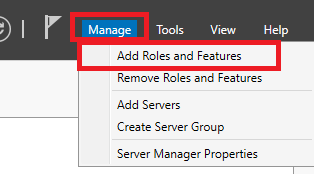
Summary

1. Select a hyper-visor of your choice. ESXi… Hyper-V…VMWare Workstation… anything!
2. Requires 2 VMs, both windows and joined to the same Windows domain. I will be using **DC01** and **DC02** for my example

Process:

1. While this is not a standard practice, I will be using my domain controller as a Root Certificate Authority.
2. Log into **DC01** as the Domain Administrator.
3. Open **Server Manager**, click on **Manage**, and **Add Roles and Features**  
    ****
4. Click **Next** on the **Before You Begin** wizard page.
5. For Installation Type, select **Role-based or feature-based installation** and click next  
     
   Graphical user interface, text, application, email

   Description automatically generated
6. On *Select Destination Server Screen*, Select **DC01** and click **Next**.  
     
   Graphical user interface, text, application, email

   Description automatically generated
7. On the *Select server roles* page, click the checkbox next to **Active Directory Certificate Services**  
     
   Text

   Description automatically generated
8. A pop-up window will appear, just click **Add Features** all this does is include the management tools needed for Certificate Services, which we would like to have.  
     
   Graphical user interface, text, application, email

   Description automatically generated
9. Once the pop-up window closes, click next.  
     
   Graphical user interface, text, application

   Description automatically generated
10. On the *Select Features* page, just click **Next**.  
      
    Graphical user interface, text, application

    Description automatically generated
11. On the first *Active Directory Certificate Services* page, it will warn that the name and domain settings of **DC01** cannot be changed after Certificate Authority is installed. This includes things such as joining a domain, promoting a server to a domain controller, changing the name etc. Acknowledge this by clicking on **Next**.  
      
    Graphical user interface, text, application, Word

    Description automatically generated
12. On the *Select Role Services*page for ADCS, you will find that **Certification Authority** is selected, but you also want to include **Certificate Enrollment Web Services** and **Certification Authority Web Enrollment** for a later lab. When checking both boxes, a pop-up window will open, just click **Add Feature** on each to check the boxes.  
      
    1. Graphical user interface, text, application

       Description automatically generated
    2. Click Add Features (for both checkboxes)  
         
       Graphical user interface, text, application

       Description automatically generated
    3. Once all three are checked, click on **Next**  
         
       Graphical user interface, text, application

       Description automatically generated
13. On *Web Server Role (IIS)* page, click **Next**  
      
    Graphical user interface, text, application, email

    Description automatically generated
14. On the *Select Role Services* page for the Web Server Role (IIS) just click on **Next**.  
      
    Graphical user interface, application

    Description automatically generated
15. Finally, on the *Confirmation* page, click on **Install**.  
      
    Graphical user interface, text, application

    Description automatically generated
16. Once the installation has finished, we will need to configure the Active Directory Certificate Services itself. Click on the blue hyperlink in the window.  
      
    Graphical user interface, text, application

    Description automatically generated
17. On the *Credentials* page, keep the default Domain Administrator credentials present and click **Next**.  
      
    Graphical user interface, application, Word

    Description automatically generated
18. For the Roles and Services to configure, select **Certification Authority** just for now and then click **Next**.  
      
    Graphical user interface, application, Word

    Description automatically generated
19. For the Setup Type, select **Enterprise CA**, and then click **Next**.  
      
    Graphical user interface, text, application

    Description automatically generated
20. For the **CA Type**, we want to select **Root CA**, since this is the first and new certifying authority within our Windows Domain.   
      
    Graphical user interface, text, application, Word

    Description automatically generated
21. For the **Private Key** we want to create a new private key, and click **Next**.  
      
    Graphical user interface, text, application

    Description automatically generated
22. For the **Cryptography for CA** page, you can keep it as default. Just make sure it is **SHA256** and the key length is **2048**. Click **Next** when you confirm the following is set.  
      
    Graphical user interface, application

    Description automatically generated
23. For the **CA Name**, keep everything as default for simplicity. The common name can be changed, but the name entered suits me fine. Click on **Next**.  
      
    Graphical user interface, text, application

    Description automatically generated
24. For the **Validity Period**, keep it as default. Unless you are aligning to a setting defined in a project plan, on the job, in the real-world, just keep this set at default, which is currently **5 years**. Click **Next** when finished reviewing.  
      
    Graphical user interface, text, application

    Description automatically generated
25. For **CA Database** for now, keep it default. Again, this may look different on the job.  
      
    Graphical user interface, text, application, email

    Description automatically generated
26. On the **Confirmation Page** go ahead and click **Configure** to finish the configuration.  
      
    Graphical user interface, text, application

    Description automatically generated
27. The configuration should take no more than 10 seconds in our lab setting. Once it is finished, click on **Close**.   
      
    Graphical user interface, text, application

    Description automatically generated
28. A small pop-up may appear asking if you want to configure the other two services, click **NO** for now.  
      
    Graphical user interface, text, application

    Description automatically generated
29. If the Role Installation wizard is still open, click on **Close**.  
      
    Graphical user interface, text, application

    Description automatically generated
30. Go ahead and close the **Server Manager** window as well.  
      
