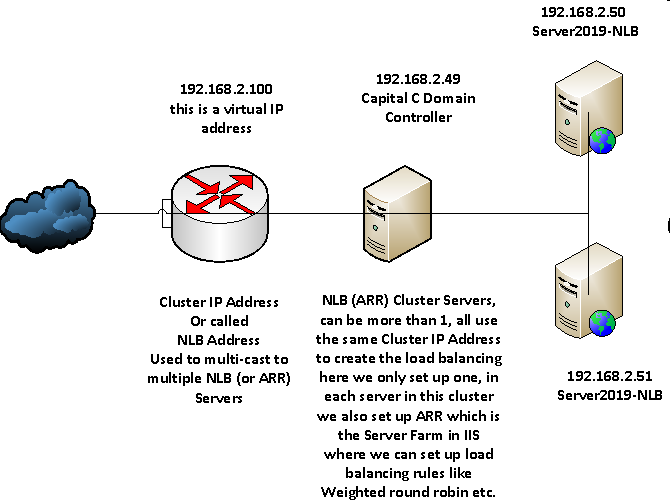
Capital C Site Network Load Balancing and ARR configuration

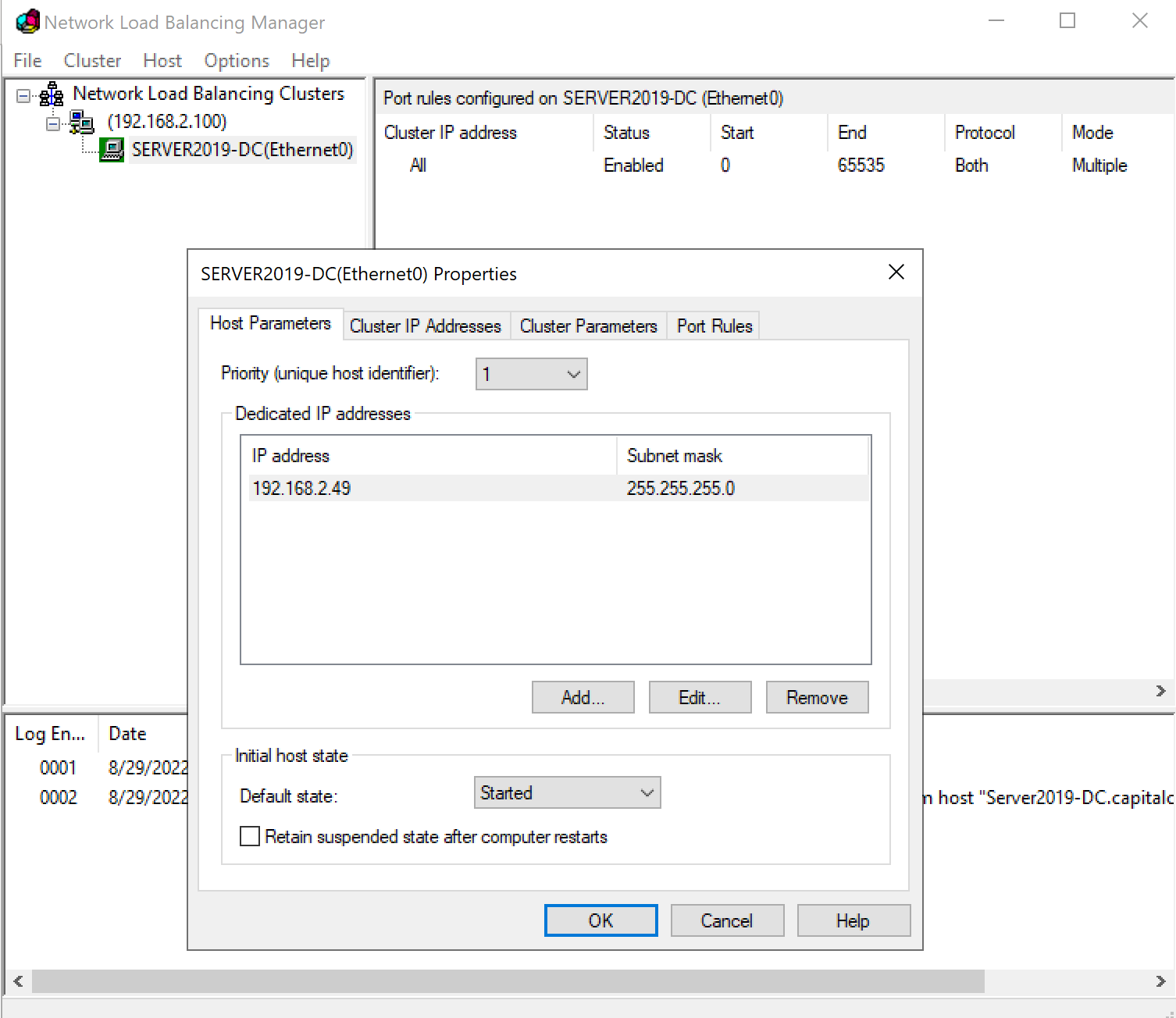
# Architecture

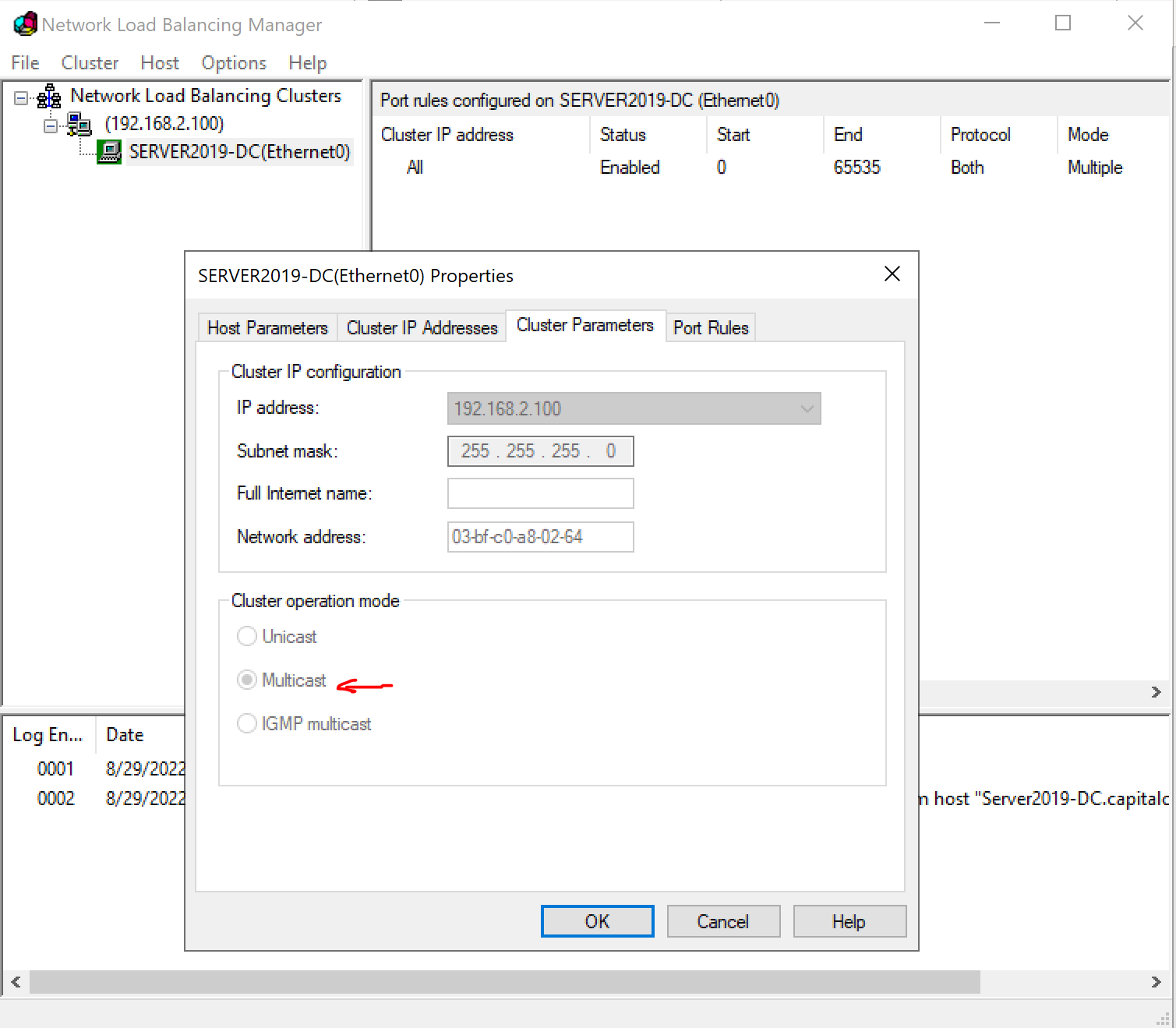


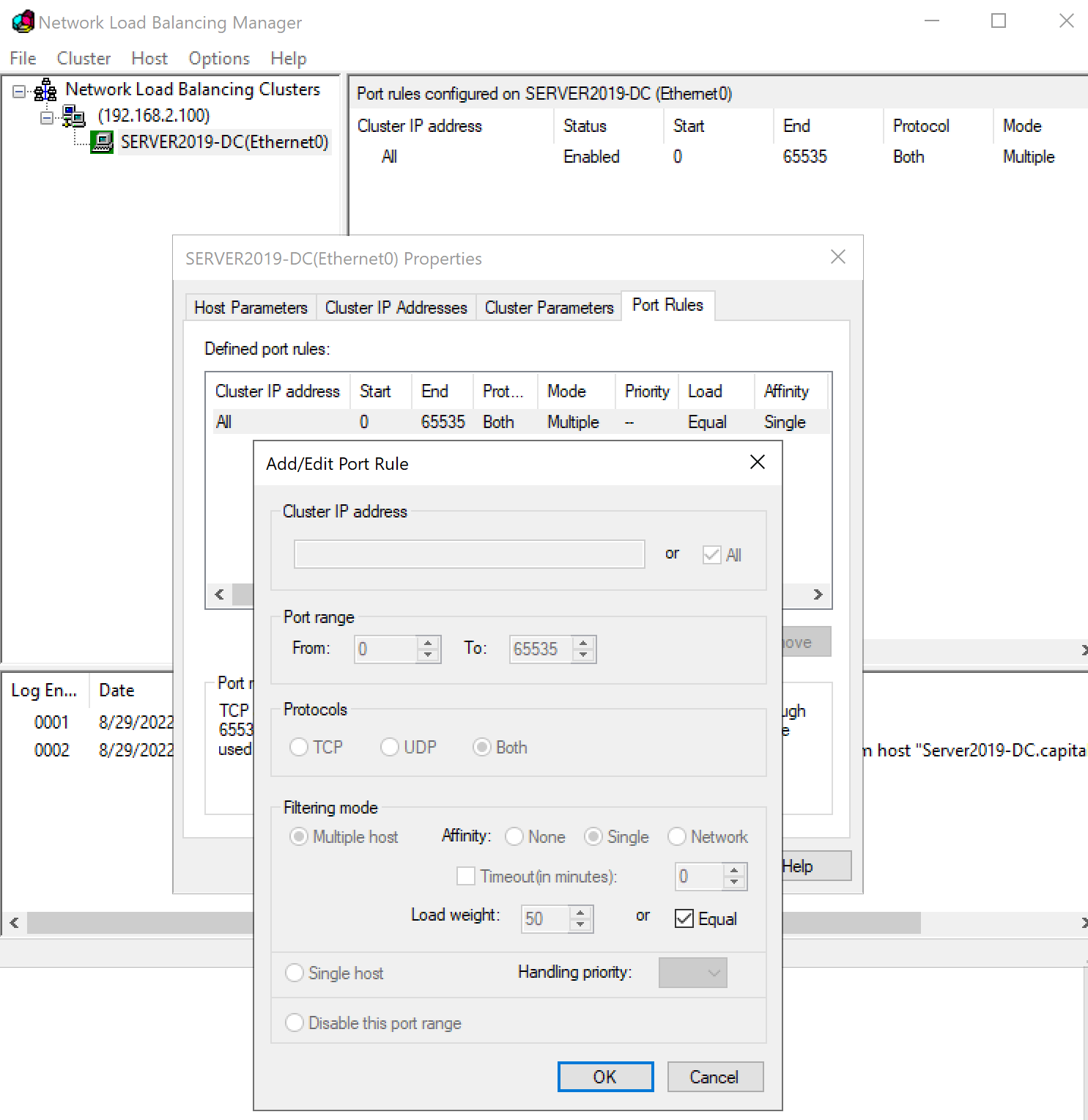
# NLB Configuration

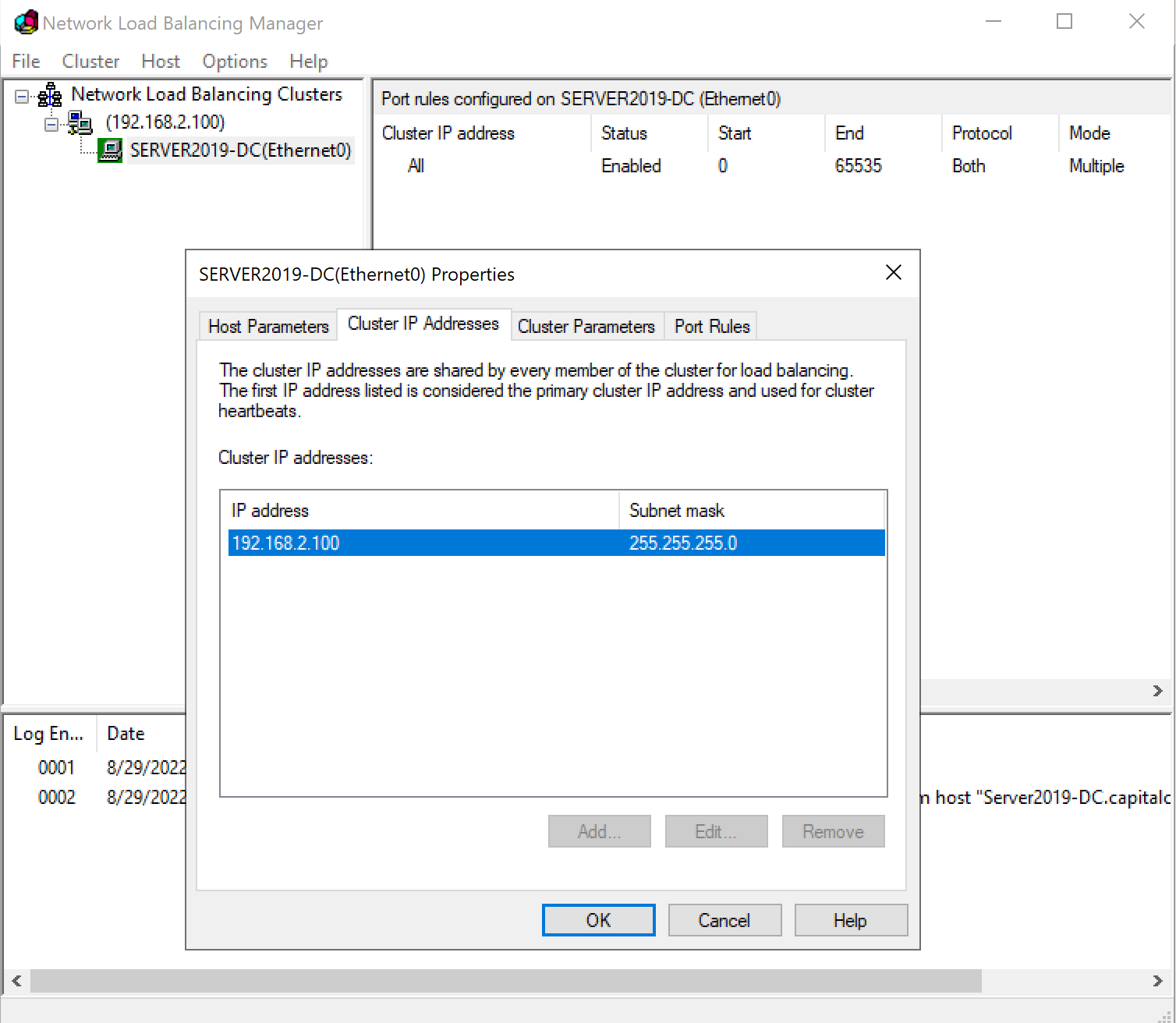
Mainly in Capital C Domain Controller:

