Setting up a Certificate Authority

Server Exploits - Module 2

Overview

What is a Certificate

HTTPS traffic is encrypted by a protocol (like TLS 1.2) and a cipher (like the 3DES cipher). In order to have full encrypted traffic over HTTPS, the server the client is connecting to will also need an SSL Certificate. This certificate is used to authenticate the identity of the server and encrypt the traffic between the server and the client. You can view an SSL Certificate in your browser by clicking on the lock icon next to a website's URL.

What is a Certificate

Certificate Viewer: *.nscc.ca

General Details

Issued To

Common Name (CN)	*.nscc.ca
Organization (O)	Nova Scotia Community College
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	GlobalSign RSA OV SSL CA 2018
Organization (O)	GlobalSign nv-sa
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Thursday, November 24, 2022 at 9:51:02 AM
Expires On	Tuesday, December 26, 2023 at 9:51:01 AM

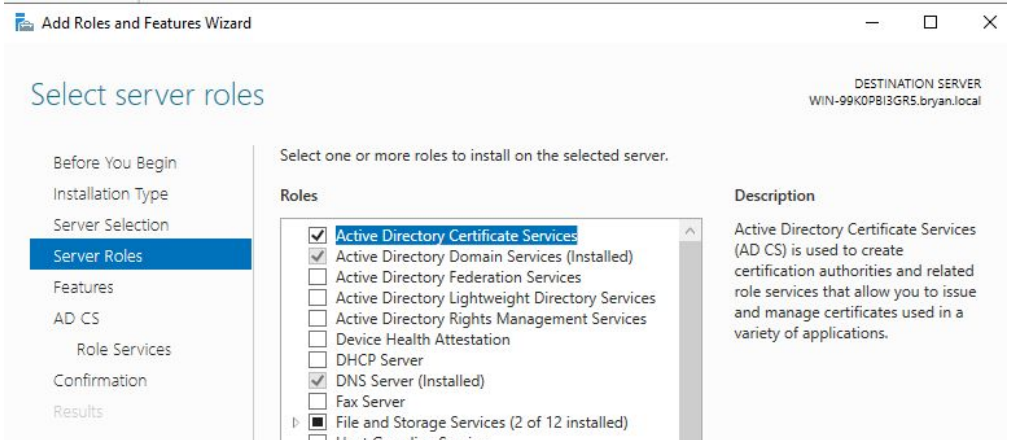
Fingerprints

SHA-256 Fingerprint	A2 FB 45 FB EF 37 A3 61 0D 29 7C C9 12 85 F1 85 93 2C 45 AB 80 89 FE 57 8C EB E6 48 75 77 38 FD
SHA-1 Fingerprint	0F E8 39 40 E8 77 72 47 6D BB 9A 6D 5B AE BF 2B 67 FC 1E 51

Setup

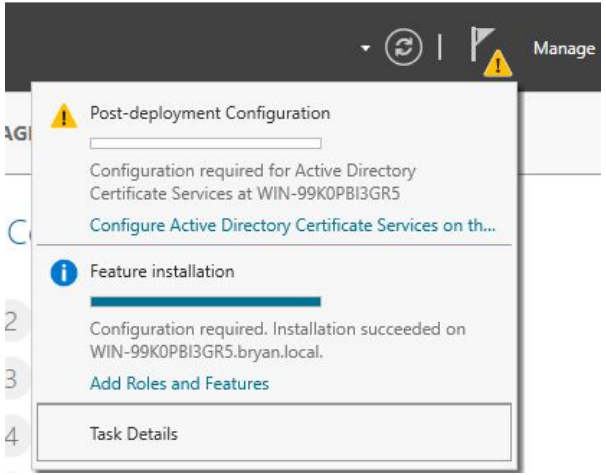
Configuring a CA

If we want to get Win-RM to communicate over HTTPS, we will have to create a certificate for the DC. Firstly, we will need to add the Active Directory Certificate Services feature. You can do this the same way you created the DC.



