

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use. [Learn more](#)



Step-By-Step: Migrating The Active Directory Certificate Service From Windows Server 2003 to 2012 R2

★★★★★



MVP Dishan Francis November 11, 2014

17

2

0

Time for an upgrade.



#CANITPRO

As you may be aware, support for both Windows Server 2003 and 2003 R2 is coming to end on July 14th 2015. With this in mind, IT professionals are in midst of planning migration. This guide will provide steps on migrating AD CS from Windows Server 2003 to Windows Server 2012 R2.

In this demonstration I am using following setup.

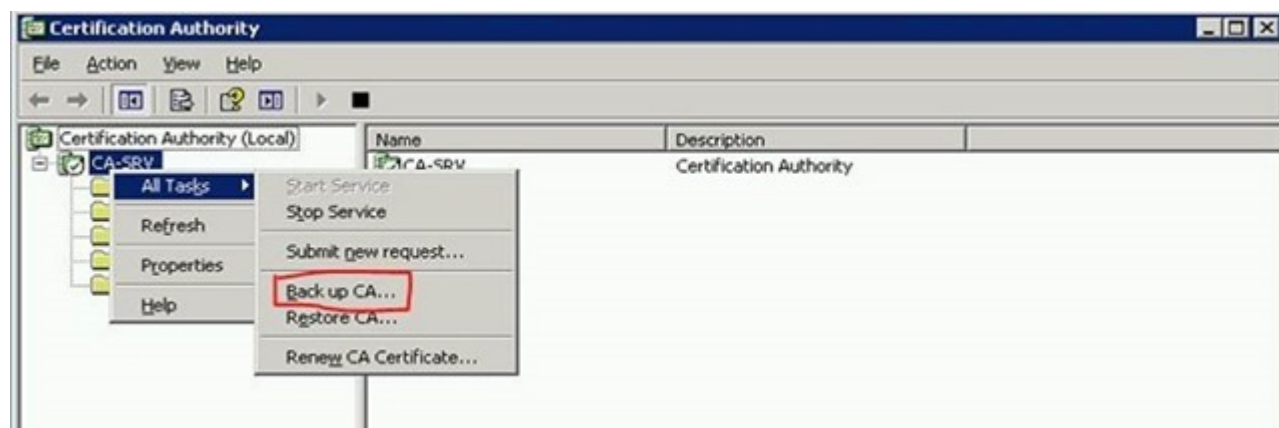
Server Name	Operating System	Server Roles
canitpro-casrv.canitpro.local	Windows Server 2003 R2 Enterprise x86	AD CS (Enterprise Certificate Authority)
CANITPRO-DC2K12.canitpro.local	Windows Server 2012 R2 x64	-

Step 1: Backup Windows Server 2003 certificate authority database and its configuration

1. Log in to Windows 2003 Server as member of local administrator group
2. Go to Start > Administrative Tools > Certificate Authority