    (Lab continues on next page)
31. On the bottom left-hand side of the desktop where it says “Type Here To Search,” enter, **certsrv.msc**, it should result in the search window opening showing the Certificate Authority MMC console shortcut. This can also be opened via **Run** or found in **Windows Administrative Tools > Certification Authority**. Likewise, go ahead and open the **Certification Authority** however you like.  
      
    Graphical user interface, text, application

    Description automatically generated
32. You should see an MMC console open with **Certification Authority (Local)** on the left side in the navigation bar. Under that should be your local Certification Authority that you just installed. Drill down by clicking the arrow to the left of **ad-DC01-CA**.  
      
    Graphical user interface, text, application

    Description automatically generated
33. The navigation tree should now show 5 different folders, Revoked Certificates, Issued Certificates, Pending Requests, Failed Requests and Certificate Templates. Click on **Issued Certificates**.  
      
    Graphical user interface, text, application

    Description automatically generated
34. If you have the second virtual machine setup and it is joined to the domain, it should automatically be issued a certificate.   
      
    Graphical user interface, text, application

    Description automatically generated
35. Log into your other VM, in my case it is **DC02**.  
    (Lab continues on next page)
36. Open **certlm.msc** via run or the Windows Search bar on the bottom left. This can also be found in MMC via a snap-in called **Certificates**, but make sure to select the **Computer Account** if you are using the snap-in option. When you open **certlm.msc** drill down in the navigation tree **Certificates – Local Computer > Trusted Root Certification Authority > Certificates**  
      
    Graphical user interface, text, application

    Description automatically generated
37. You should see the **ad-DC01-CA** certificate within this folder. This was automatically distributed to this VM which is **DC02**, from the Root CA from **DC01**.   
      
    Text

    Description automatically generated
38. **Documentation continues on next page. This is to prepare you for the Windows Update Services Lab Later On.**
39. On my Root CA server **DC01**, I logged in and opened **Microsoft Management Console** (MMC).  
    1. Right-Click the Start Button and click on **Run**
    2. Type **MMC**Graphical user interface, text, application, email

       Description automatically generated
    3. Press **ENTER**
40. This will open a blank window. Go to **File > Add/Remove Snap-in** or use key combination **CTRL+M**.  
      
    Graphical user interface, text, application

    Description automatically generated
41. Click on **Certificate Templates** in the left side of the window, click **Add** so it appears on the right-side. Then click **OK**.  
      
    Graphical user interface

    Description automatically generated
42. Your MMC window will now have the snap-in called **Certificate Templates**, go ahead and click on it in the navigator.  
      
    Graphical user interface, application, Word

    Description automatically generated
43. It should now populate the center screen of the console with the **Certificate Templates**, scroll down to find **Web Server**, right-click and click **Duplicate**.  
      
    Graphical user interface, application

    Description automatically generated
44. A properties window will appear. Click on the **General** tab and fill in the following:  
    1. Template Display Name: **JY Web Server Template** (replace JY with your initials)
    2. Template Name: (this will auto populate, don’t change it)
    3. Validity Period: **5 Years**
    4. Ensure **Publish certificate in Active Directory** is **CHECKED** in it’s box.
    5. Do not click apply yet, please confirm with the photo on the next page.
45. Validate the instructions you just followed here, do not click apply just yet, we need to modify one more thing.Graphical user interface, text, application, email

    Description automatically generated
46. Click on the **Security Tab** next within the properties window:  
    1. Click on **Domain Admins** to ensure it is highlighted
    2. Below where it says *Permissions for Domain Admins* make sure the following is checked under **Allow**:
       1. Read
       2. Write
       3. Enroll
       4. Auto-Enroll
    3. Read, Write and Enroll should already be checked but make sure to check the **Auto-Enroll** checkbox for allow.
    4. Do not click apply yet, review my picture on the next page
47. Review the Security settings below  
      
    A picture containing graphical user interface

    Description automatically generated
48. Once you have confirmed the **General** and **Security** tab settings, click on **Apply** and then on **OK**. This should create the new template and you should see it populate on the MMC console window.  
      
    Background pattern, icon

    Description automatically generated
49. You are now complete with the lab. You installed a certificate authority role on a Windows Server, confirmed that it was handing out a basic certificate to domain devices and configured a custom Web Server template that you can use later on to request certificates for an internal domain.
50. **Key Takeaways:**
    1. A Root CA server/role/service should not be installed on a Domain Controller in a production environment. However, others in the industry may justify it in certain circumstances. I.E., Saving money on Windows Licensing. Which is ok.
    2. For best practices, you want to install the Active Directory Certificate Services on a member server with no other roles on it so that it is dedicated to performing that one task. [**You can also add redundancy by installing ADCS on two servers and configuring Failover Cluster Manager.**](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc742450(v=ws.10)?redirectedfrom=MSDN)
    3. The true reason to have an Active Directory Certificate Services role available in a Windows Domain environment is to allow you to encrypt all your internal network traffic, files, emails and to establish an on-premises PKI.
    4. Your Security team may yell at you if the Domain Admins Security group has access to auto-enroll certificates. I recommend that you create a different Security group in Active Directory to lock down auto-enroll to those who only need it and not all Domain Administrators. Assign the security group as needed and take away as needed. Only a very selective list of System Administrators need access to create and enroll certificates.
    5. A key feature of the auto-enroll that will assist you in saving time is when you Domain Join a new Windows device, when you perform the action as a Domain Administrator, your credentials also allows for the backend automation to assign and distribute a certificate from the Root CA server to the device so that is entrusted by other Windows domain devices on the network.