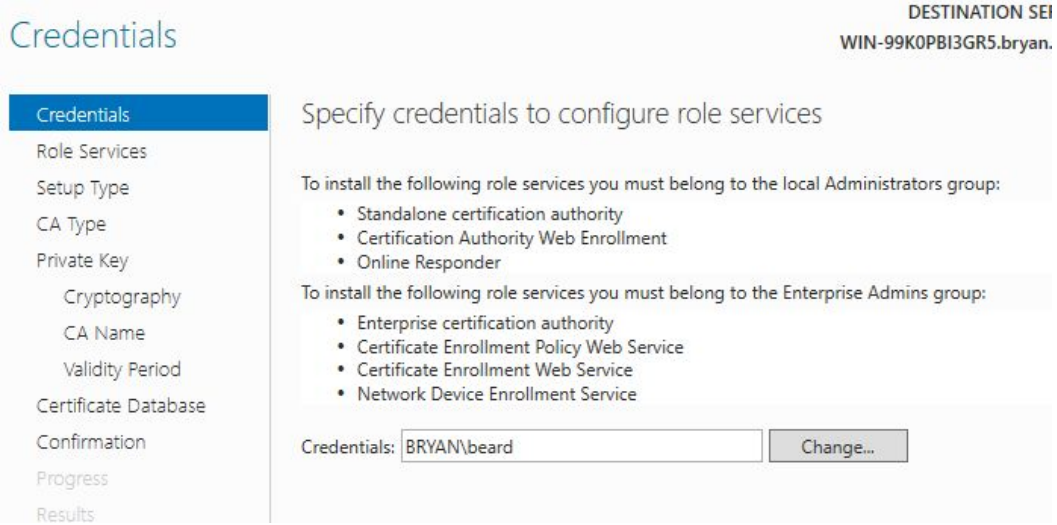
Configuring a CA

For the roles, we just need a certificate authority. This will designate the DC as the authority to create and sign SSL Certificates for your domain. You will see an alert message to Configure AD Certificate Services.



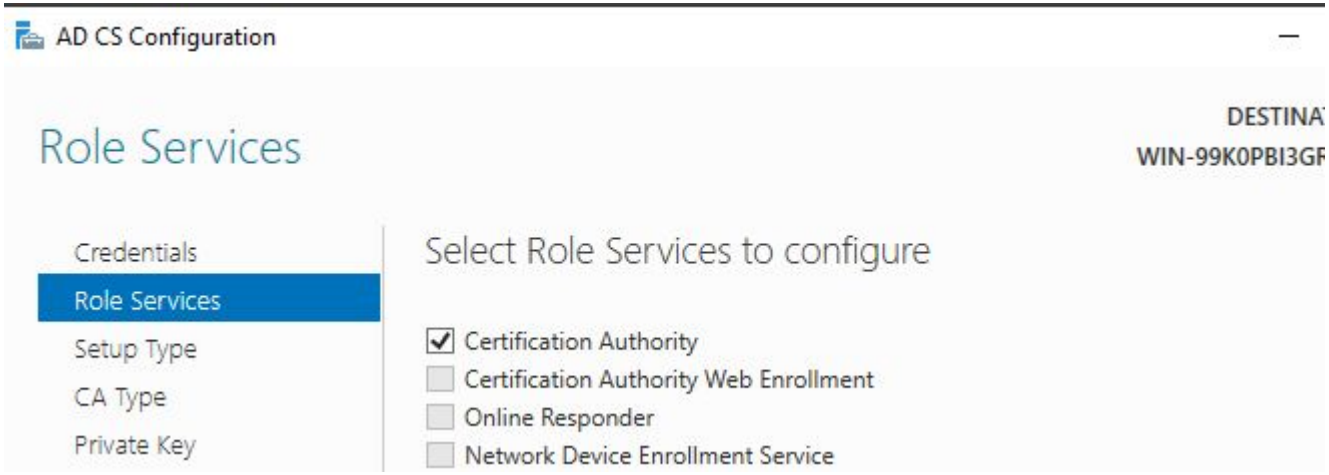
Configuring a CA

You will need to add your Domain Admin's credentials.