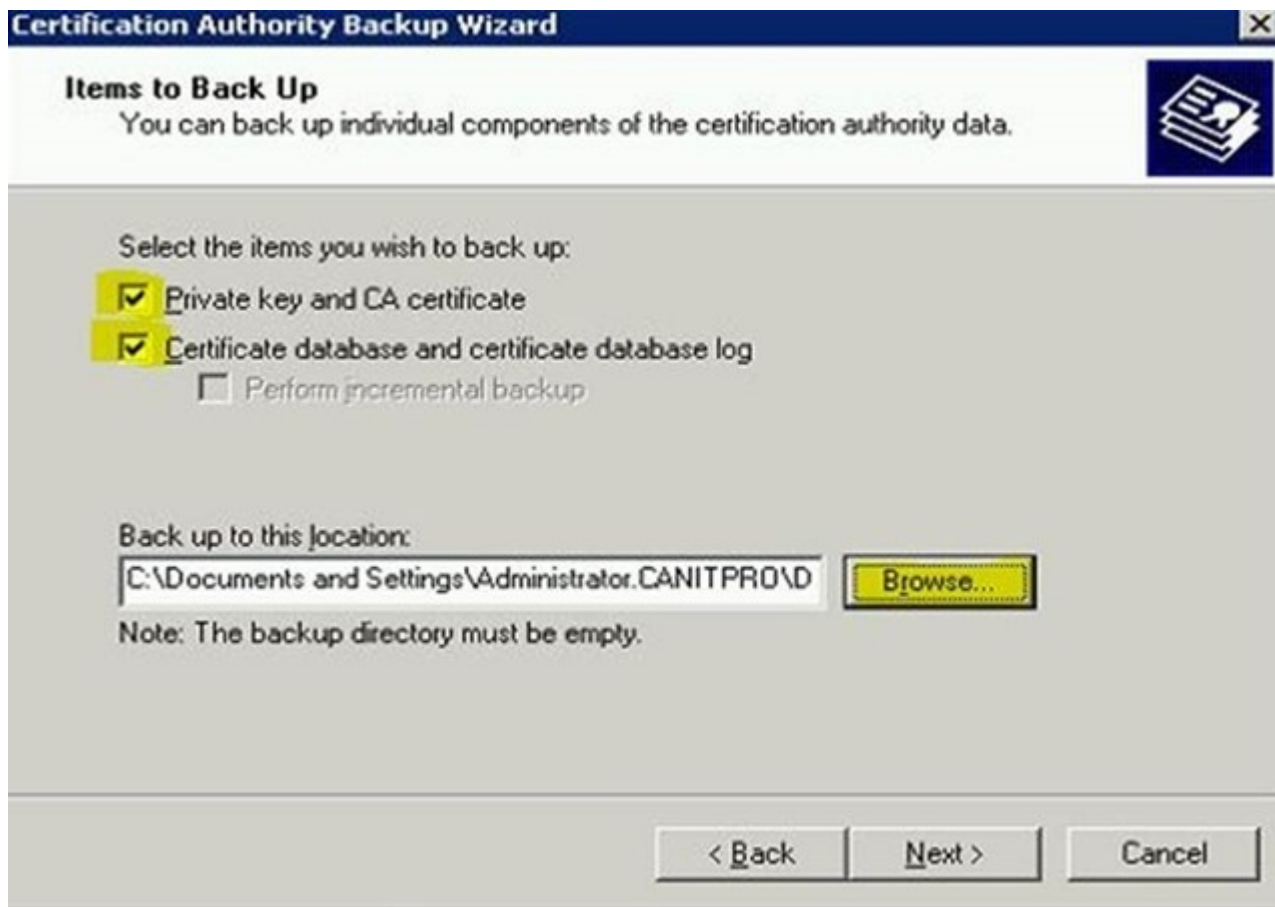
3. Right Click on Server Node > All Tasks > Backup CA



4. Then it will open the “Certification Authority Backup Wizard” and click “Next” to continue



5. In next window click on check boxes to select options as highlighted and click on “Browse” to provide the backup file path location where it will save the backup file. Then click on “Next” to continue



Certification Authority Backup Wizard

Items to Back Up
You can back up individual components of the certification authority data.

Select the items you wish to back up:

- ☒ Private key and CA certificate
- ☒ Certificate database and certificate database log
- ☐ Perform incremental backup

Back up to this location:
C:\Documents and Settings\Administrator\CANITPRO\D **Browse...**

Note: The backup directory must be empty.

< Back Next > Cancel

6. Then it will ask to provide a password to protect private key and CA certificate file. Once provided the password click on next to continue



Certification Authority Backup Wizard

Select a Password
For encryption and decryption of messages, both a public key and a private key are required. You must supply a password for the private key.

This password is required to gain access to the private key and the CA certificate file.

Password:
[password field]

Confirm password:
[password field]

To maintain private key security, do not share your password.

