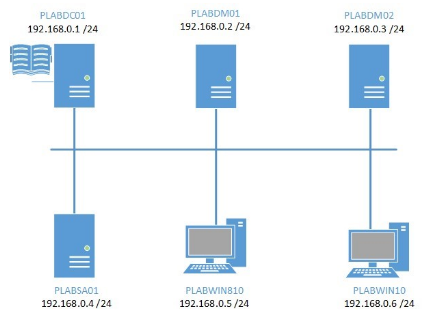
Mise en place d’un certificat racine

Public Key Infrastructure (PKI) is a set of policies and guidelines that control the creation, management, distribution and revocation of certificates (digital ID) in an organization.

Windows Server 2016 implement PKI using Active Directory (AD) Certificate Services. When AD Certificate Services is deployed in a corporate network, it is considered as an internal resource as most users who will request certificates are members of the organization. This type of resource is called an internal Certification Authority (CA). For companies that transact business with the public like e-commerce or internet banking, it will require the service of a trusted external CA to establish a trust with its customers.

The trusted CA proves the identity of an organization to the public as a trustworthy and legitimate business.

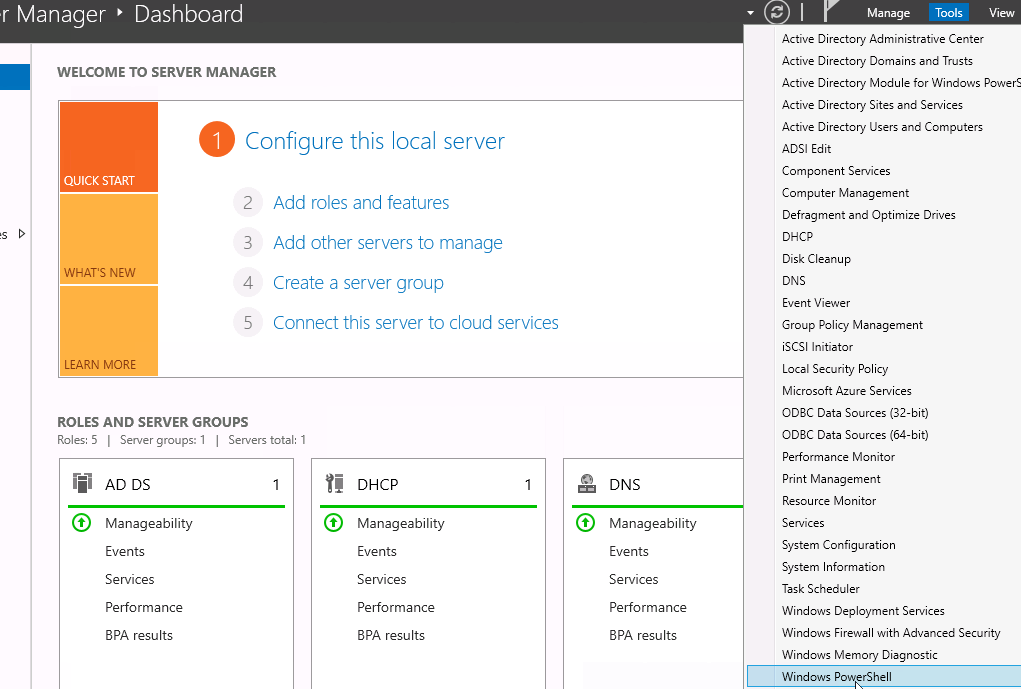


add then install a parent/root CA which is the starting point of a Windows PKI. The root CA generates a self-signed certificate. After which you will add, install a subordinate CA which forms a hierarchy and trust path with the root CA.

* Install AD Integrated Enterprise Certificate Authority (CA)
* Install Enterprise Subordinate CA
* Configure Certificate Revocation List (CRL) distribution points
* Configure CA backup and recovery

Launching powershell to add Active Directory Certificate Services and Certification Authority Web Enrollment features

In the **Server Manager > Dashboard**window, I click on the **Tools**menu and select **Windows PowerShell**.



Command lines:

Add-WindowsFeature -Name ADCS-Cert-Authority,ADCS-Web-Enrollment -IncludeManagementTools



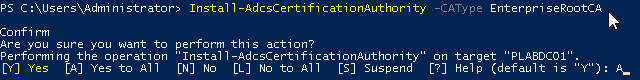
Once it is installed, it indicates a successful installation of features:



Now we have to make them capable of issuing certificates to a requesting user, computer or service.