* Add Roles and Features 🡪 Network Load Balancing
* Network Loading Balancing Manager 🡪 Add Cluster
* If just use NLB, you can add multiple Cluster IP addresses and each one serves as a load balancing web server; you can also add multiple Cluster IP addresses and each one serves as an ARR server (Application Request Routing)



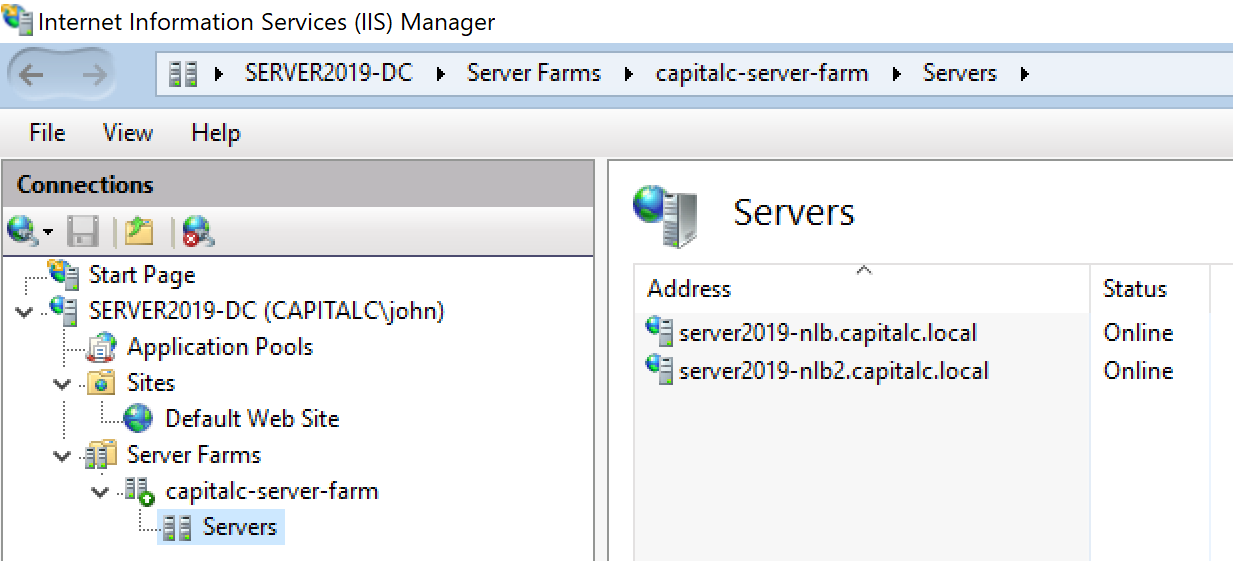




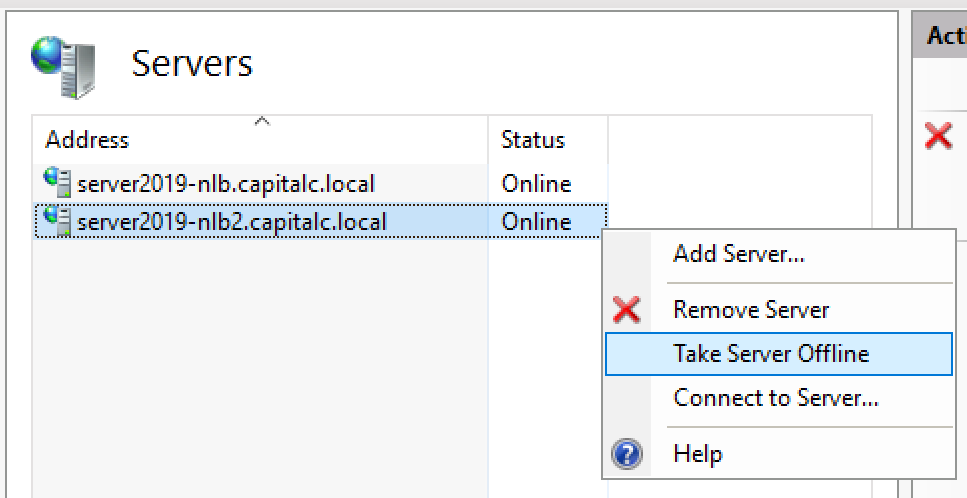


# ARR (Application Request Routing) Configuration

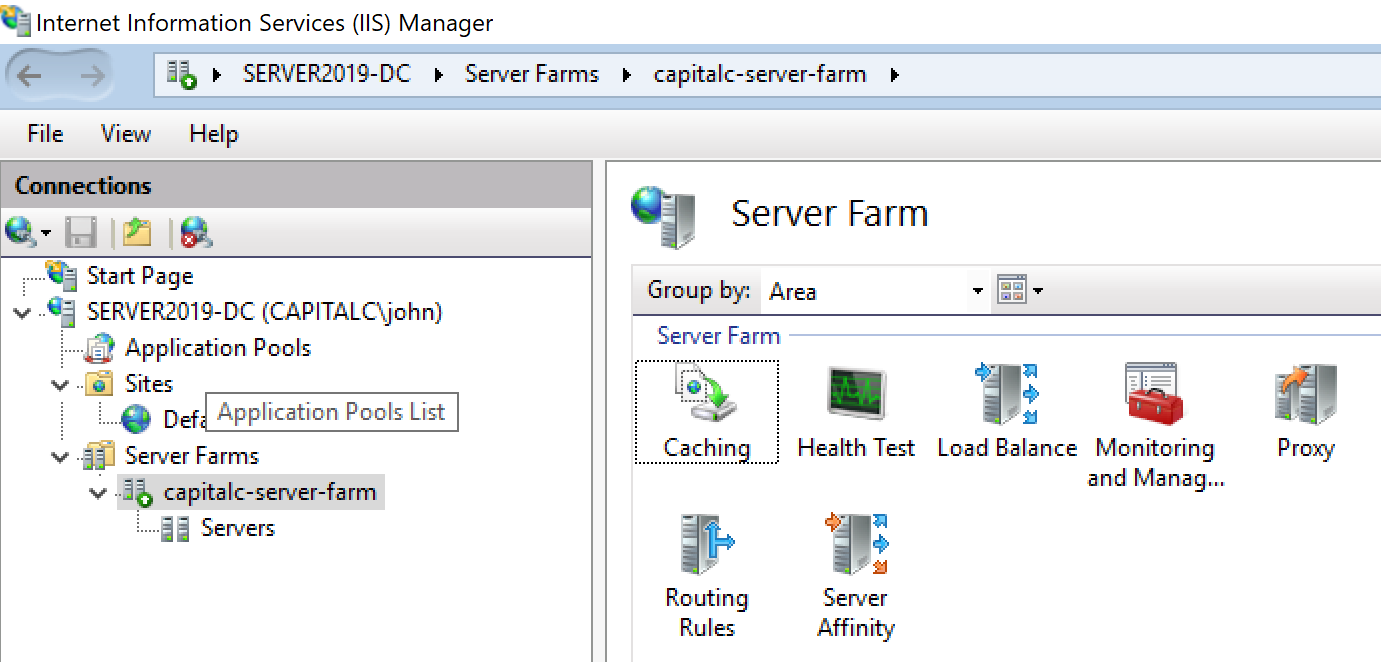
* Launch the Web Platform Installer, and do a search for URL > Select URL Rewrite > Add > Repeat the process, searching for ARR, and add Application Request Routing version 3, (Not the 2.5 version at the top!) > Next > Follow the wizard and complete the install.
* Open Internet Information Services (IIS) Manager 🡪 Server Farms 🡪 Create Server Farms 🡪 Add 2 Load Balancing and Fail Over web servers



You can manage Fail Over by taking server online/offline

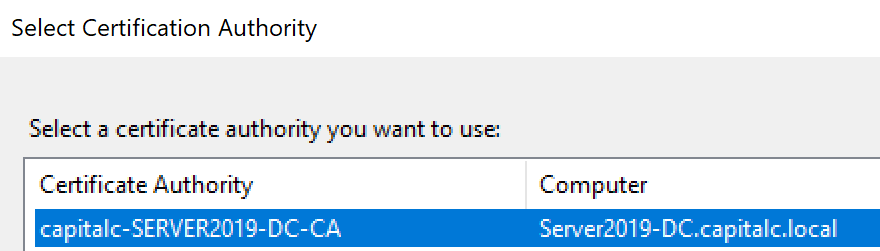


You can also manage the Load Balancing and Routing Rules

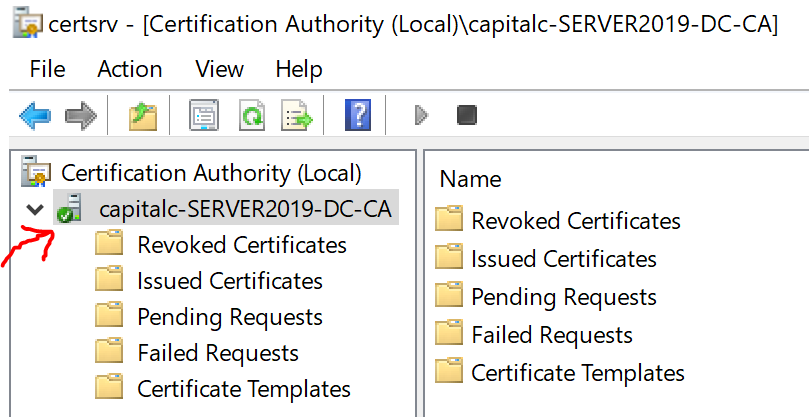


# Install SSL

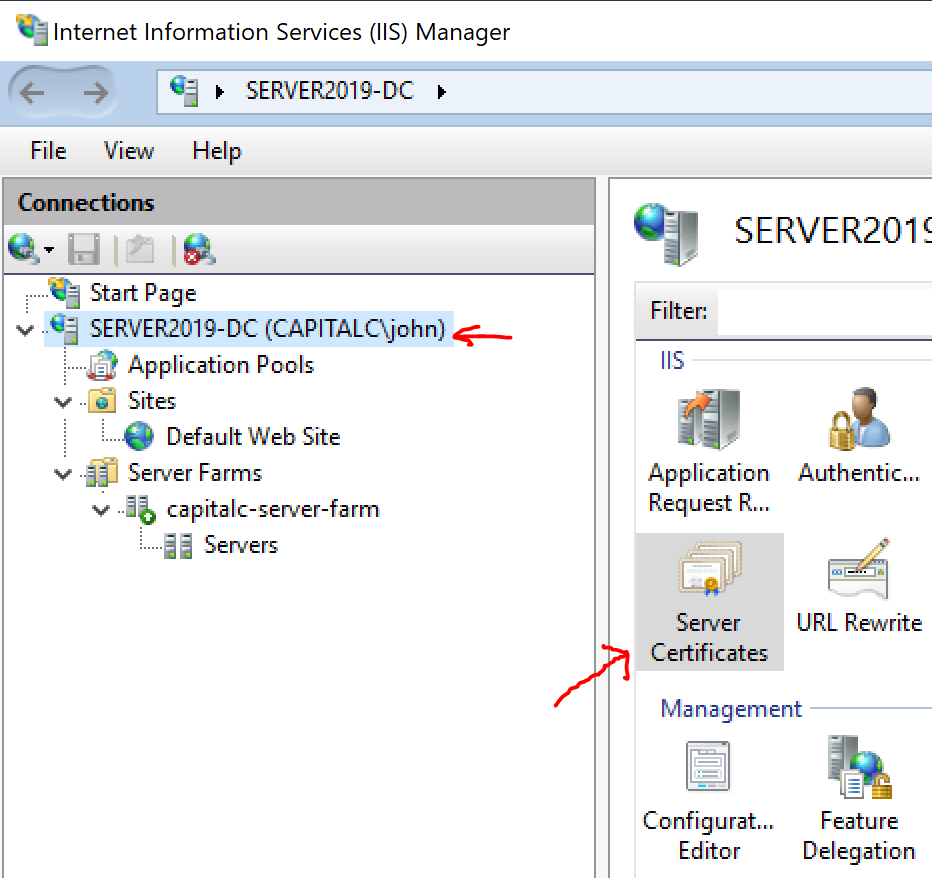
* Certificate Authority works like a tree, to set up the local Domain Certificate we need to create the root Domain Certificate first.
* Domain Certificate Authority

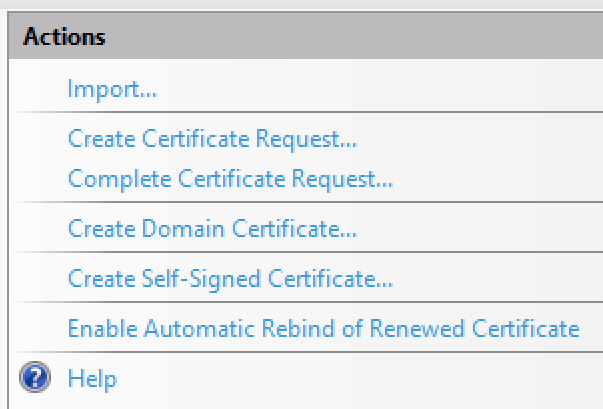


Domain Certificate Authority use its own certificate private key to sign incoming new certificate request issued by the Domain CA.



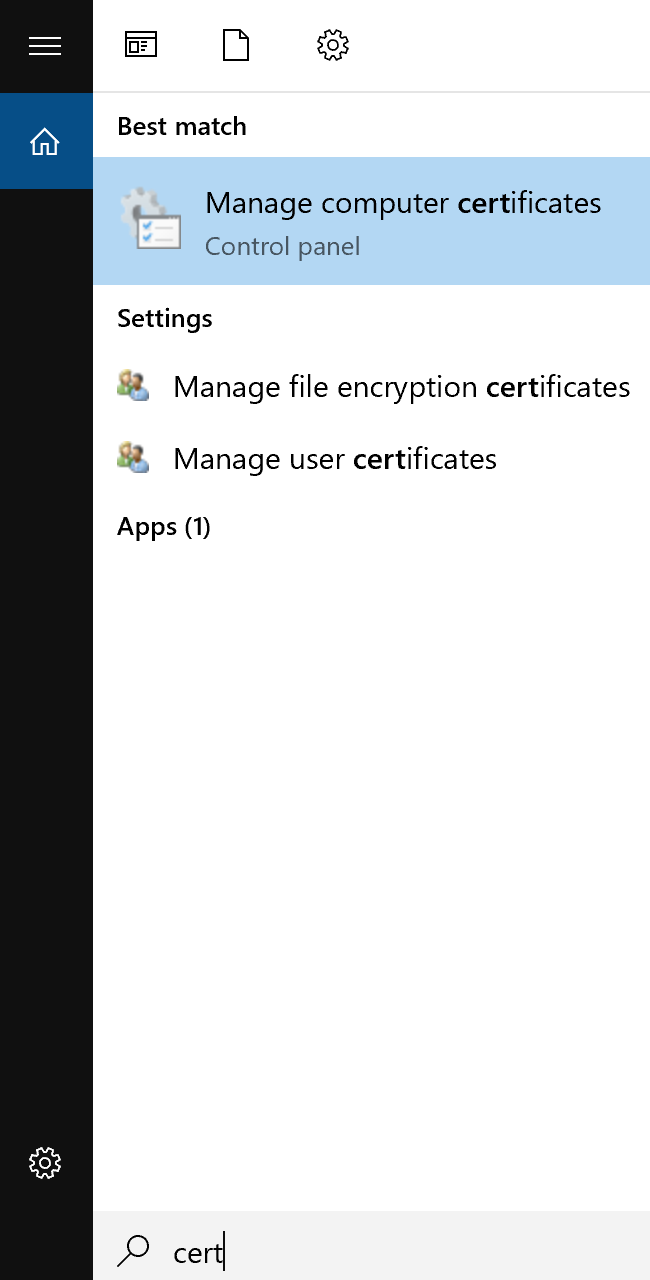
* Certificate Request can be generated by Internet Information Server (IIS) Manager 🡪 Server 🡪 Server Certificates, but this does not work with Microsoft’s Domain CA due to formatting issue.