< Back **Next >** Cancel

7. In next window it will provide the confirmation and click on “Finish” to complete the process

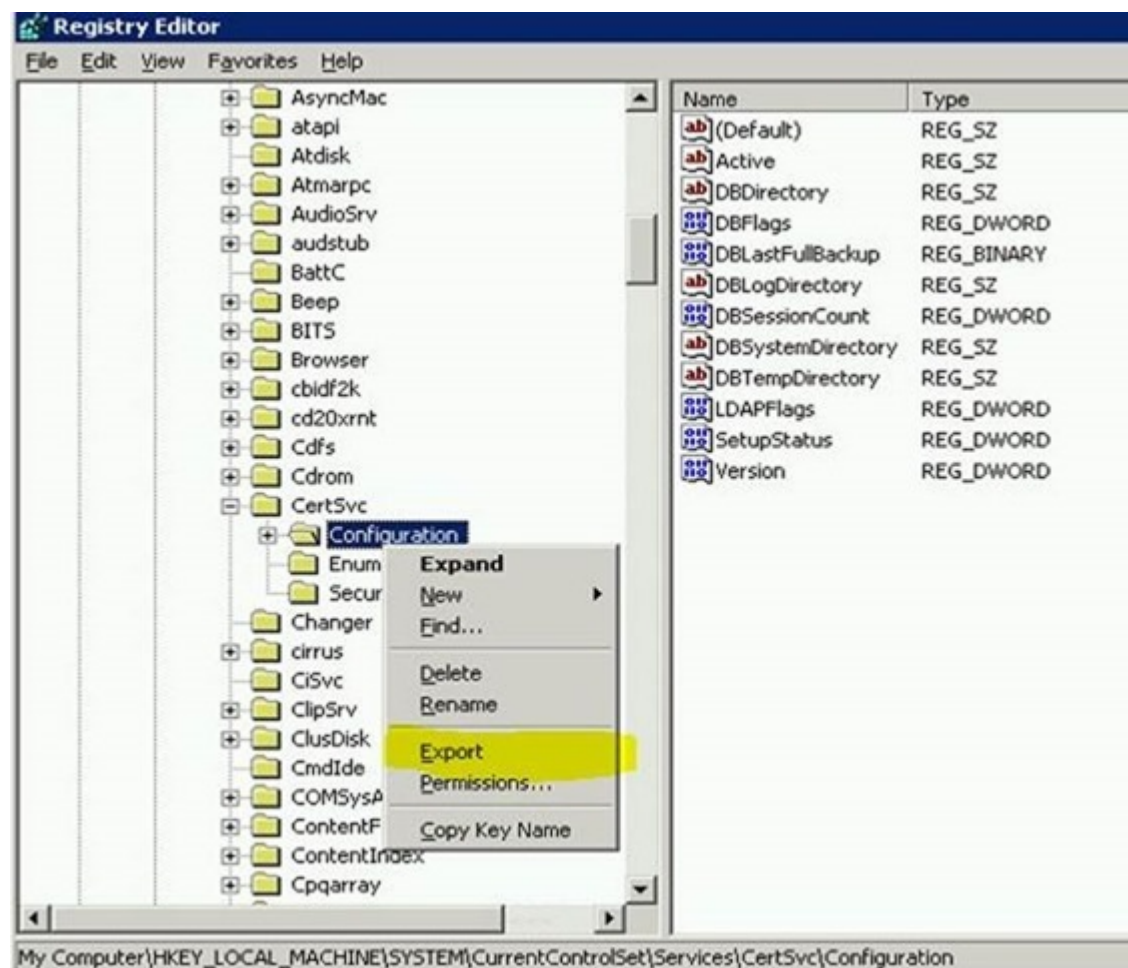
Step 2: Backup CA Registry Settings

1. Click Start > Run and then type **regedit** and click “Ok”

