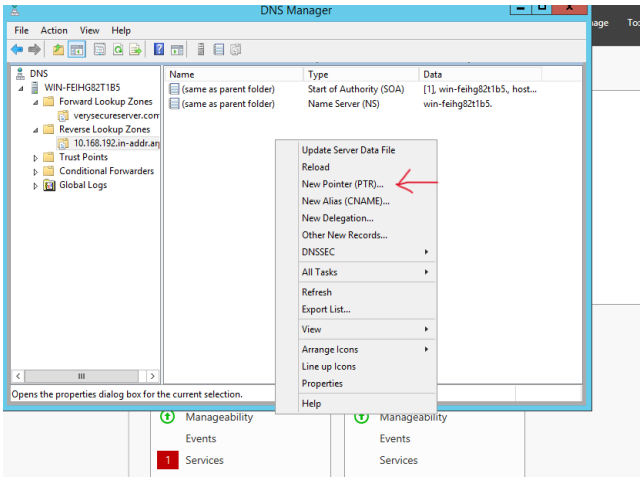
- **Create a new zone in the Reverse lookup zone**

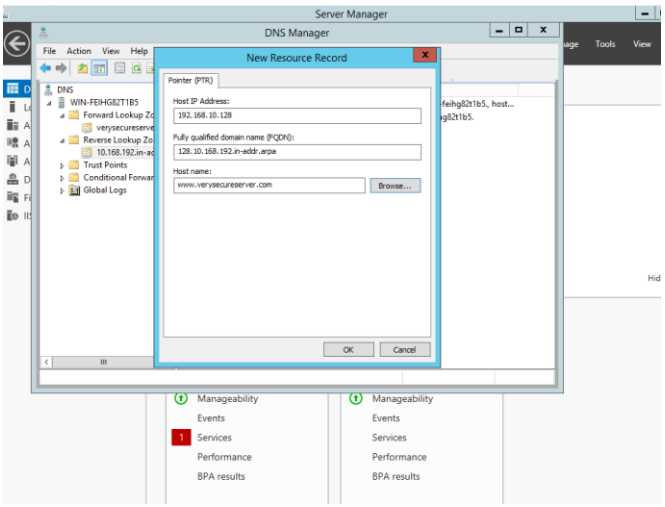


- **In network id enter the first 3 octaves of IP address**

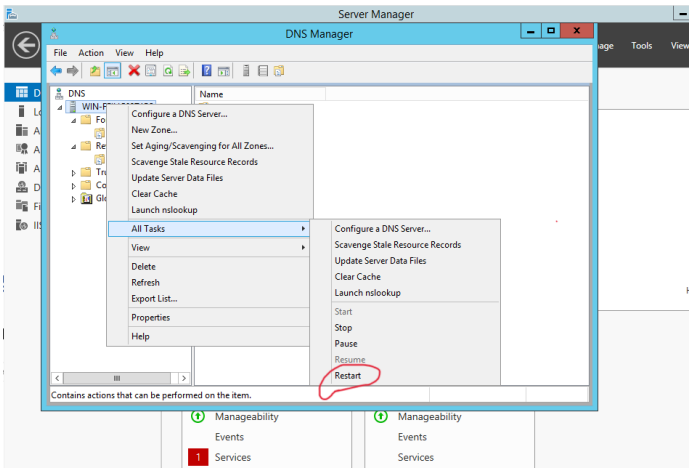


- **Create a new Pointer Under Reverse lookup zone**

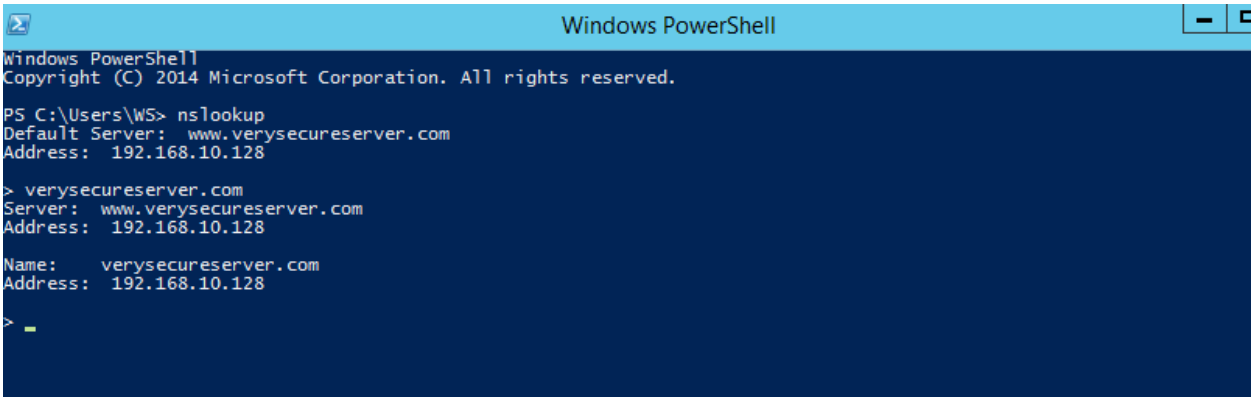




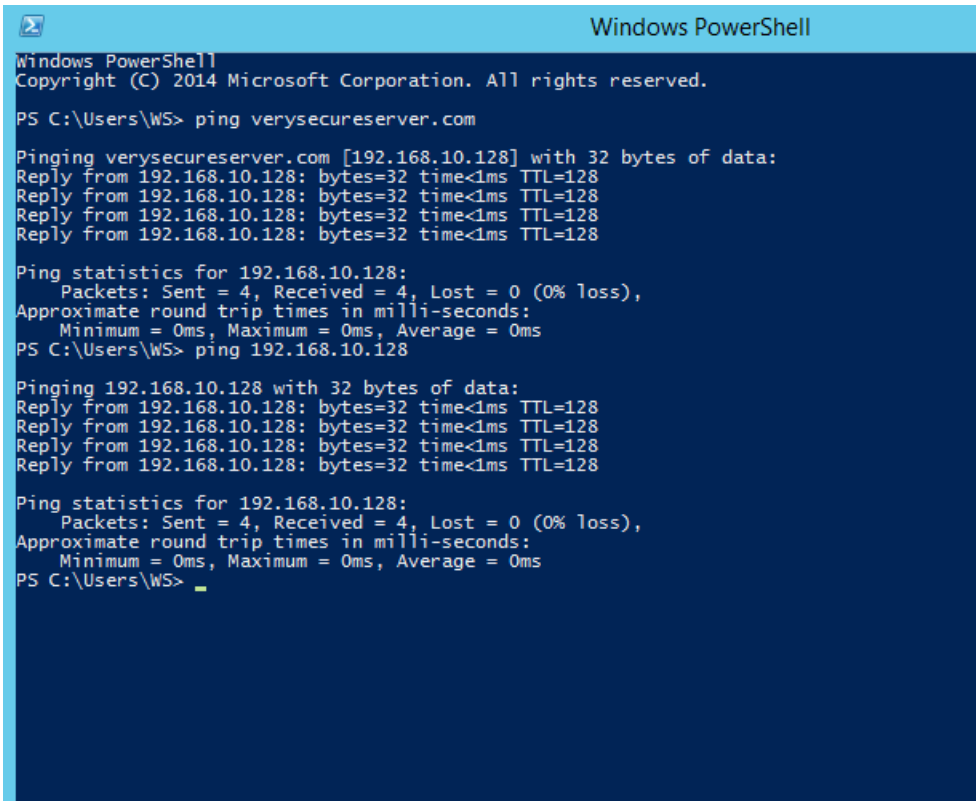
- **Restart the DNS Manager**



- **Check the server configuration from nslookup**



- **Check server communication right by ping the network**