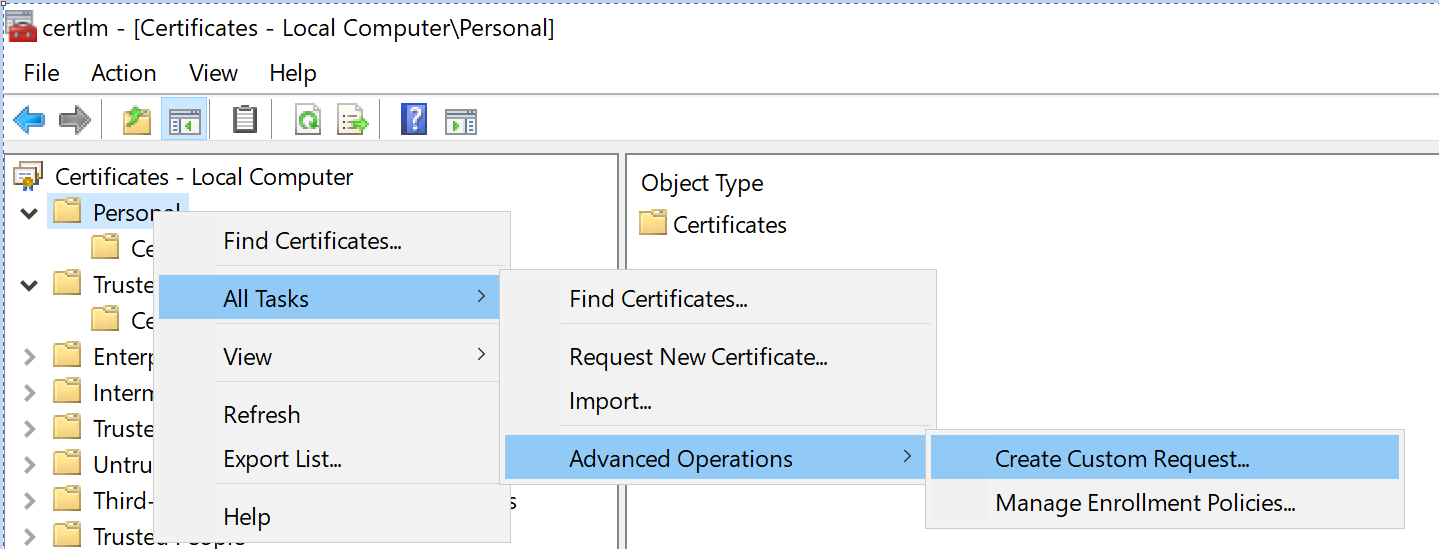


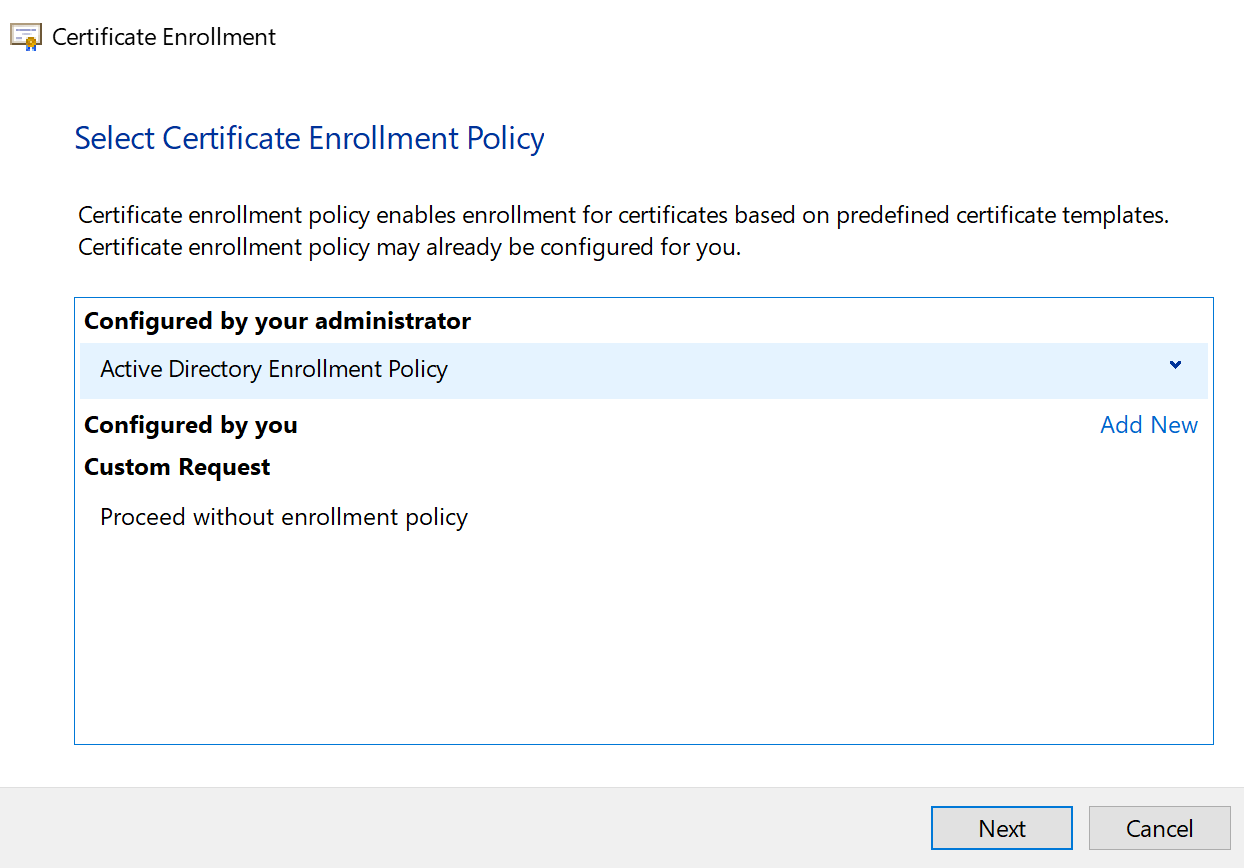


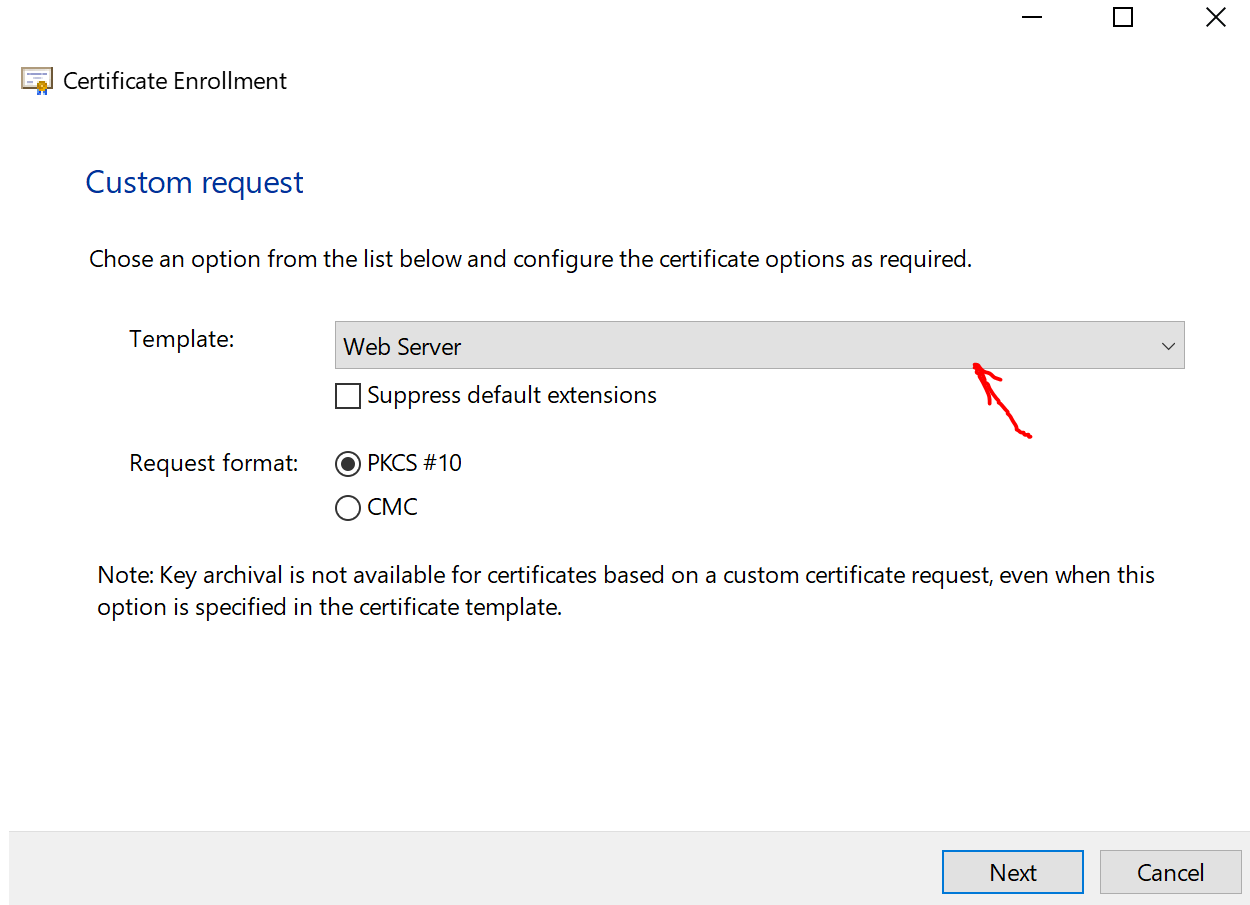
* Create a Web Server Certificate Request

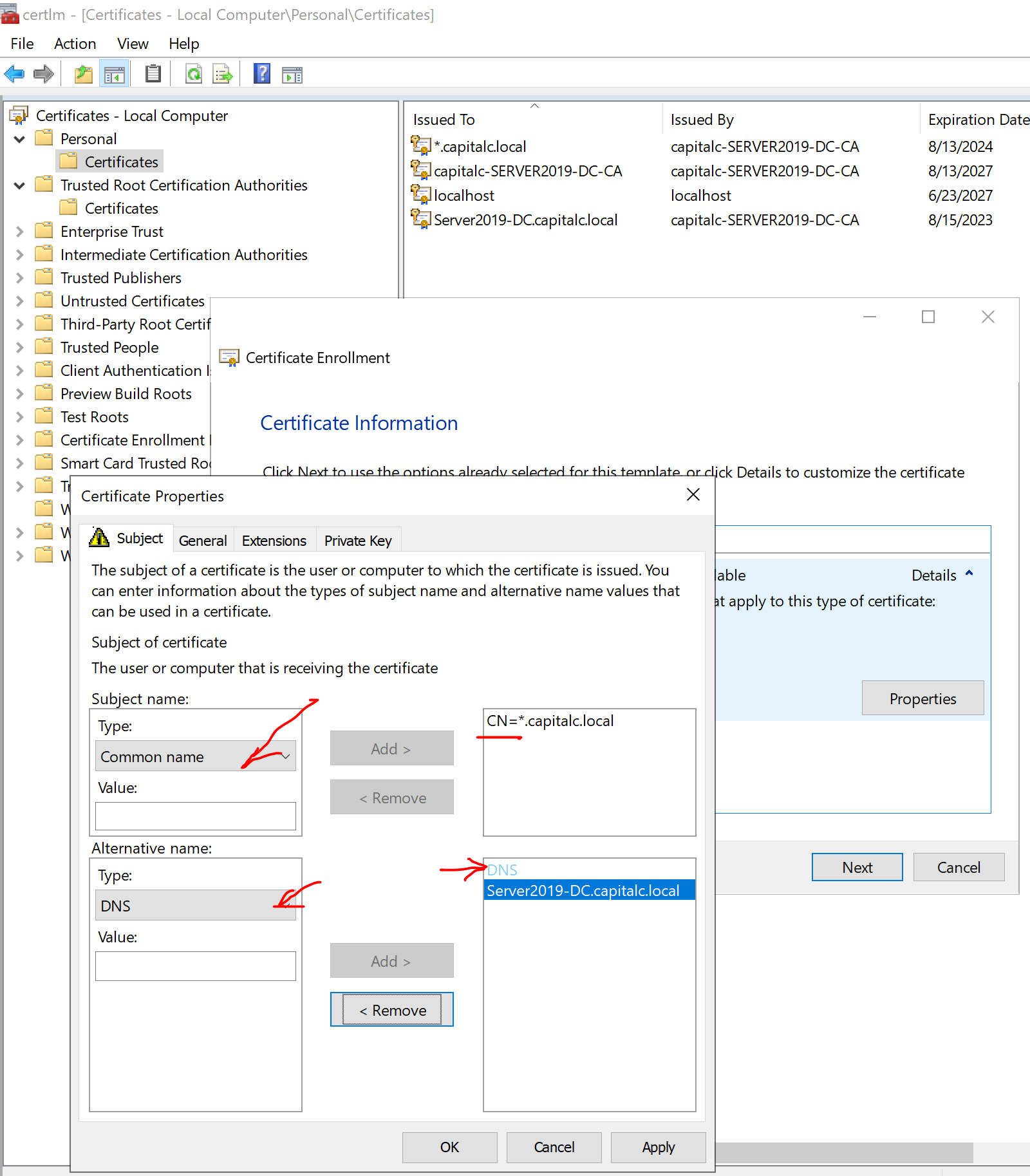
Open Manage computer certificates by typing “certificate” in lookup