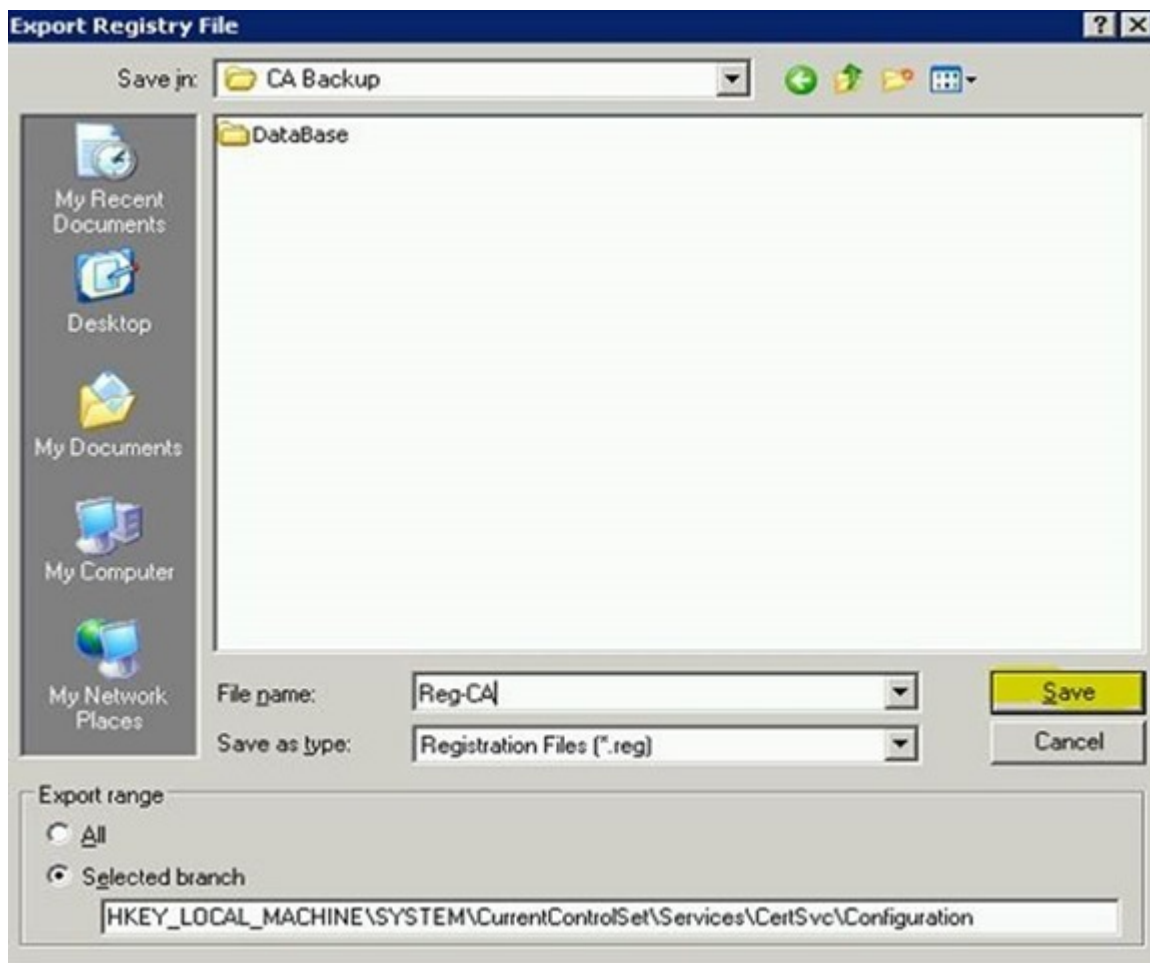


2. Then expand the key in following path **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc**

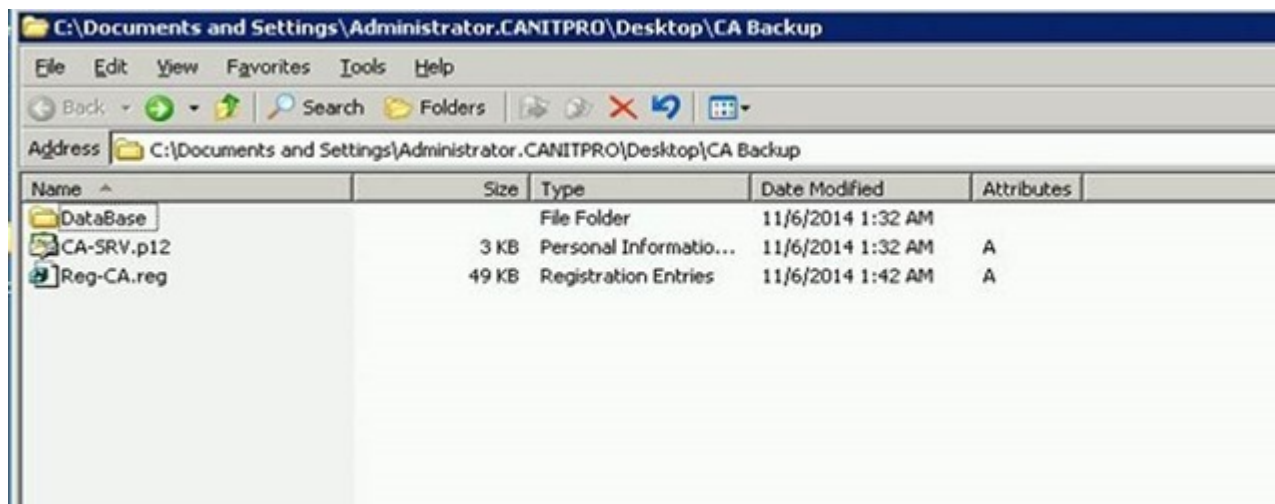
3. Right click on “Configuration” key and click on “Export”