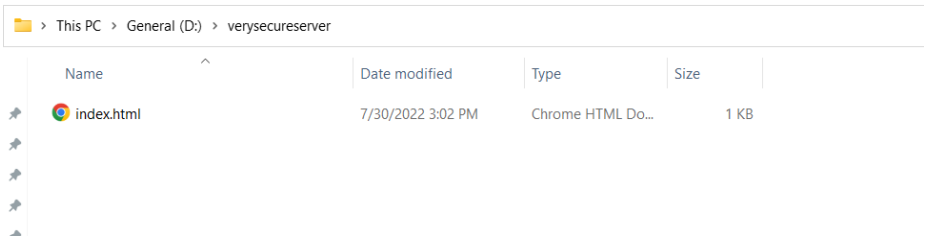


Important Notes:

- Static Ip is always preferable for launching a server
- For client access all the networks should be in the same local area network
- In client PC, DNS configuration should be manual and follow up the exact server DNS address.

SSL Configuration

- **Create a File Uploading HTML file. Save it into VerySecureServer Folder.**

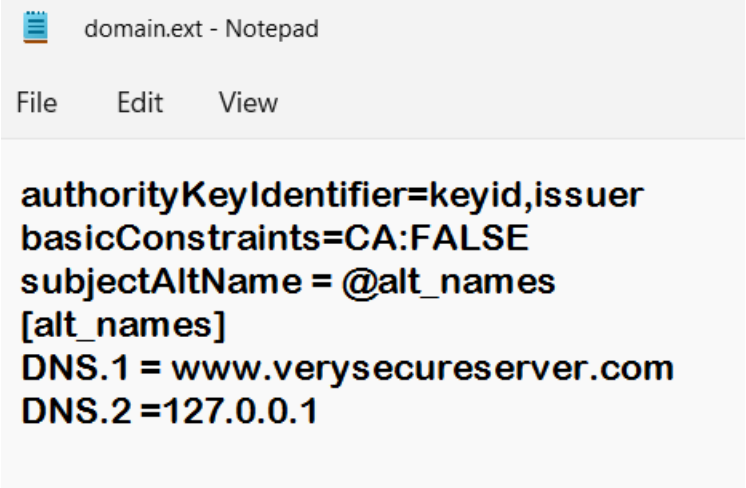


- **Go To *C:\xampp\apache\conf***

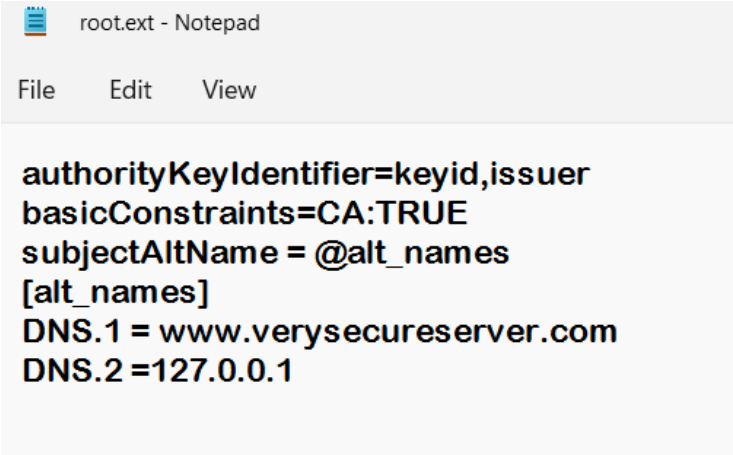
- **Edit httpd.conf file**
  DocumentRoot "D:/verysecureserver" [Location of the webpage]
  <Directory "D:/verysecureserver">
-
- **Go To *C:\xampp\apache\bin***

- **Create domain.ext and root.ext file.**

- **In domain.ext add,**



- **In root.ext add,**



- **Go To *C:\xampp\apache\conf\extra***

- **Edit file httpd-vhosts.conf**

```
<VirtualHost  *:443>
    DocumentRoot D:\verysecureserver
    ServerName verysecureserver.com
    ServerAlias www.verysecureserver.com
</VirtualHost>
```