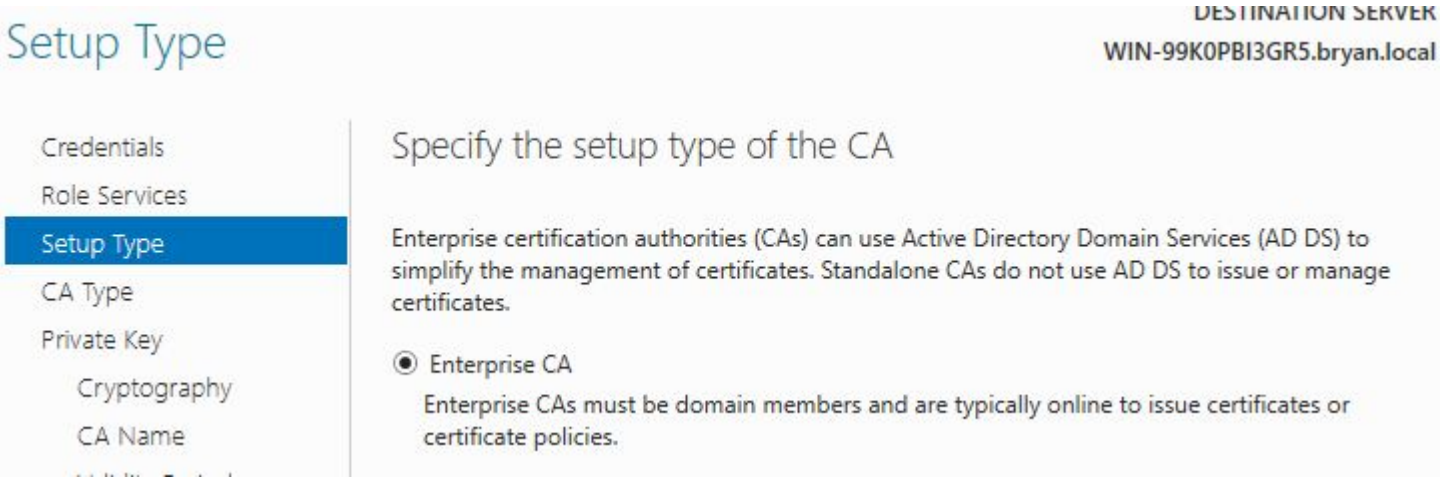
Configuring a CA

Roll Services will just be Certificate Authority



Configuring a CA

Click Enterprise CA. This is for domain members.



Configuring a CA

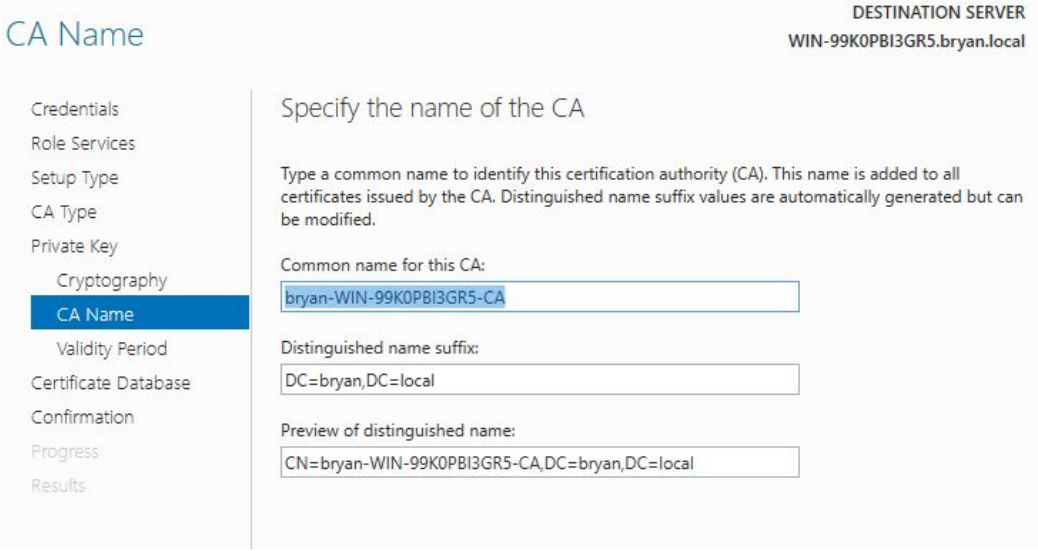
Because this is our first Certificate Authority, click Root CA. Click Next and create a new private key.

Configuring a CA

For your private key, there are some best practices. Nowadays, the private key should be at least RSA 2048 for its cryptographic provider and the signing algorithm must be at least SHA256 (do not use SHA1 or MD5 as these are weak encryption algorithms).

Configuring a CA

Your CA Name details should be automatically filled out. This sets your DC as the CA.