4. In next window select the path you need to save the backup file and provide a name for it. Then click on save to complete the backup



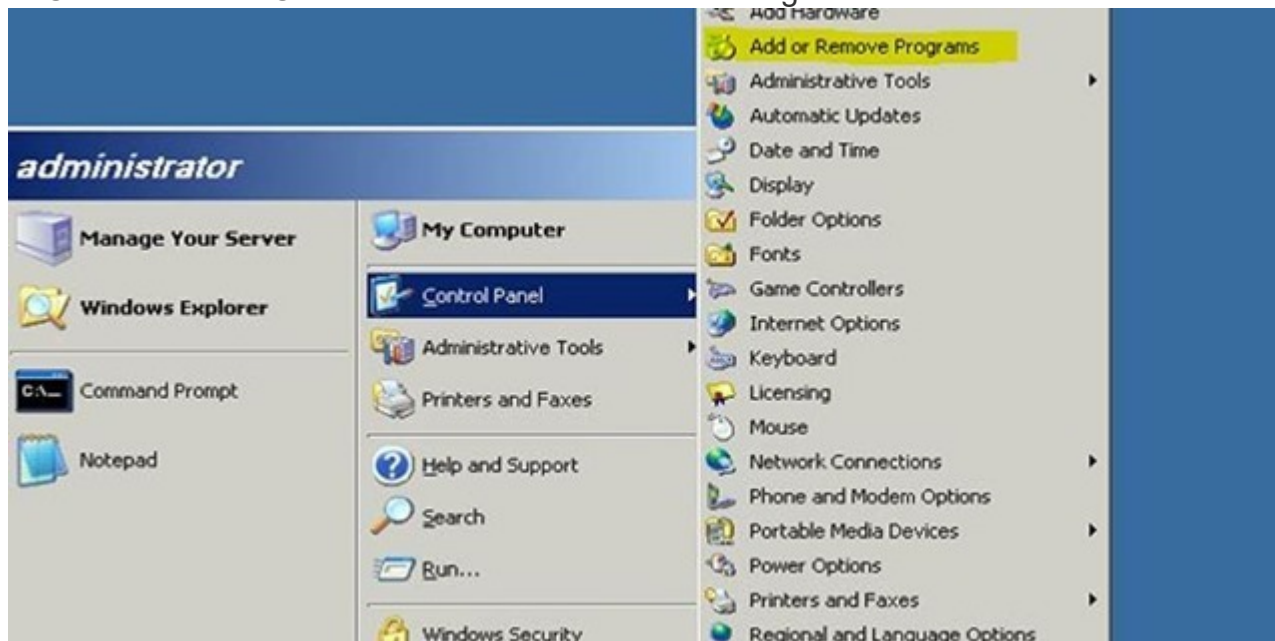
Now we have the backup of the CA and move these files to the new windows 2012 R2 server.