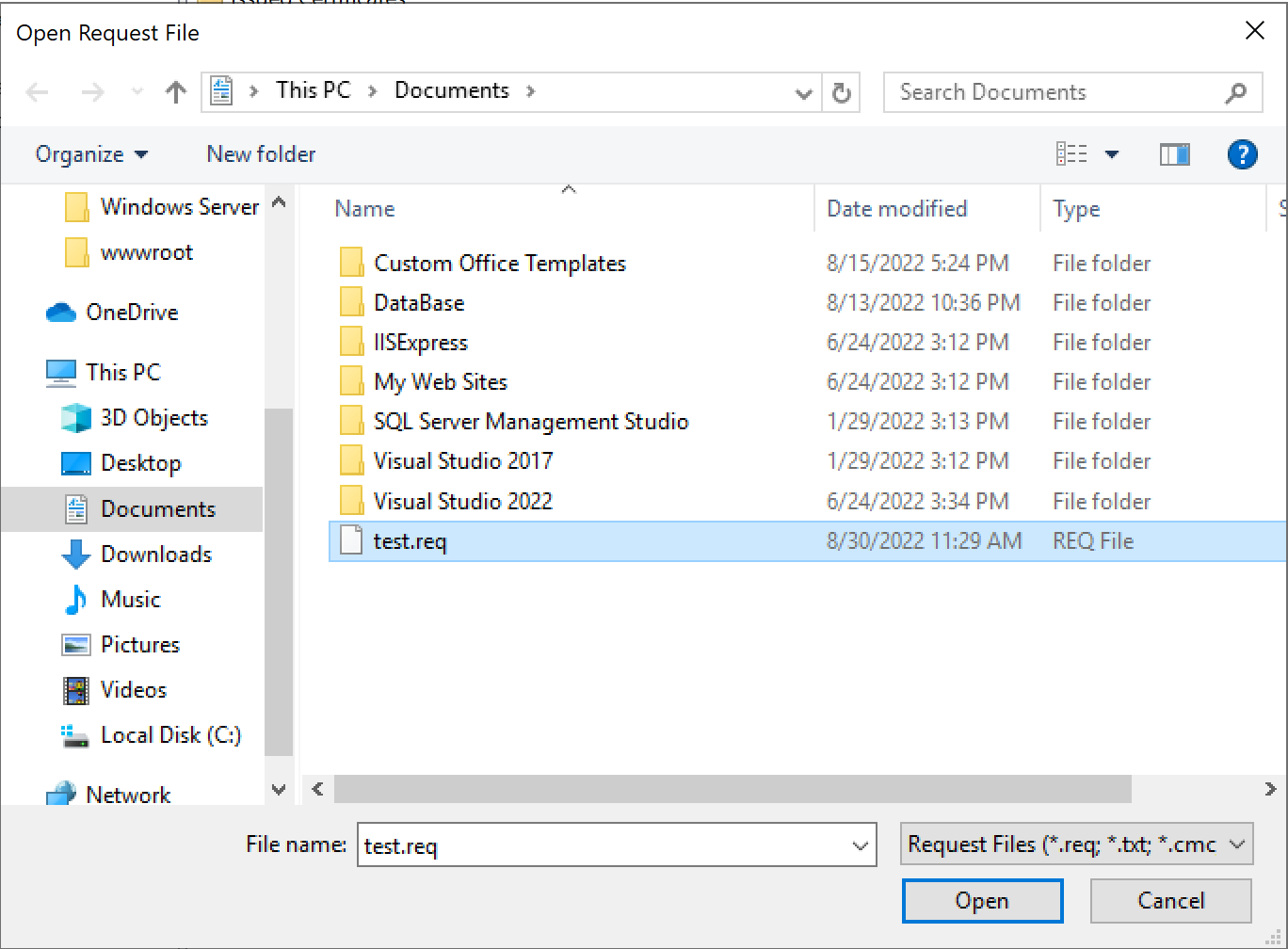




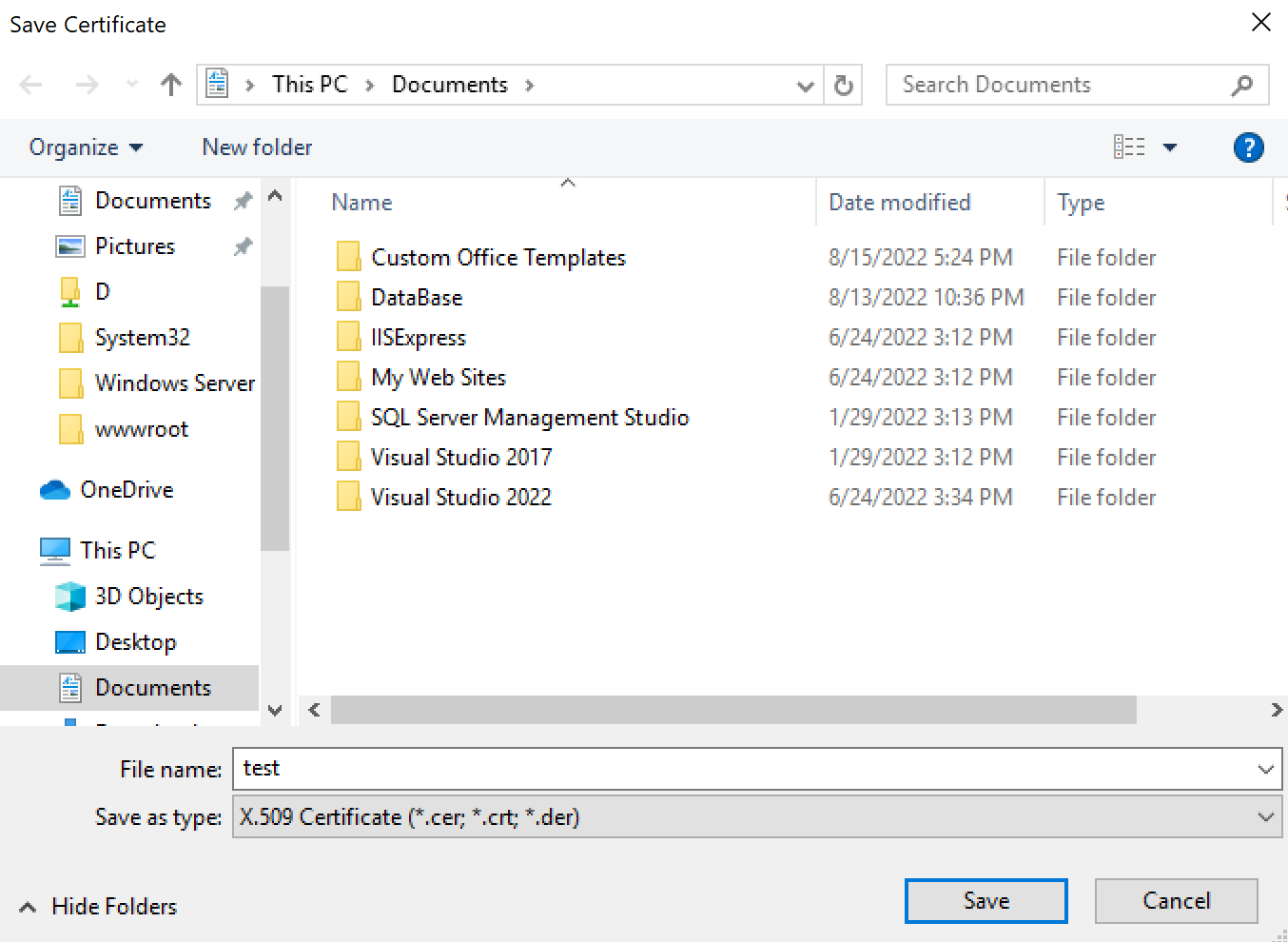


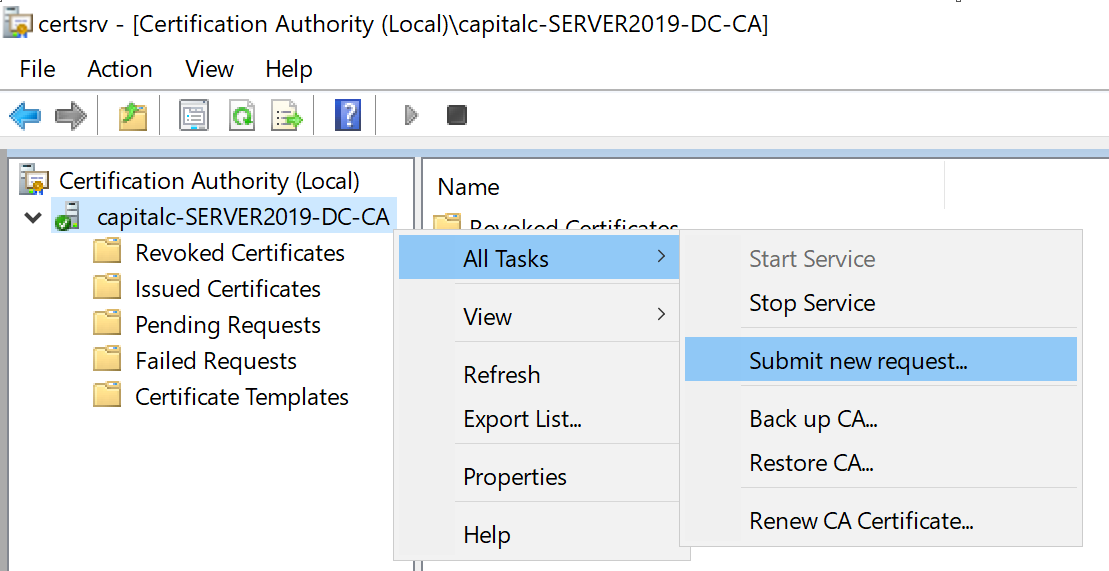


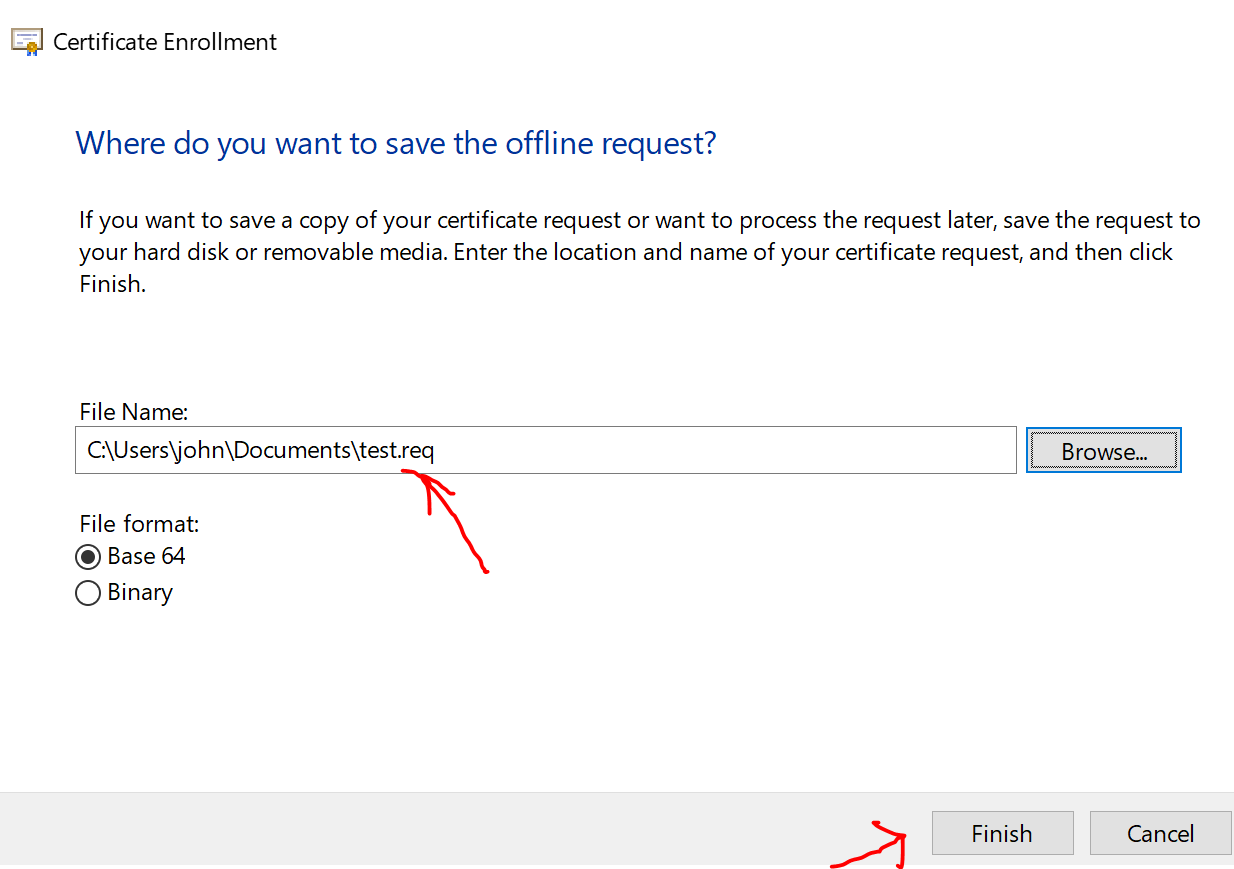
Open Certificate Authority 🡪 Submit new request 🡪 select the \*.req file created by previous steps



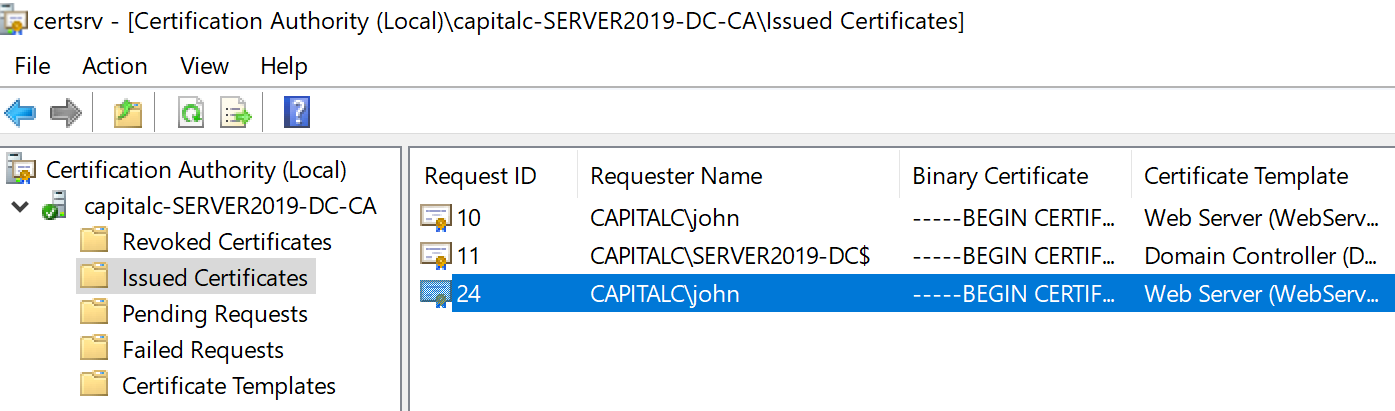
Once request completed it will ask you to save the generated certificate:







You can see the newly generated web server certificate appear in Issued Certificates list in Certification Authority application:

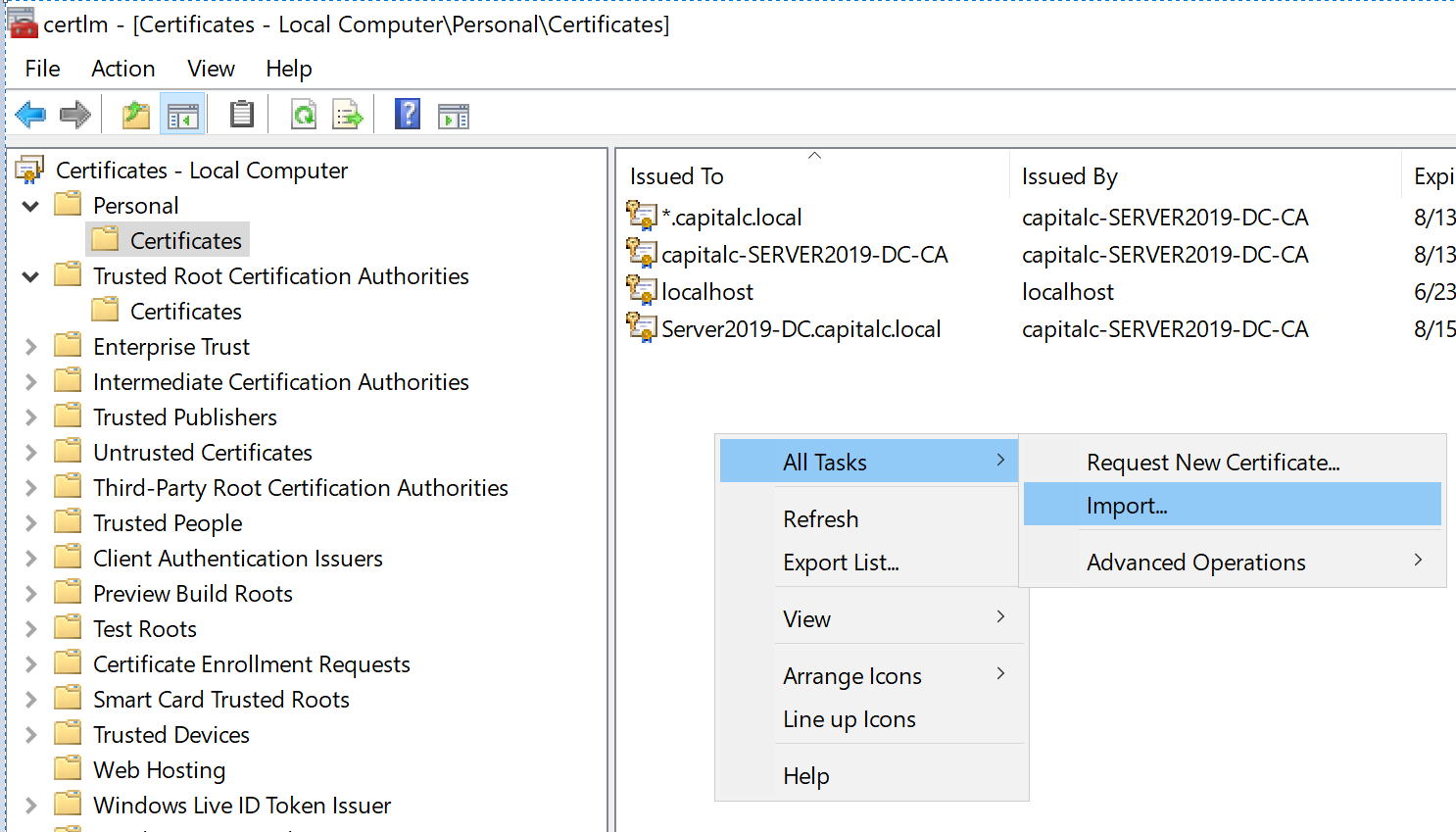


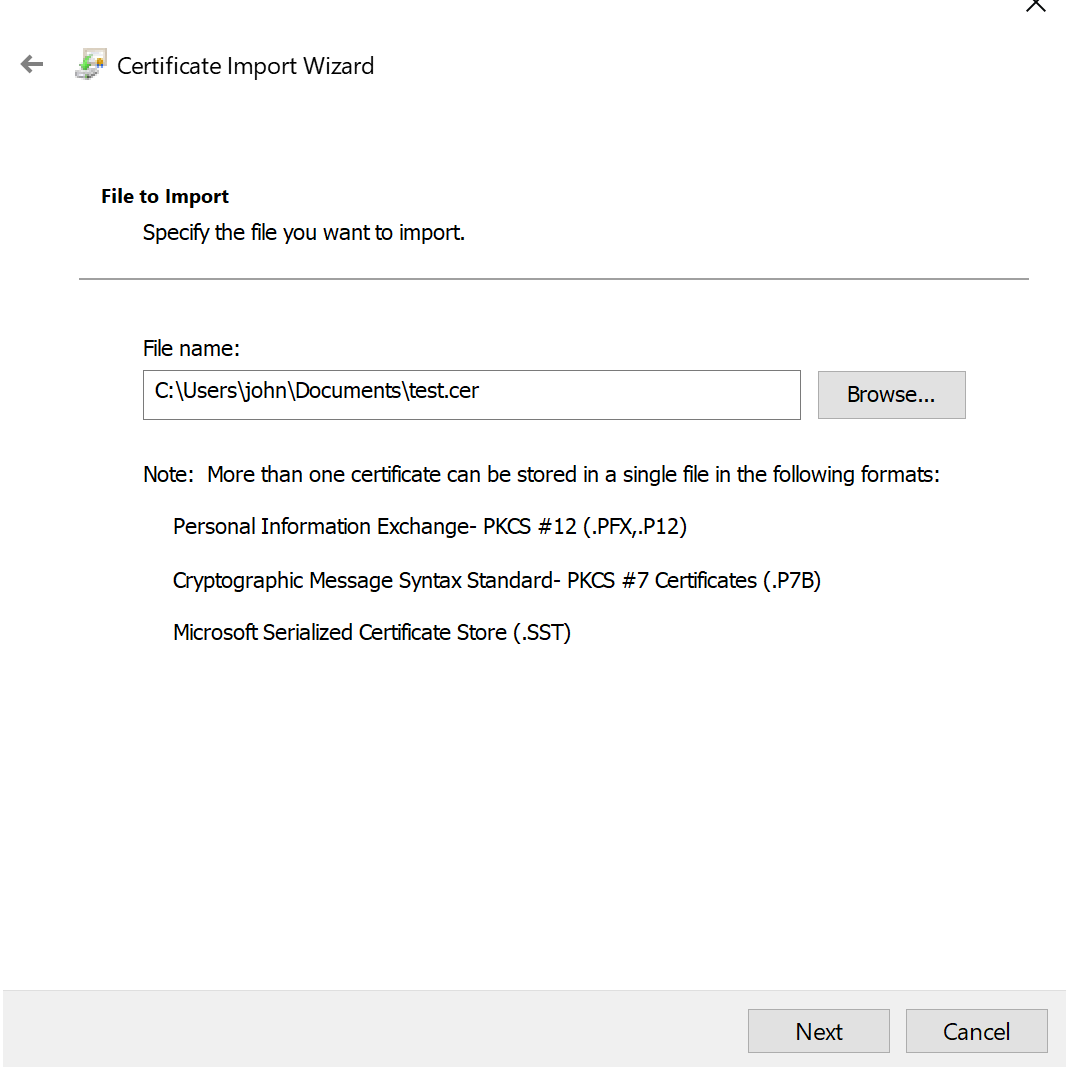
Here we can export the binanary \*.cer file from certsrv.

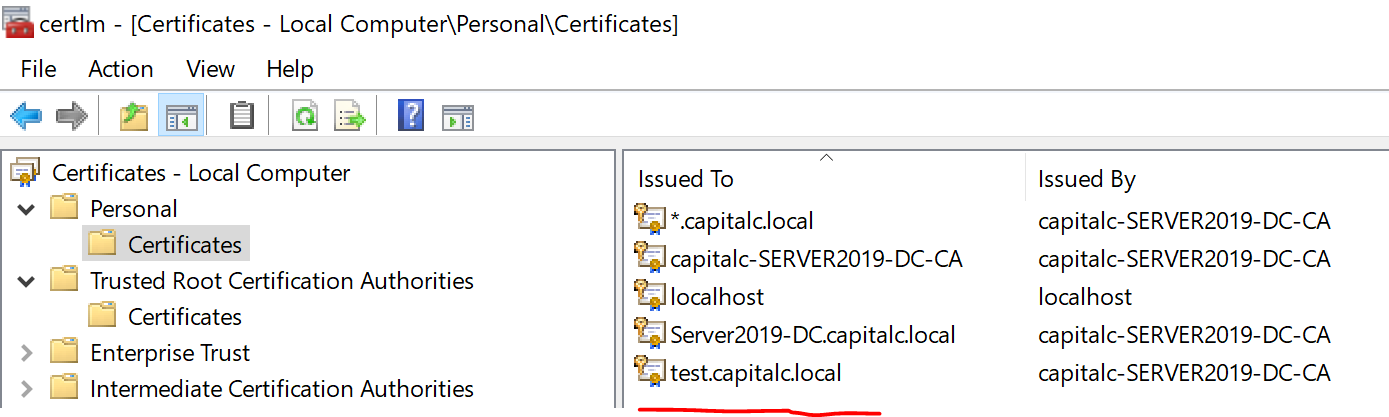
CER File Format 1 The PKC S#7 comprise Base64 ASCII encoding 2 Its file extensions are p7b or p7cZ 3 For binary content, the certificate would be DER or pkcs12/pfx.

* Install web server certificate to IIS web site

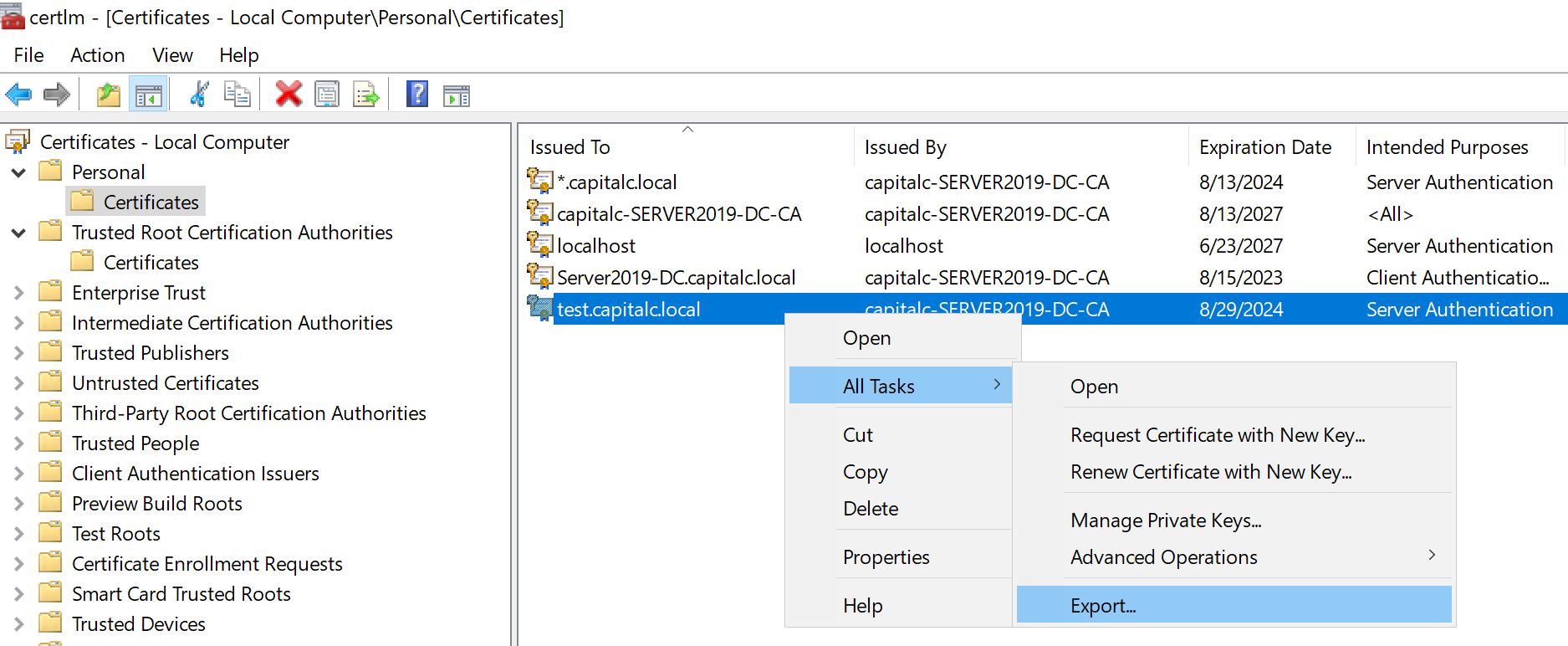
Import the generated web site certificate to MMC