Configuring a CA

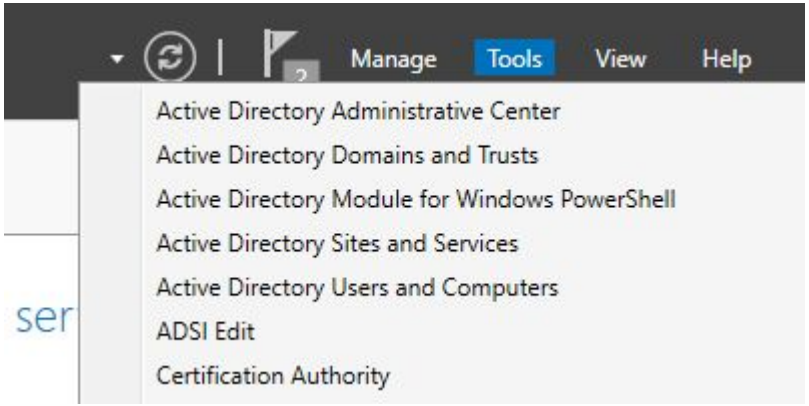
You can set your validity period to be however long you want. 5 Years is good. This means you will have to redo your CA in 5 years time.

The default certificate database folder path is OK, so don't change that either.

Click Configure when you are done.

Configuring a CA

You should now see Certificate Authority under your Tools in Server Manager. Open it.



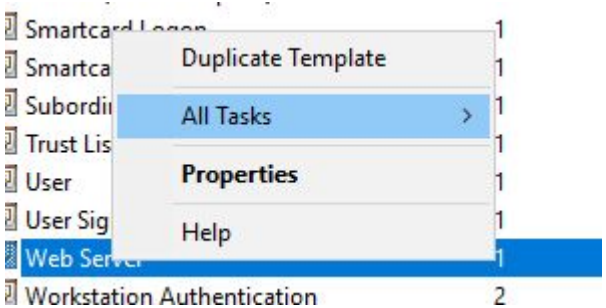
Creating a Certificate

Creating a Certificate

Right-Click Certificate Templates and hit Manage

Creating a Certificate

Find the Web Server Template and right-click and select Duplicate Template

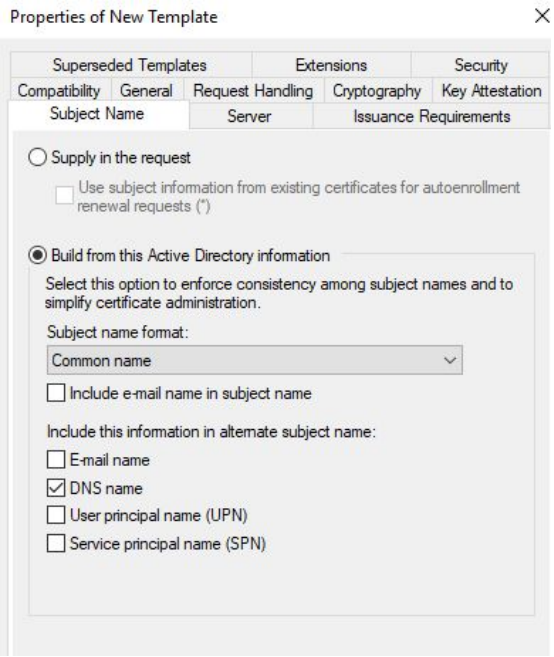


Creating a Certificate

Under the General tab, you can name your new certificate template under the Template display name field. I have called mine WinRM.

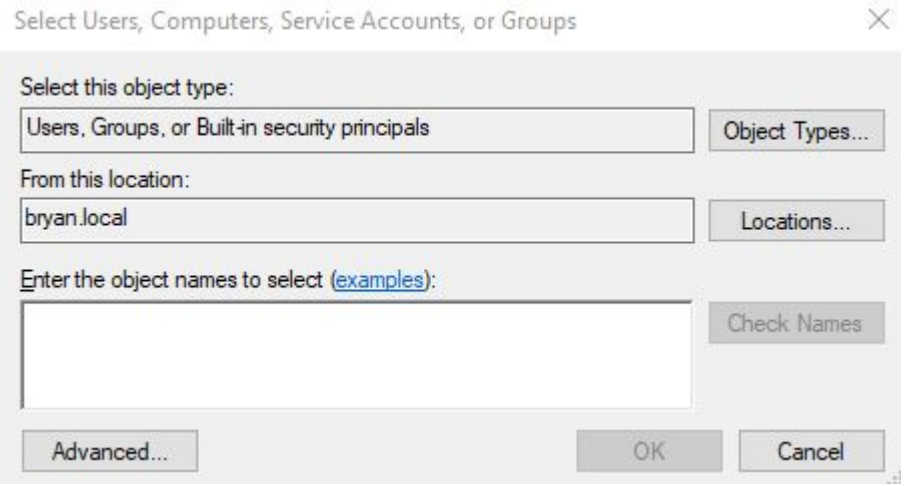
Creating a Certificate

Under the Subject Name Tab, select “Build from AD Information”. Select Common name for the Subject Name Format, and include only DNS name as alternate subject name.