Step 3: Uninstall CA Service from Windows Server 2003

Now we have the backup files ready and before configure certificate services in new Windows Server 2012 r2, we can uninstall the CA services from windows 2003 server. To do that need to follow following steps.

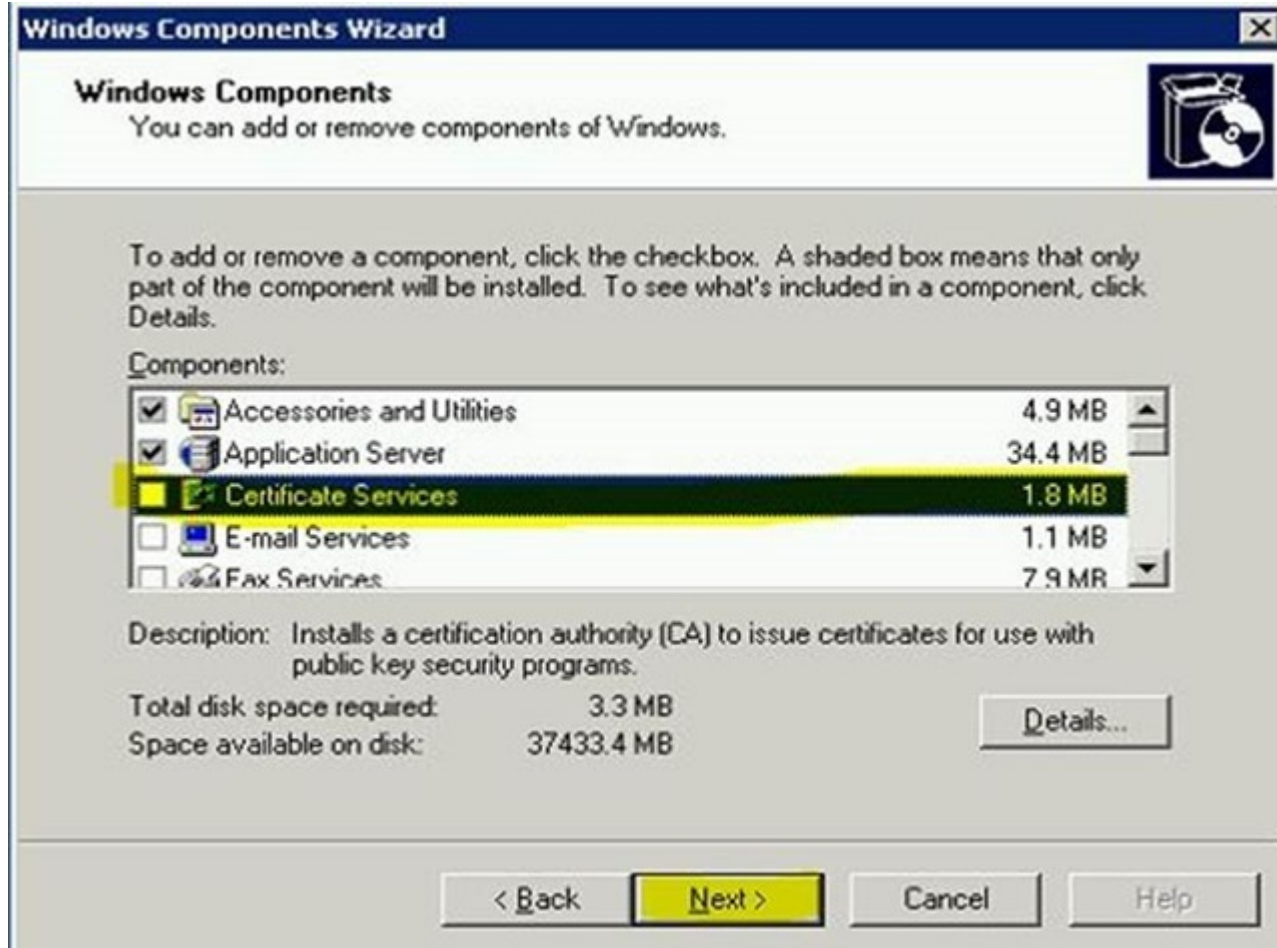
1. Click on Start > Control Panel > Add or Remove Programs