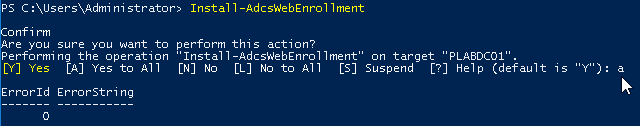
To install AD Certification Authority as an Enterprise Root CA using default settings, I type the following command:

Install-AdcsCertificationAuthority -CAType EnterpriseRootCA

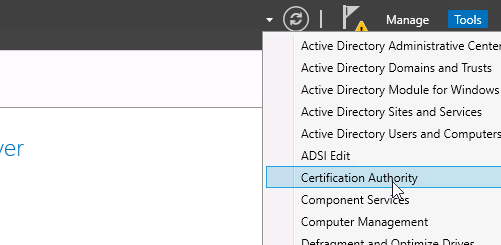


To install AD Certification Authority Web Enrollment I type:

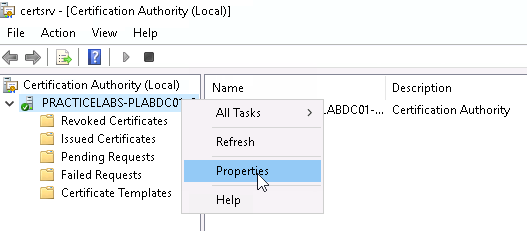
Install-AdcsWebEnrollment



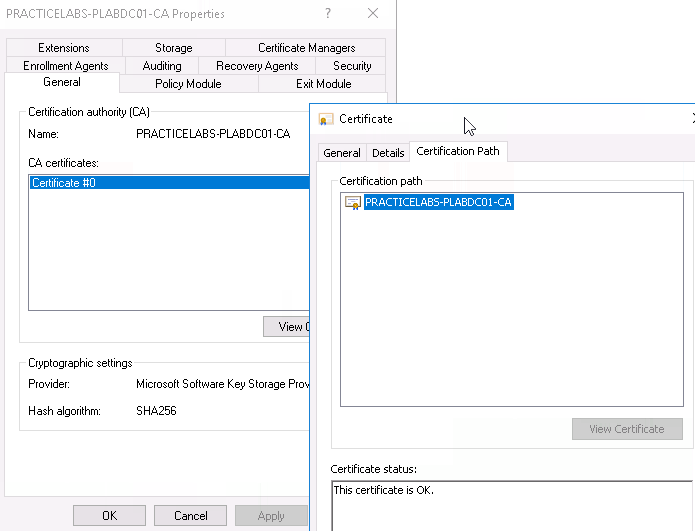
To verify that AD CS is working, we check in the **Server Manager > Dashboard**window, then to **Tools > Certification Authority**



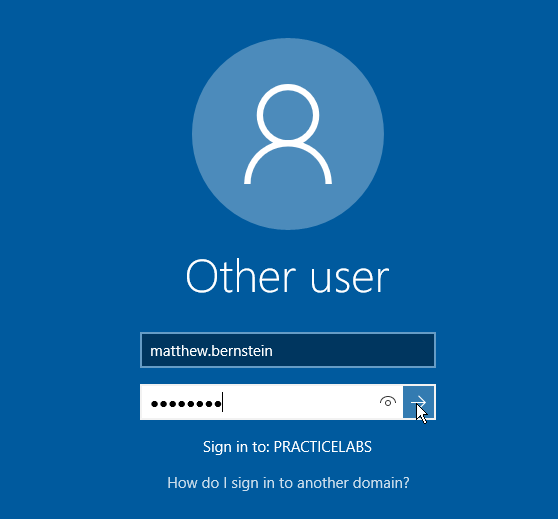
Once the **Certification Authority** windows appears, I click on the Practicelabs node and select **Properties.**

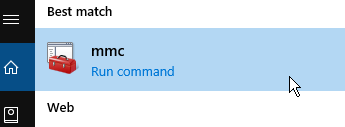


The **Certification Path**tab displays the relationship between **PRACTICELABS-PLABDC01-CA**which is the Root or Parent CA with **PRACTICELABS-PLABDM01-CA**which is the Subordinate CA.