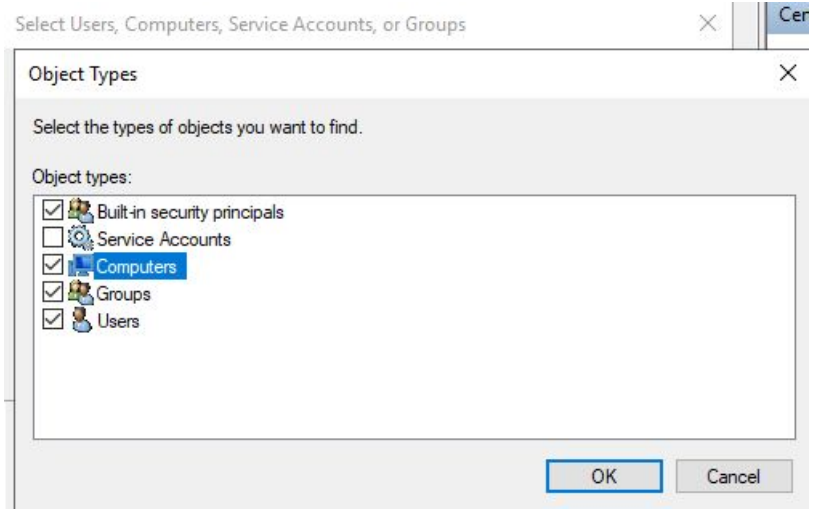
Creating a Certificate

Under the Security tab, click Add to Add a group. You will see the following Window.



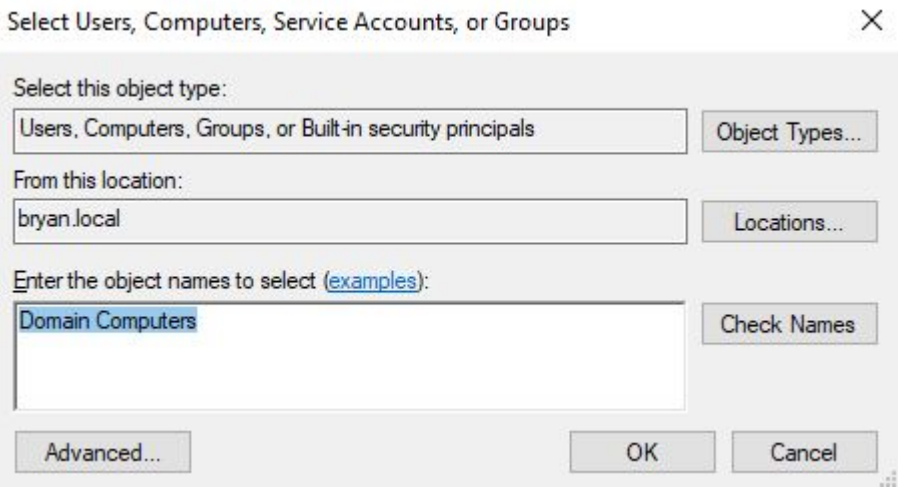
Creating a Certificate

Click “Object Types and ensure the Computers box is checked. Hit OK when you are done.



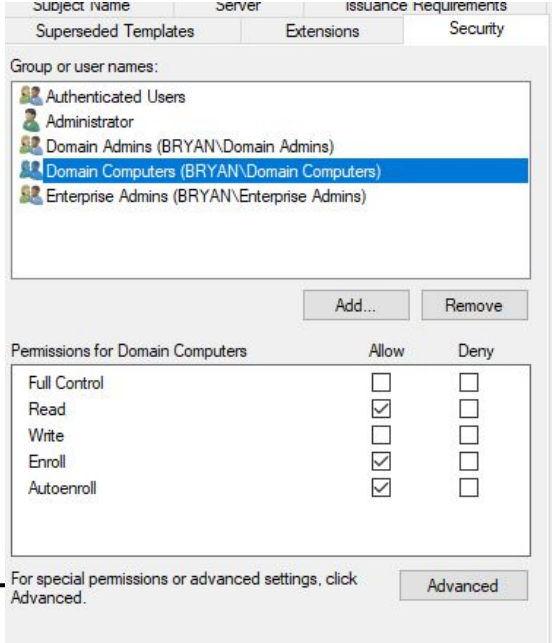
Creating a Certificate

Now Add the Domain Computers group and hit OK.