- **Run cmd as Administrator**

- **Use command →**
  set OPENSSL_CONF=C:\xampp\apache\conf\openssl.cnf **to set openssl environment path.**

- **Go To *C:\xampp\apache\bin***

- ***Run openssl.exe***

```
C:\xampp\apache\bin>openssl.exe
OpenSSL>
```

- **Creating a Root Certificate with following command**
  req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt

```
-----
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]:BD
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EWU
Organizational Unit Name (eg, section) []:DCSE
Common Name (e.g. server FQDN or YOUR name) []:AcmeRootCA
Email Address []:arif@gmail.com
OpenSSL>
```

- **Creating a Sub Root certificate with the following Command →**
  req -newkey rsa:2048 -keyout subrootCA.key -out subrootCA.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]:BD
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EWU
Organizational Unit Name (eg, section) []:DCSE
Common Name (e.g. server FQDN or YOUR name) []:AcmeCA
Email Address []:arif@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:arif
An optional company name []:arif
OpenSSL>
```

- **Create a new Server Certificate With the Command →**
  req -newkey rsa:2048 -nodes -keyout server.key -out server.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]:BD
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EWU
Organizational Unit Name (eg, section) []:DCSE
Common Name (e.g. server FQDN or YOUR name) []:verysecureserver.com
Email Address []:arif@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:arif
An optional company name []:arif
OpenSSL>
```

- **Signing subrootCA certificate with rootCA certificate with following command**
  x509 -req -CA rootCA.crt -CAkey rootCA.key -in subrootCA.csr -out subrootCA.crt -days 365 -CAcreateserial -extfile root.ext

- **Exporting the subrootCA key file in subrootCA pfx file with following command**
  pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx

```
OpenSSL> pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx
Enter pass phrase for subrootCA.key:
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

- **Signing server certificate with subrootCA certificate with following command →**
  x509 -req -CA subrootCA.crt -CAkey subrootCA.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile domain.ext

- **Exporting the server key file in the server .pfx file with following command→**
  pkcs12 -inkey server.key -in server.crt -export -out server.pfx

```
OpenSSL> pkcs12 -inkey server.key -in server.crt -export -out server.pfx
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

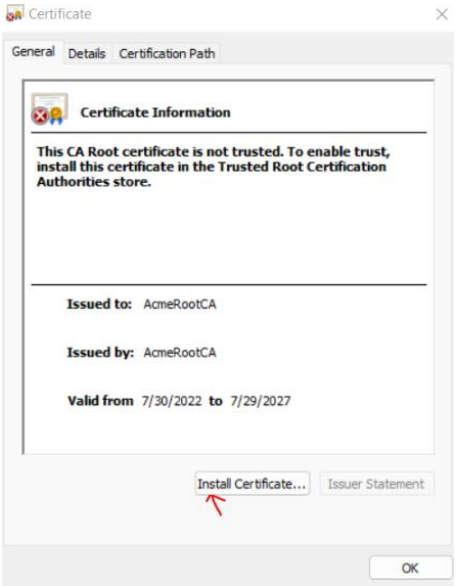
- **Replacing the RSA encryption from the server and subrootCA key for setting the validity with commands**
  - *rsa -in server.key -out server.key*
  - *rsa -in subrootCA.key -out subrootCA.key*