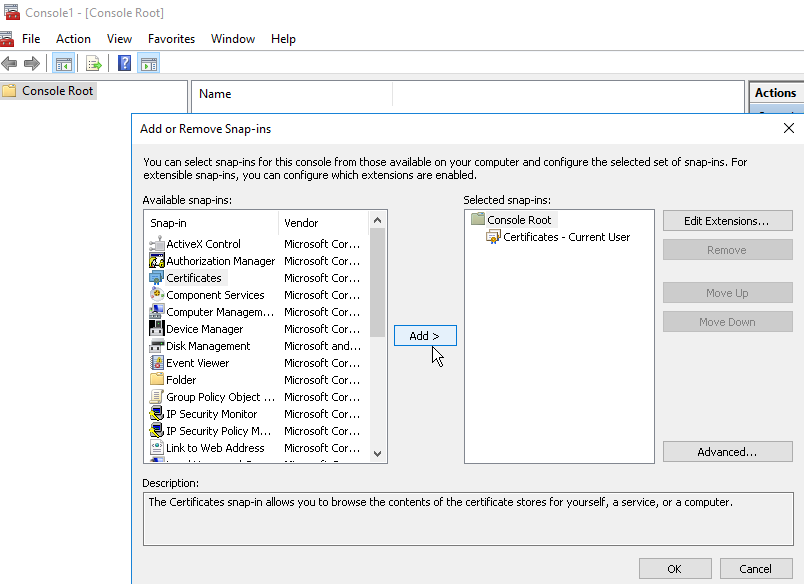


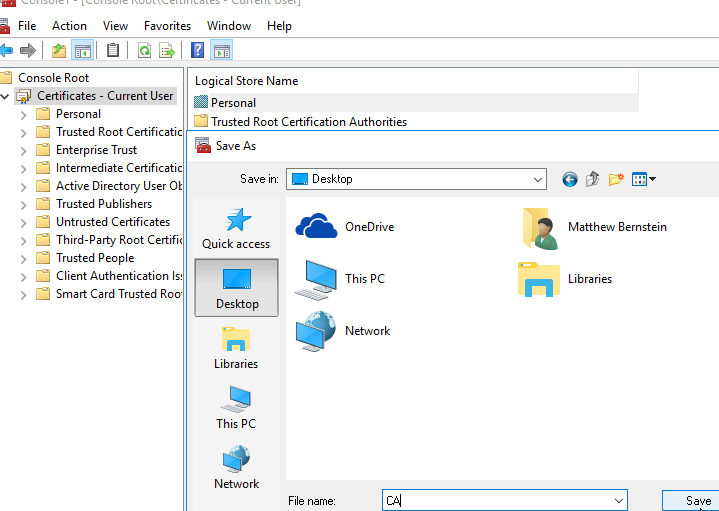
To request a certificate from a subordinate CA I sign out and logged in with a user account



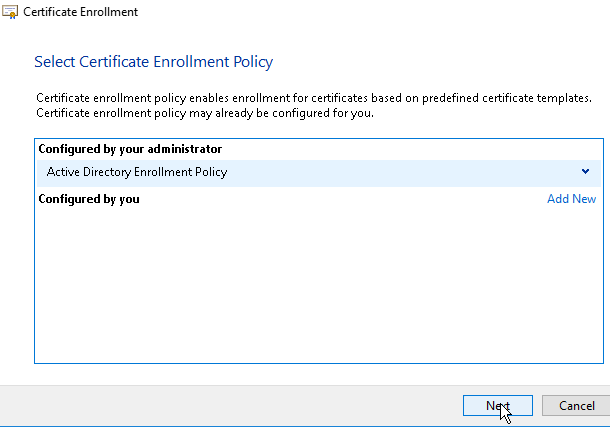


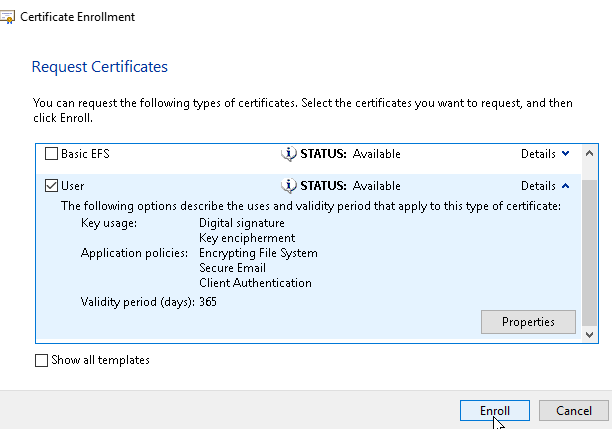
Launching Microsoft Management Console

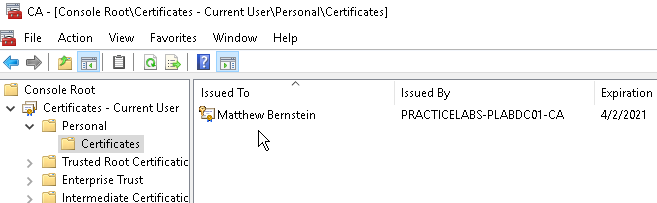
In the **Add or Remove Snap-in**dialog box, under the **Available snap-ins**box, click **Certificates**and click **Add**.

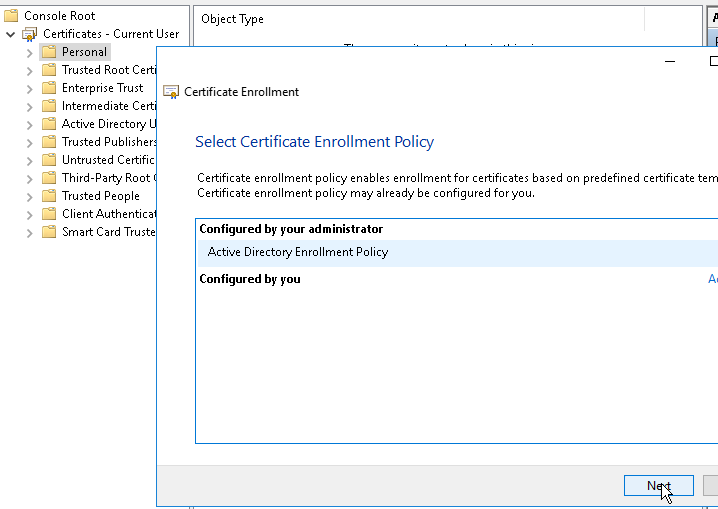


Once saved, I rebooted the distant machine and once back in the CMM requested a Certificate Enrollment









The certificate issued to **Matthew Bernstein**by **PRACTICELABS-PLABDM01-CA**which is the subordinate CA in the domain.