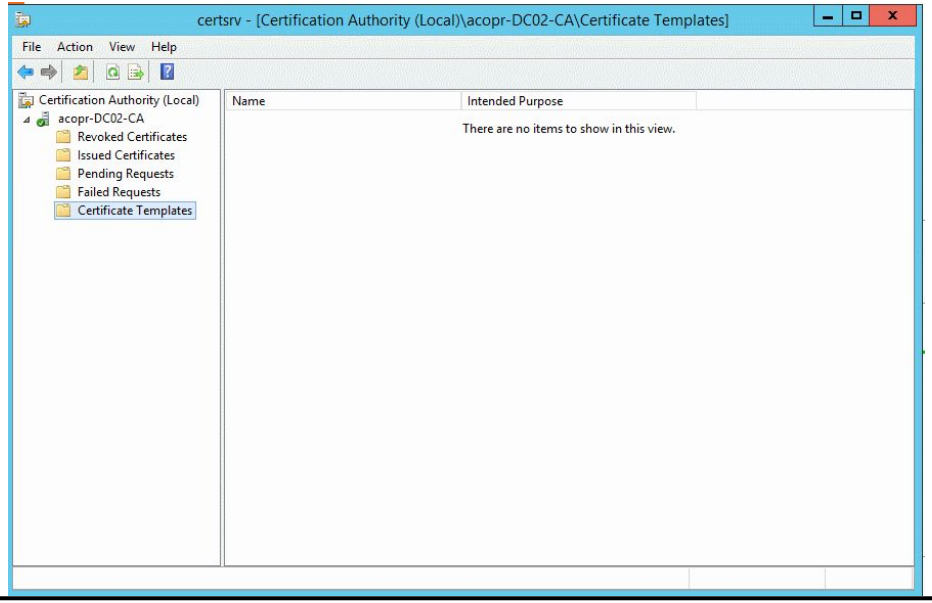
Creating a Certificate

Give Read, Enroll and Autoenroll permissions to the Domain Computers group. The hit Apply.



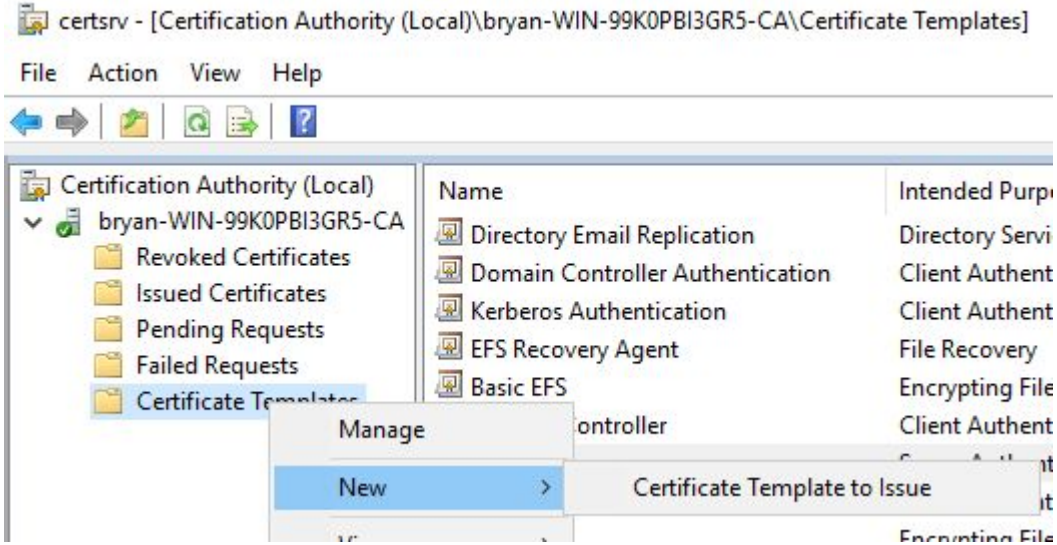
Creating a Certificate

Here is an animation of the previous steps. This animation checks UPN under Subject Name, which is not required.