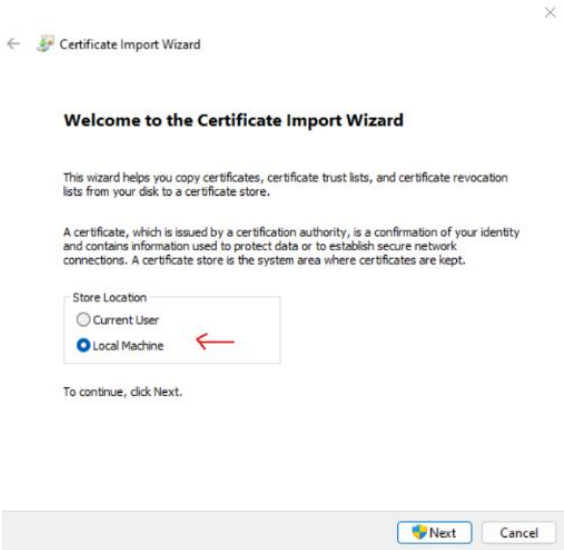
```
OpenSSL> rsa -in server.key -out server.key
writing RSA key
OpenSSL> rsa -in subrootCA.key -out subrootCA.key
Enter pass phrase for subrootCA.key:
writing RSA key
OpenSSL>
```

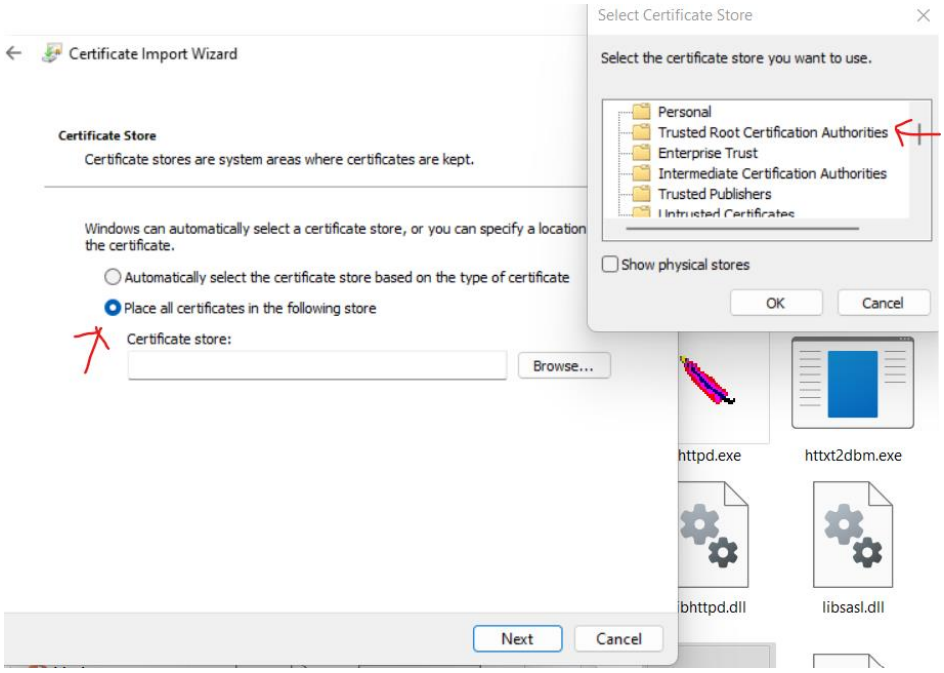
n

Install Certificate Manually

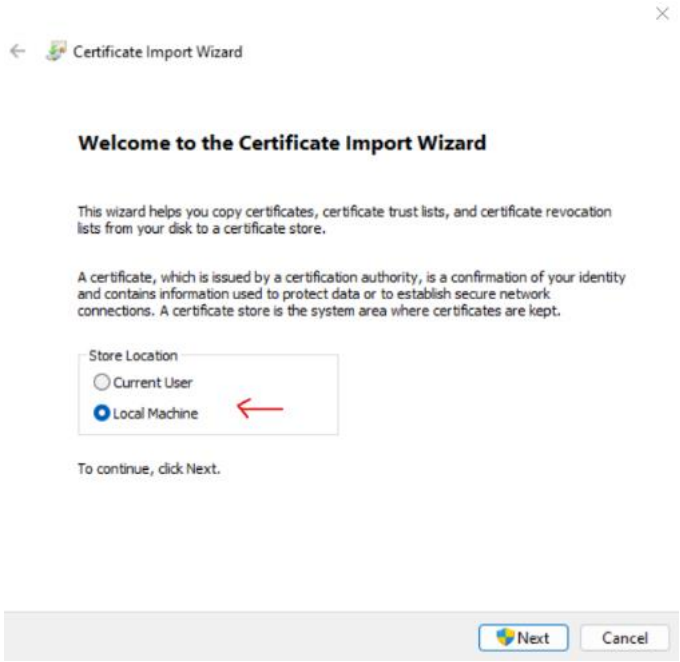
- **Go To *C:\xampp\apache\bin***
  - **Select rootCA.crt**