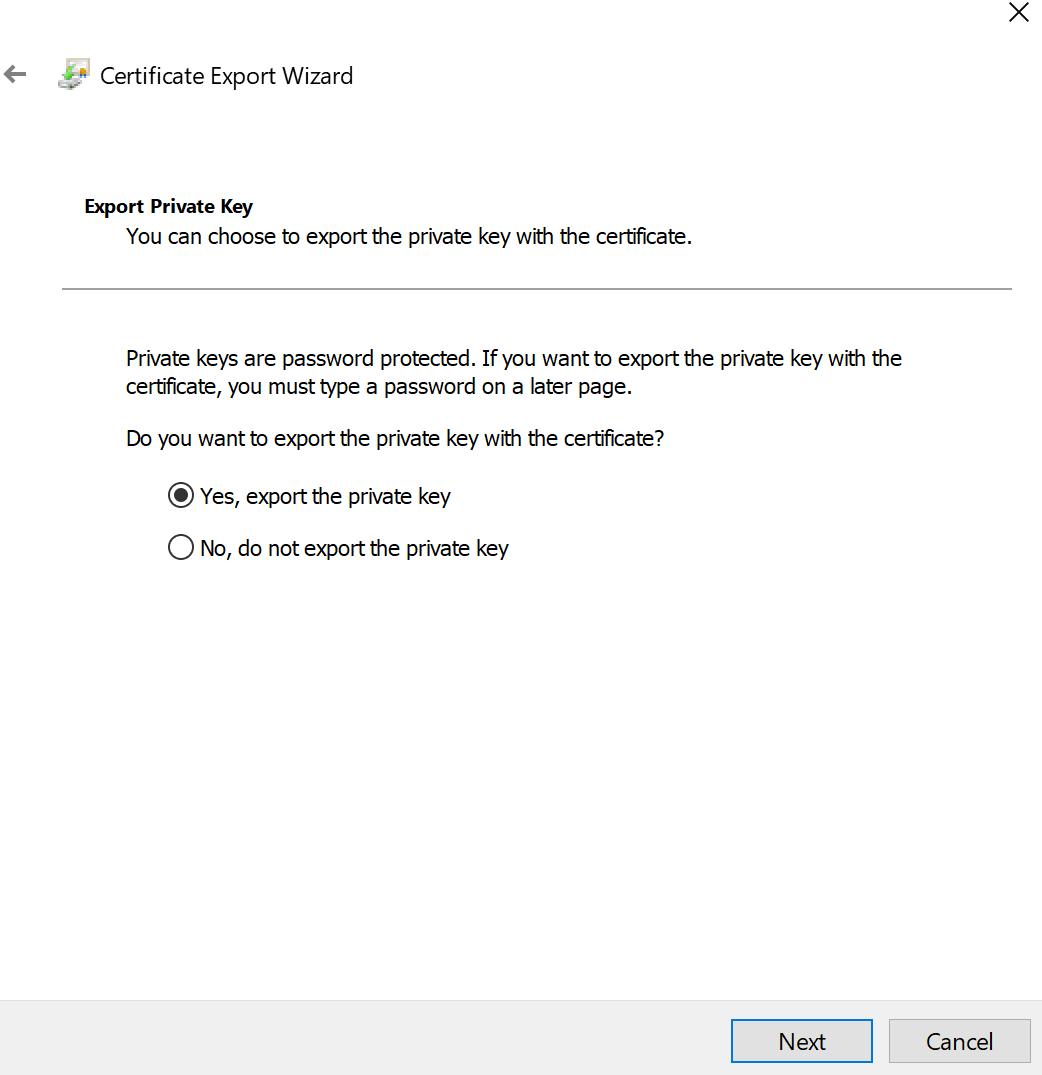


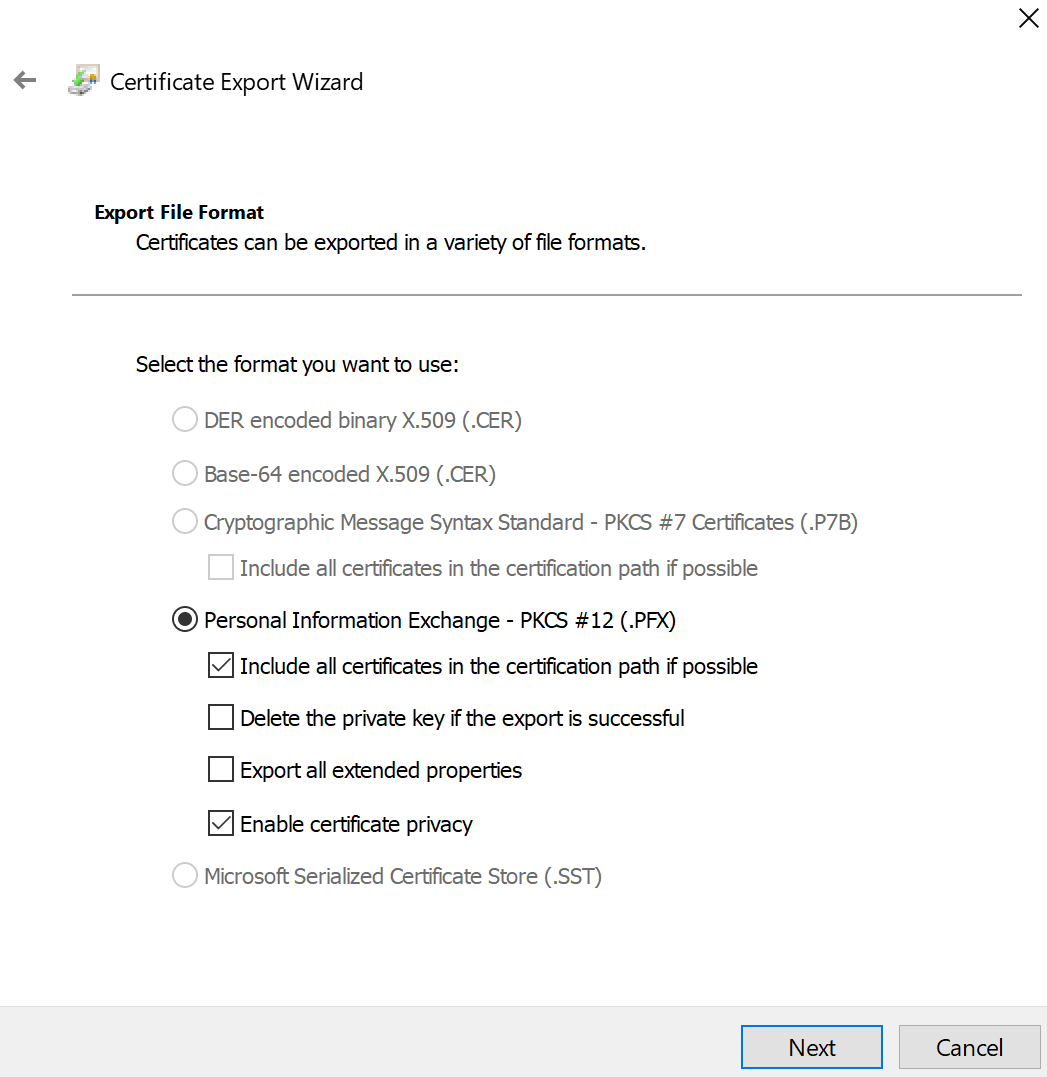


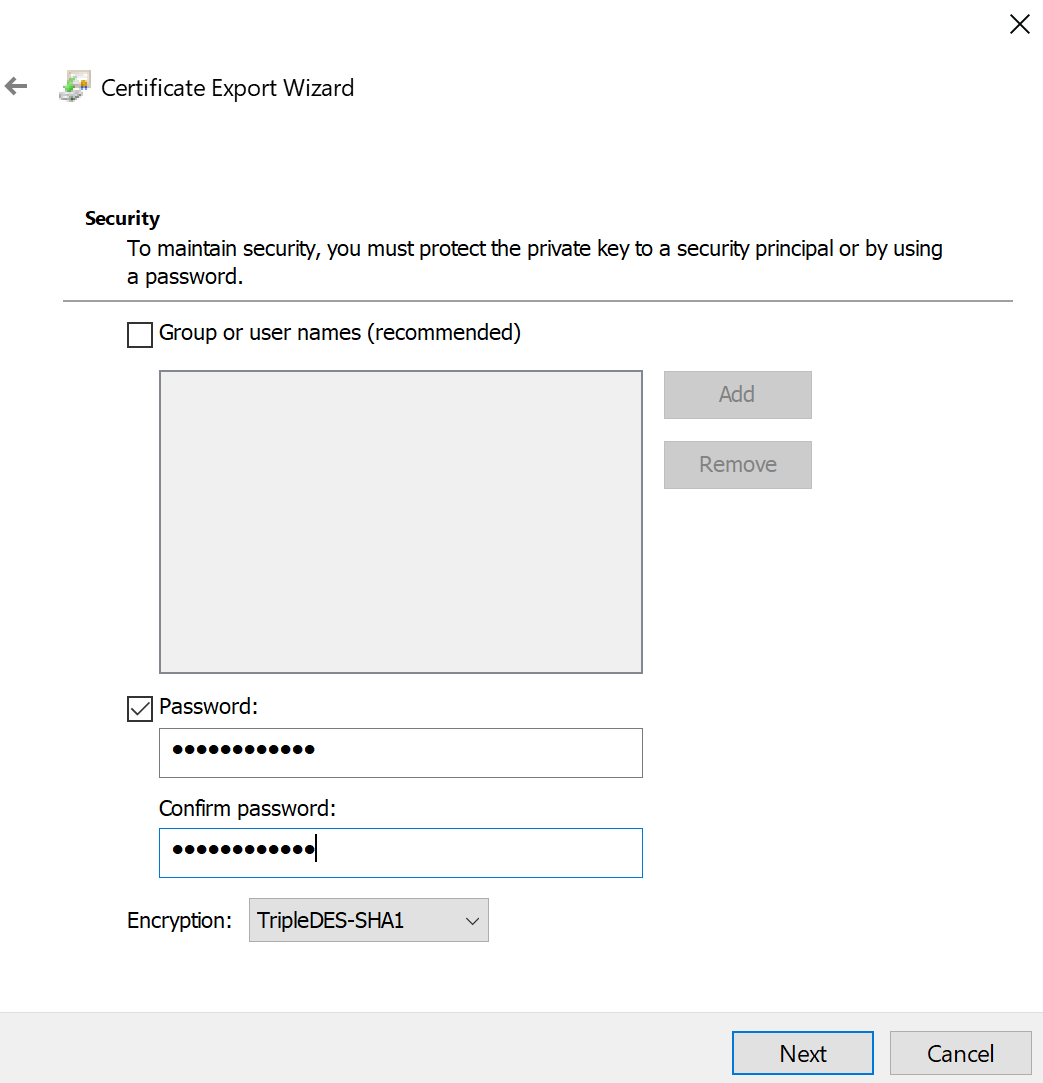


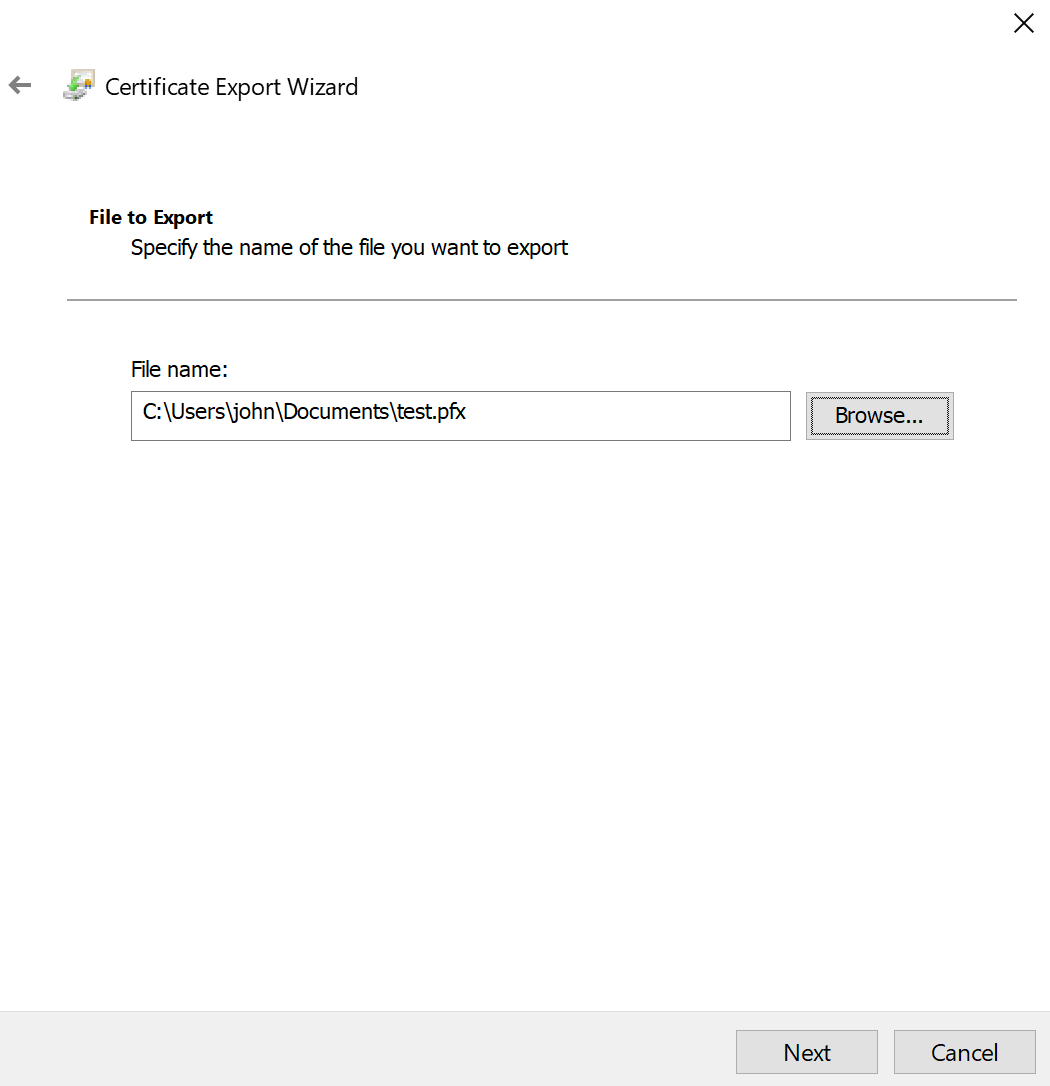
Export the certificate from Personal store to a \*.pfx file:



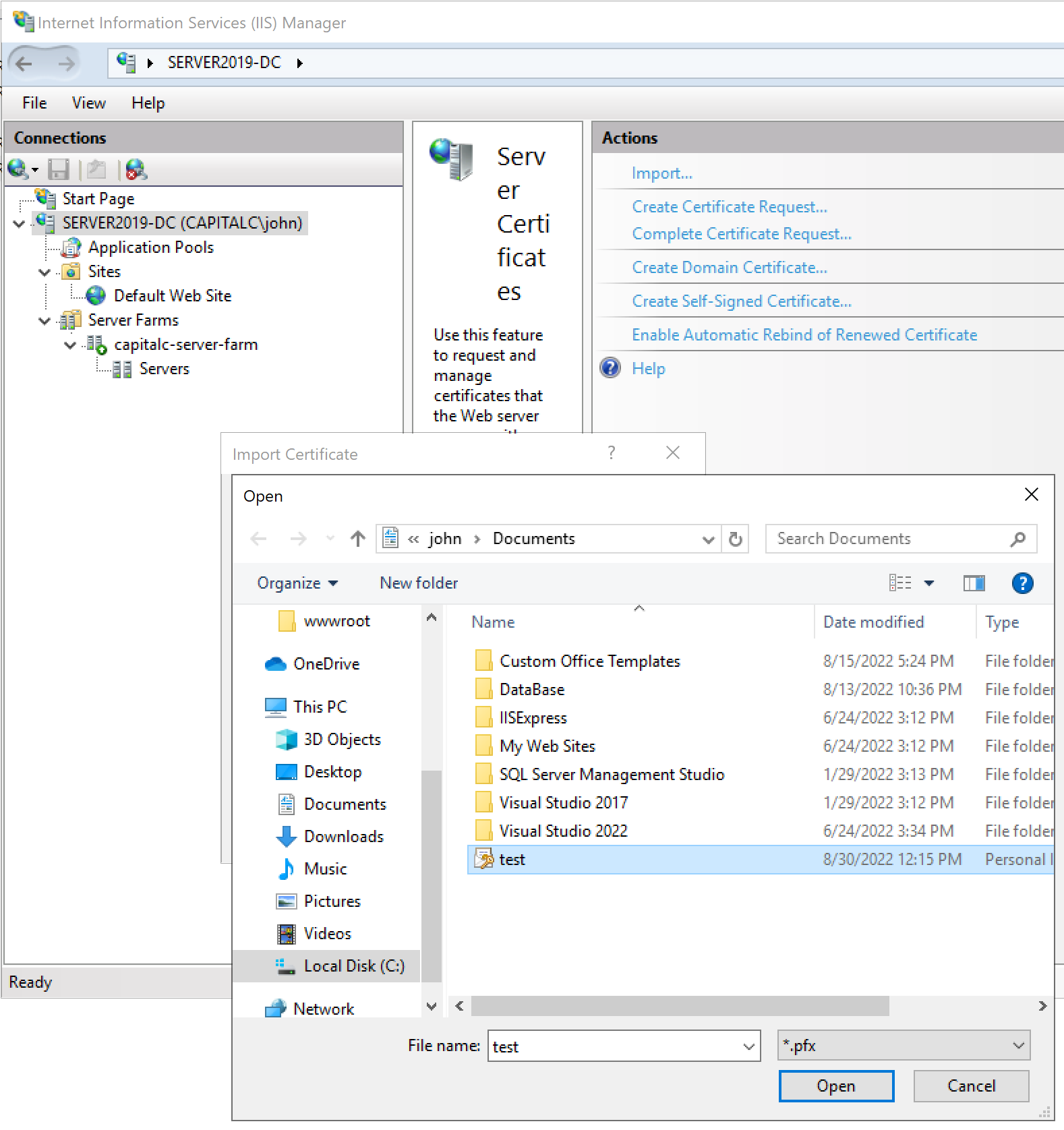


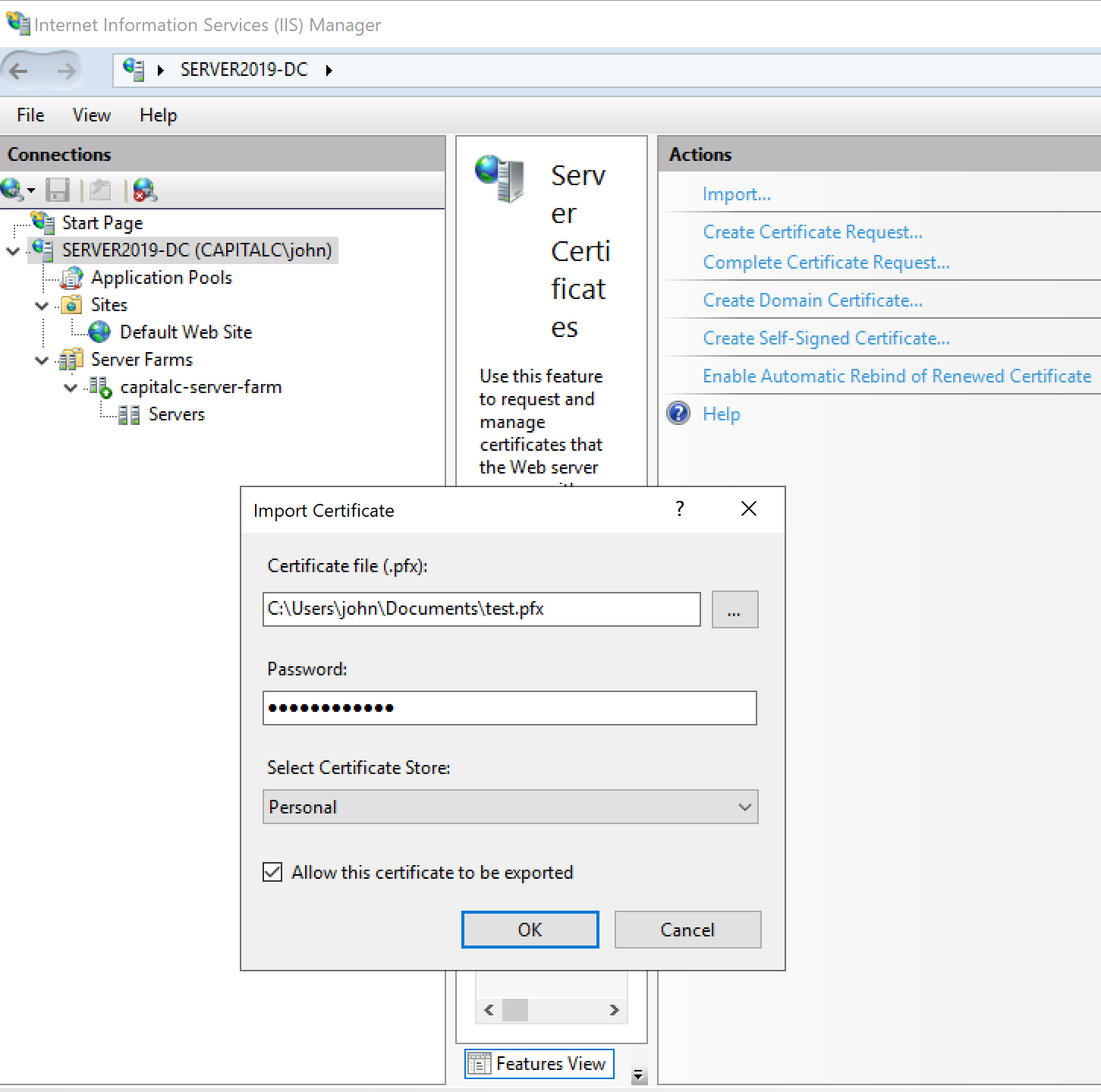


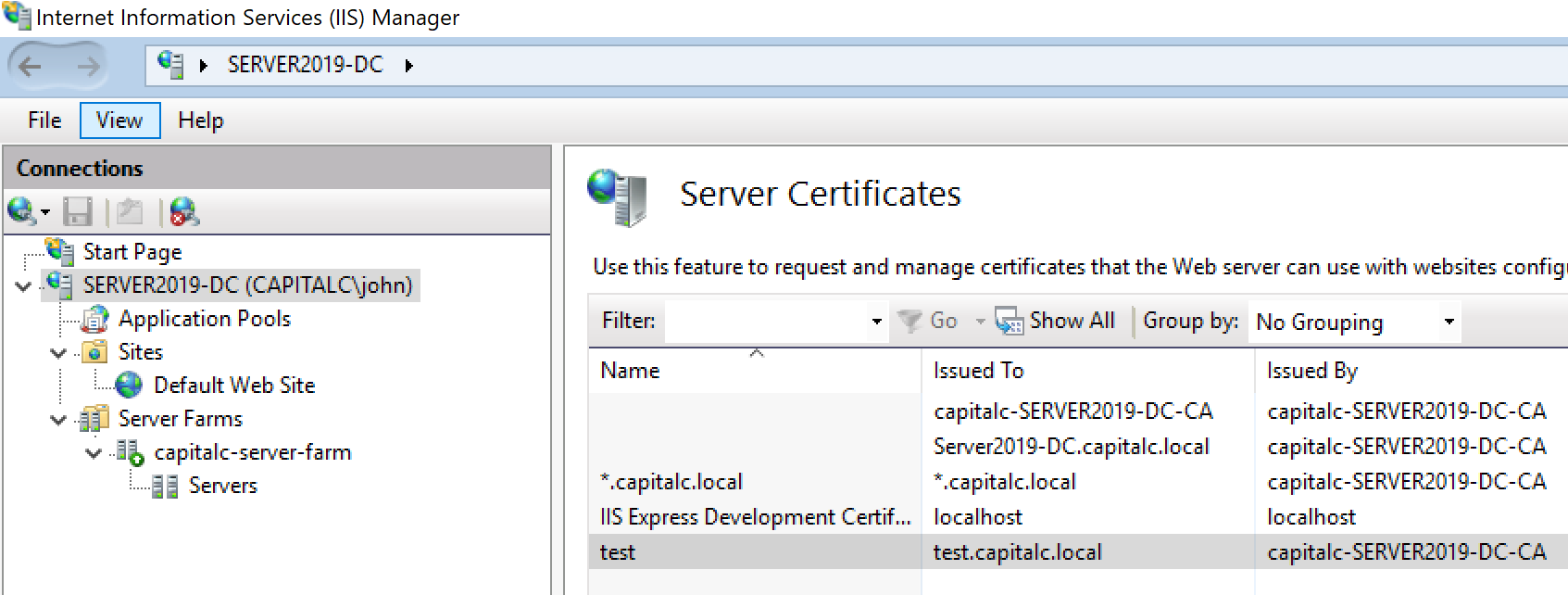




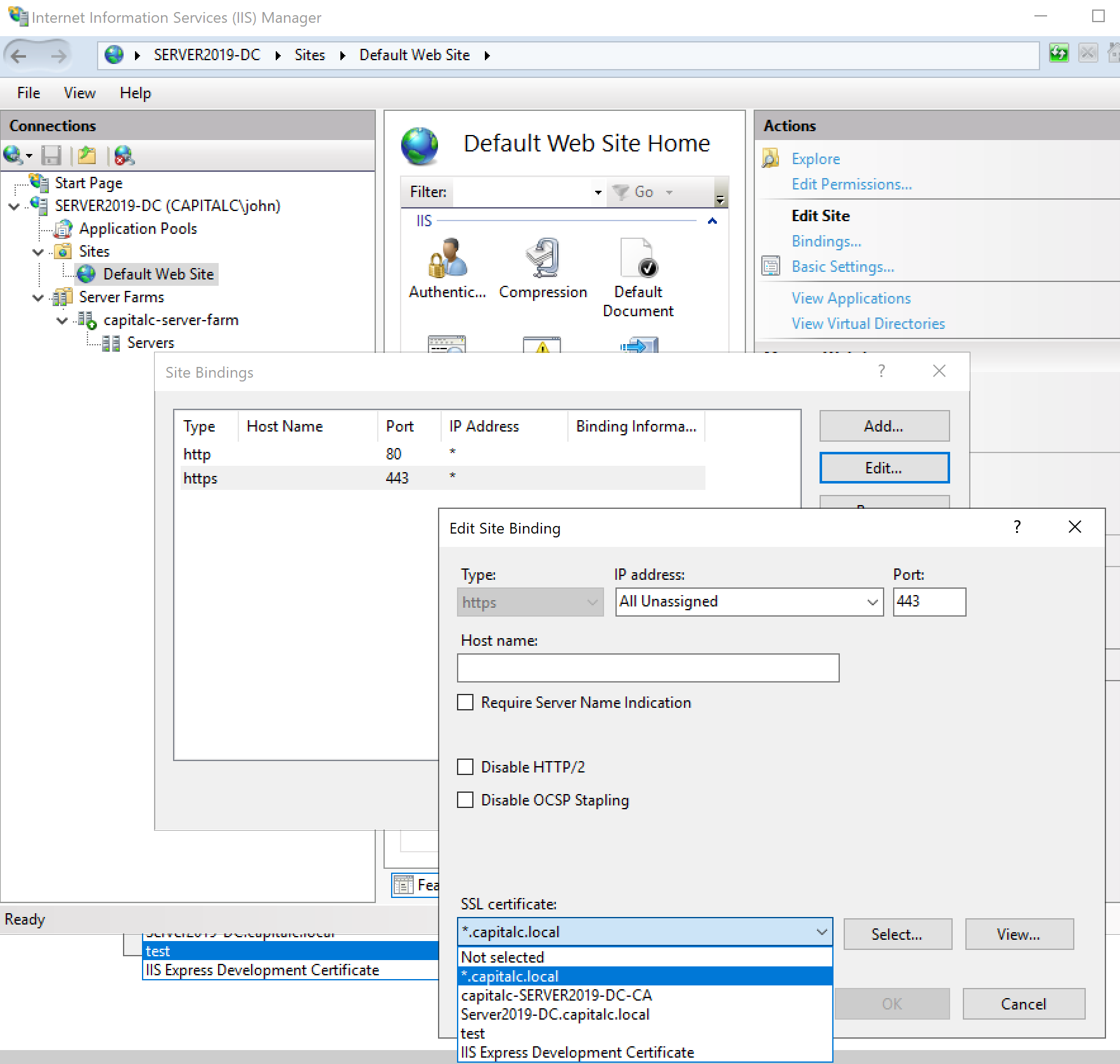
Import the web site certificate to IIS:

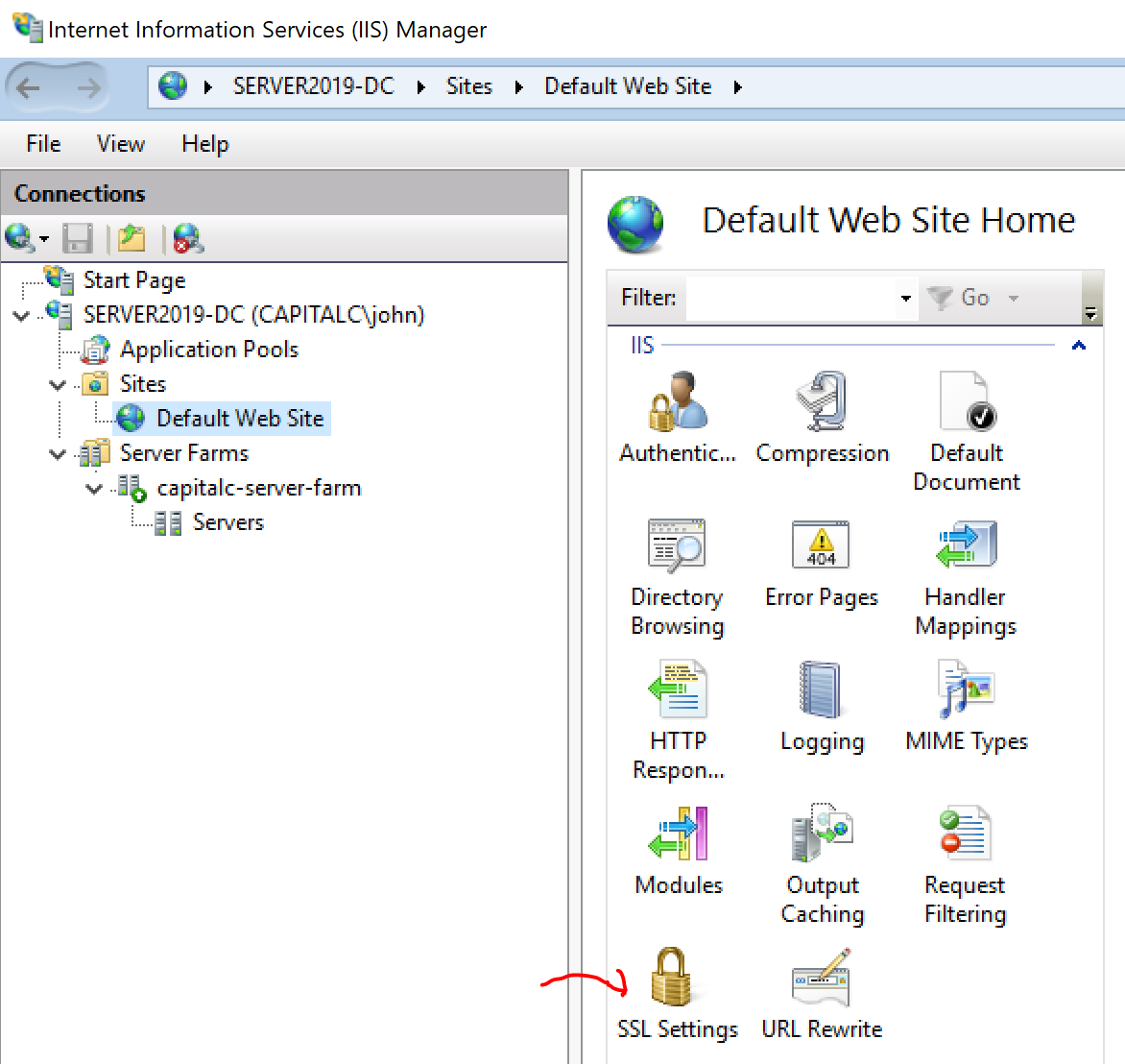


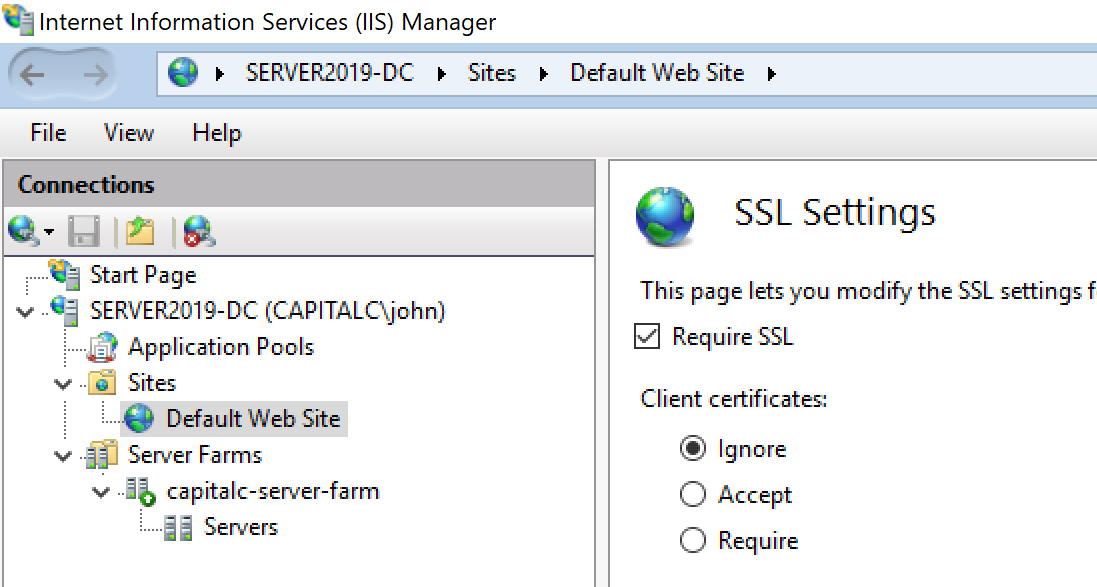




Pick a certificate for a web site:

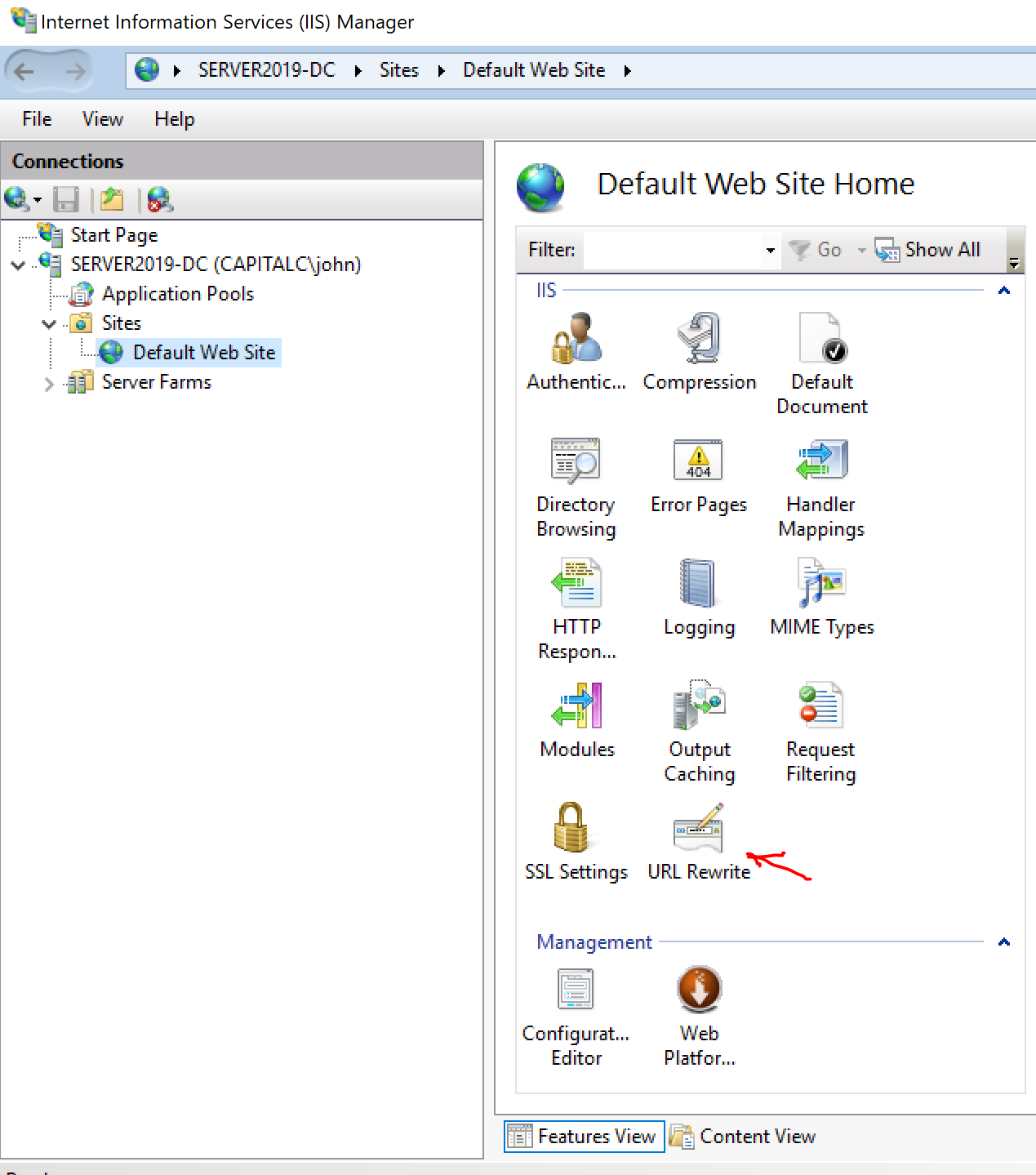


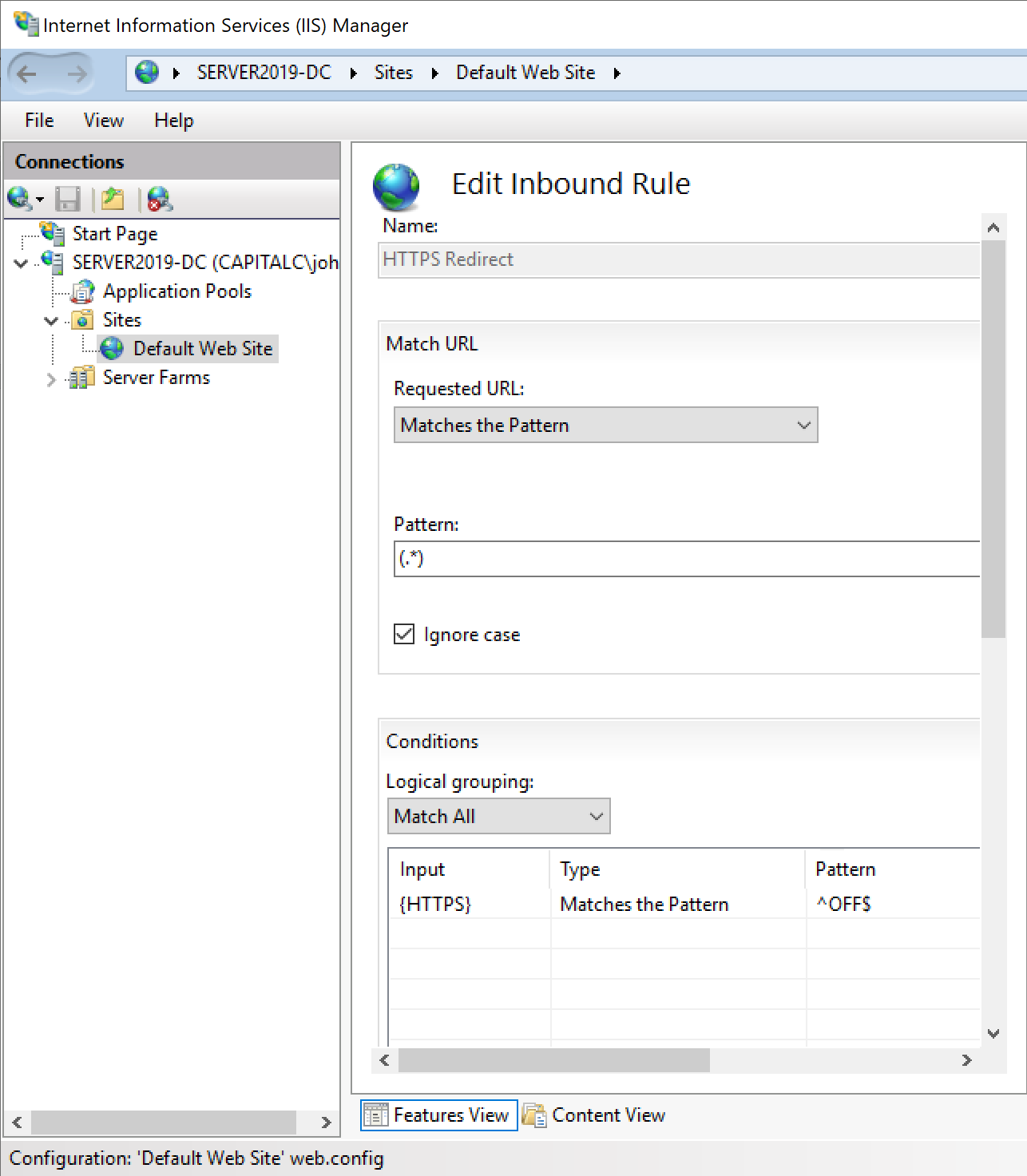




If “Required SSL” is checked it means user has to use https, if type http:// there will be an error reported from the browser.

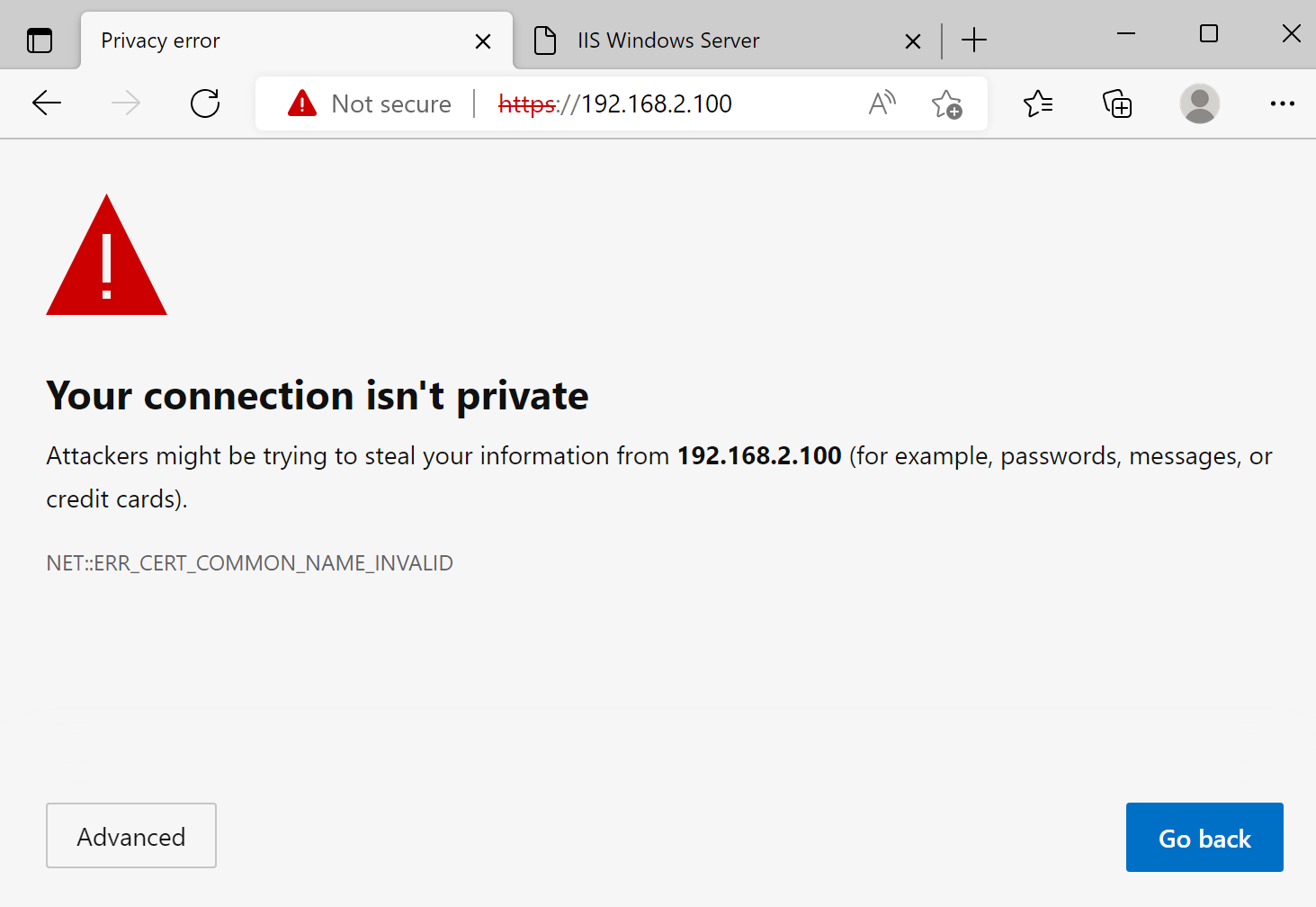
URL Rewrite is used to redirect http:// to https:// automatically. This also works in the ARR setting, all the http:// requests to NLB server farm (in our case is Server2019-DC.capitalc.local) will be redirected to use https:// automatically.





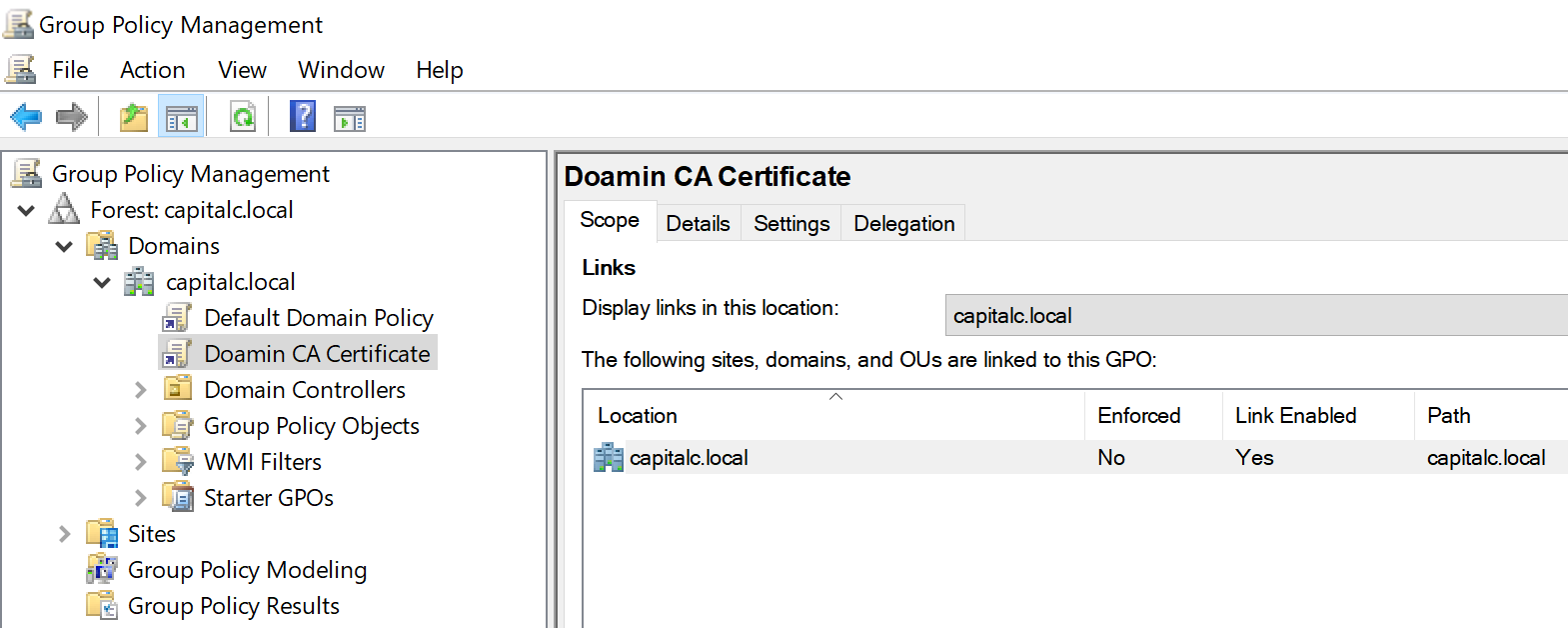
This URL Redirect rule only applies to [www.capitalc.local](http://www.capitalc.local) pattern, it won’t work for <http://192.168.2.100>

And the Web Site Certificate only works for \*.capital.local patter, won’t work for <https://192.168.2.100>



# Trust Domain Certificate

As long as Domain CA Certificate is installed then all the web site certificates are automatically trust by browser running against the domain web site with name \*.capitalc.local



# Configure DNS for [www.capitalc.local](http://www.capitalc.local)