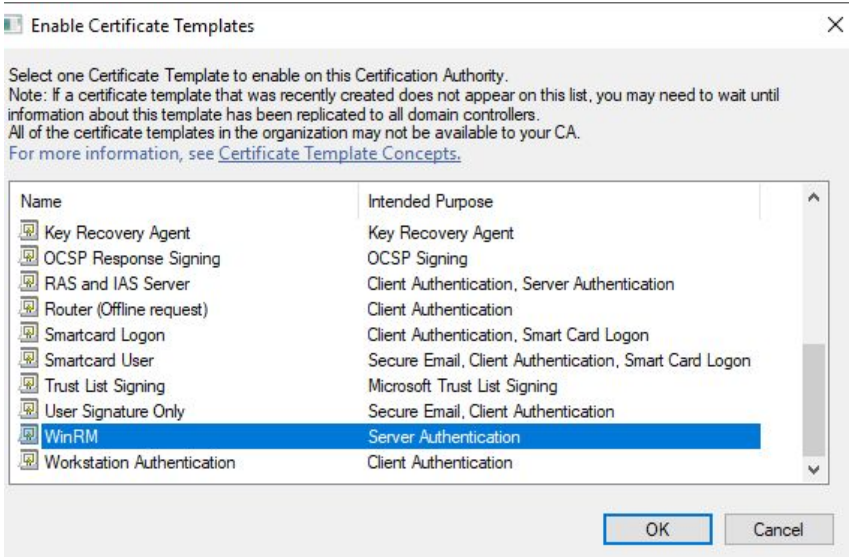
Creating a Certificate

Go back to the certsrv window, right click Certificate Templates -> new -> Certificate Template to Issue



Creating a Certificate

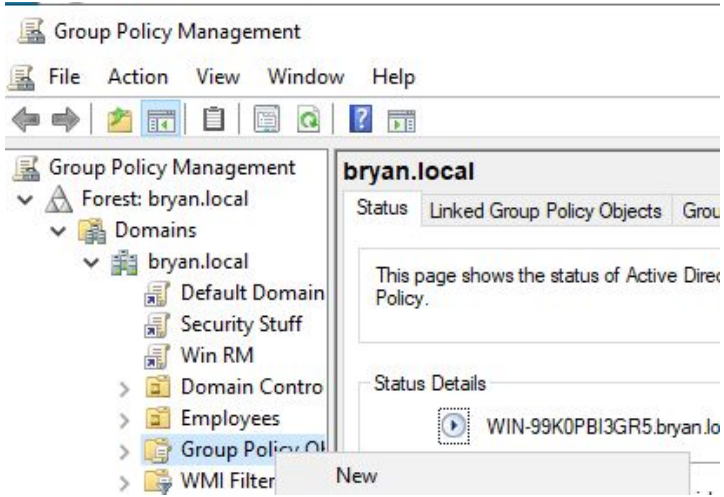
Find your WinRM certificate and Click OK.



Pushing Out the Certificate

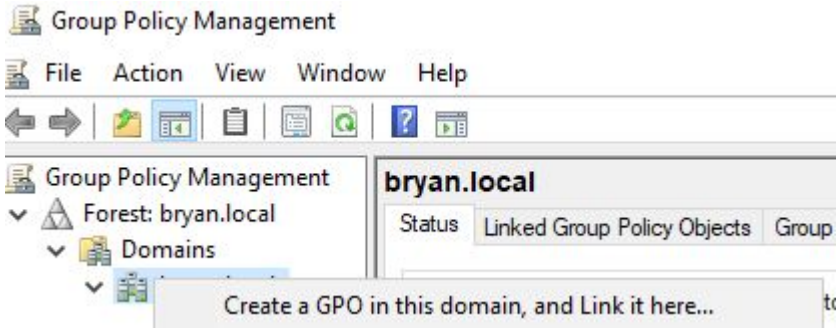
Creating a Certificate

With the certificate created, we can now use a GPO to push it out to all machines in your domain. Open up GPMC and create a new GPO. You can call it whatever you'd like.



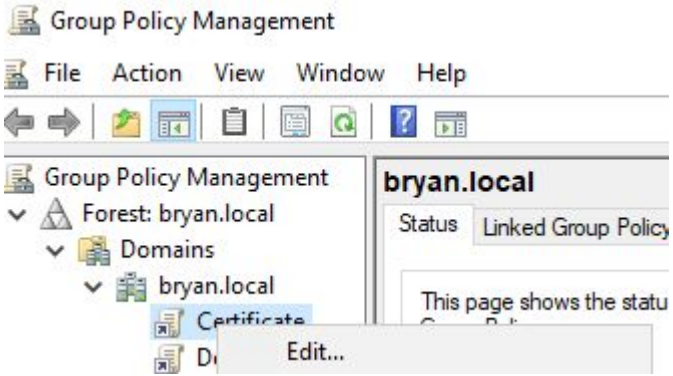
Creating a Certificate

With the certificate created, we can now use a GPO to push it out to all machines in your domain. Open up GPMC and create a new GPO by right-clicking your domain and clicking Create a GPO in this domain and Link it here. You can call it whatever you'd like, I have called mine "Certificate".