- **Select subrootCa.pfx**



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\xampp\apache\bin\subrootCA.pfx

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next Cancel

Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••

Display Password

Import options:

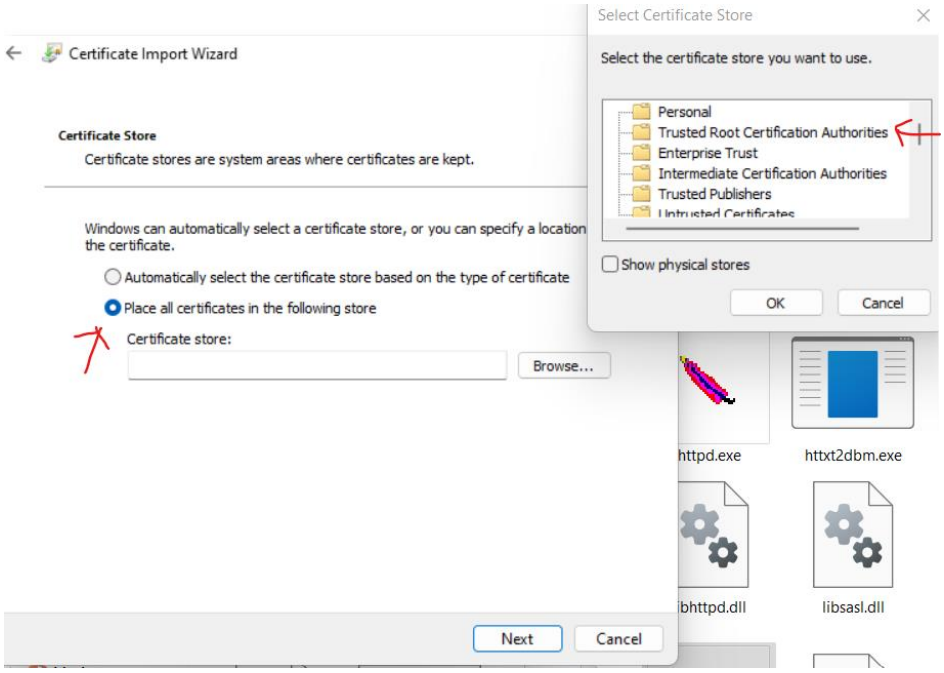
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Protect private key using virtualized-based security(Non-exportable)

Include all extended properties.

Next Cancel



- **Copy the server.crt, server.csr, & server.key and replace it with *C:\xampp\apache\conf\ssl.crt\server.crt, C:\xampp\apache\conf\ssl.csr\server.csr, & C:\xampp\apache\conf\ssl.key\server.key***

- **Go To *C:\xampp\apache\conf\extra***

- **Add SSL conf on httpd-vhosts.conf**

```
<VirtualHost  *:443>
    DocumentRoot D:\verysecureserver
    ServerName verysecureserver.com
    ServerAlias www.verysecureserver.com
    SSLEngine  on
    SSLCertificateFile "conf/ssl.crt/server.crt"
    SSLCertificateKeyFile "conf/ssl.key/server.key"

</VirtualHost>
```

- **Check the SSL key on a browser by running https://www.verysecureserver.com**