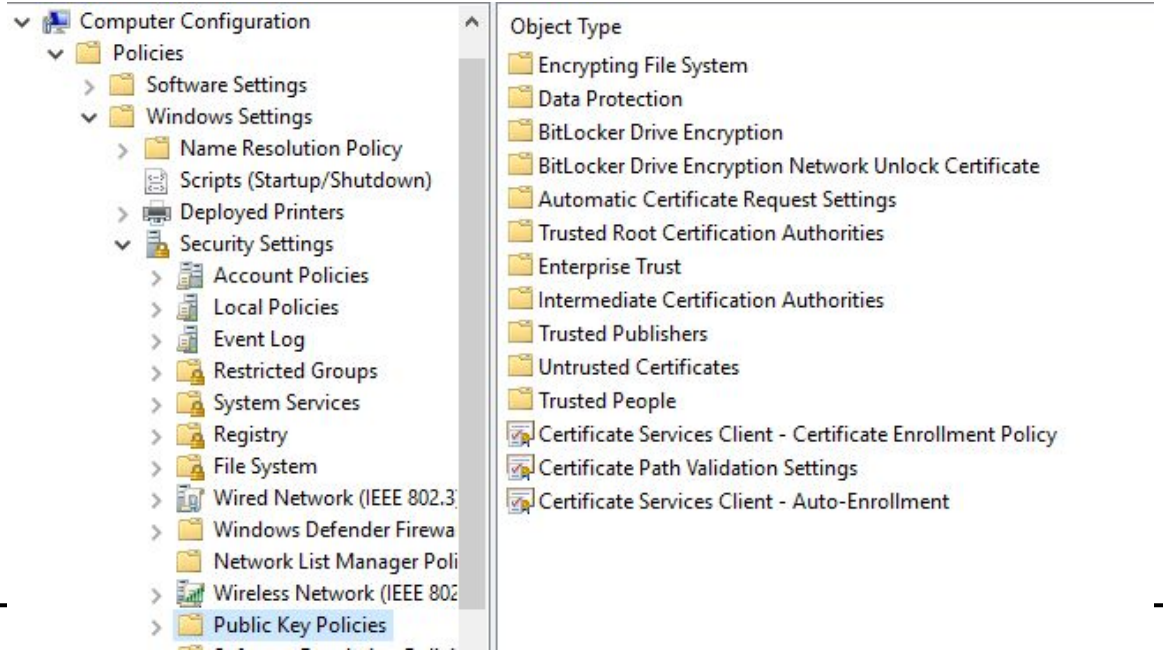
Creating a Certificate

Right-click your new GPO and click Edit.



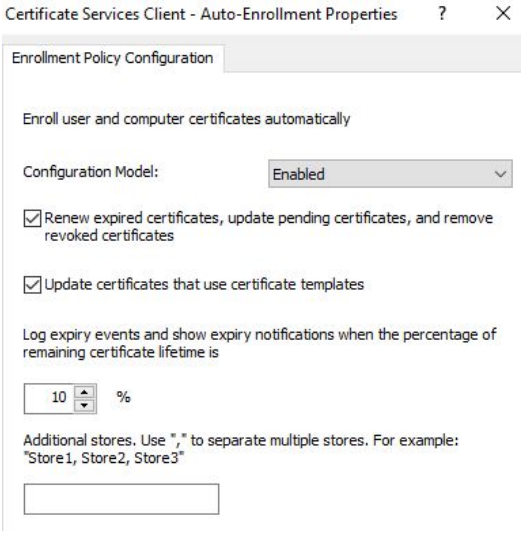
Creating a Certificate

Go to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Public Key Policies



Creating a Certificate

Double click Certificate Services Client - Auto Enrollment and set the configuration model to enable. Check both boxes.



Creating a Certificate

Hit apply and run gpupdate /force on your workstation and DC. If you go back to your Certificate Authority under Tools in Server Manager, then go to Issues Certificates, you should see your certificates issued to your workstation and DC.