2. Then click on “Add/Remove Windows Components” button



3. In next window **remove** the tick in “Certificate Services” and click on next to continue



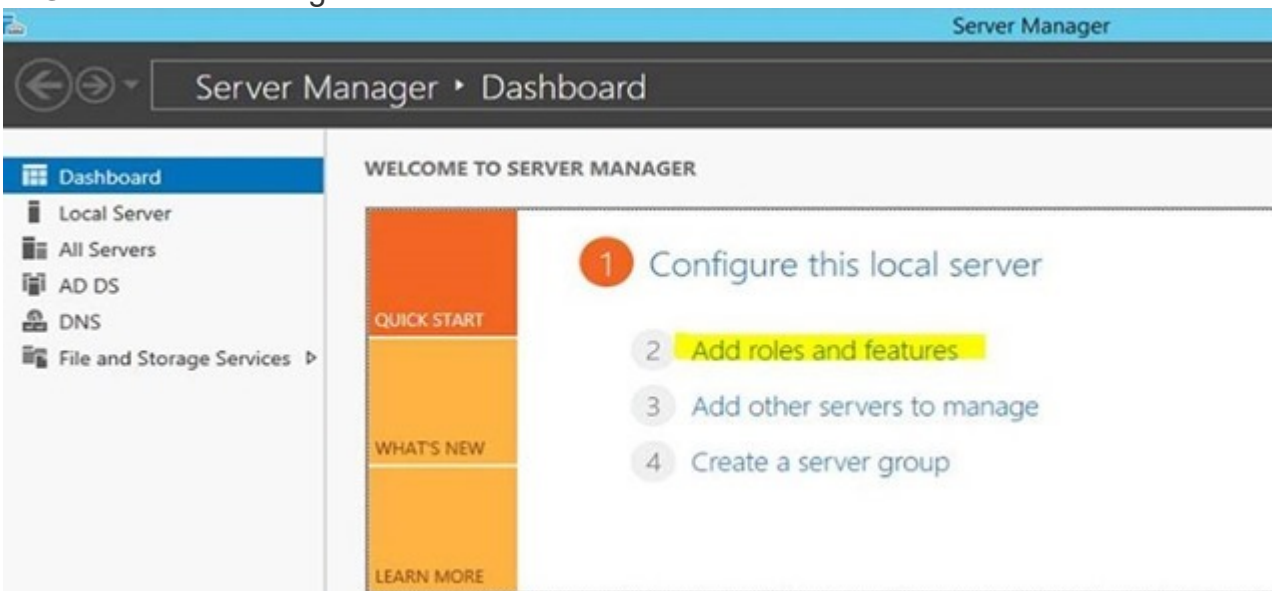
4. Once its completed the process it will give the confirmation and click on “Finish”



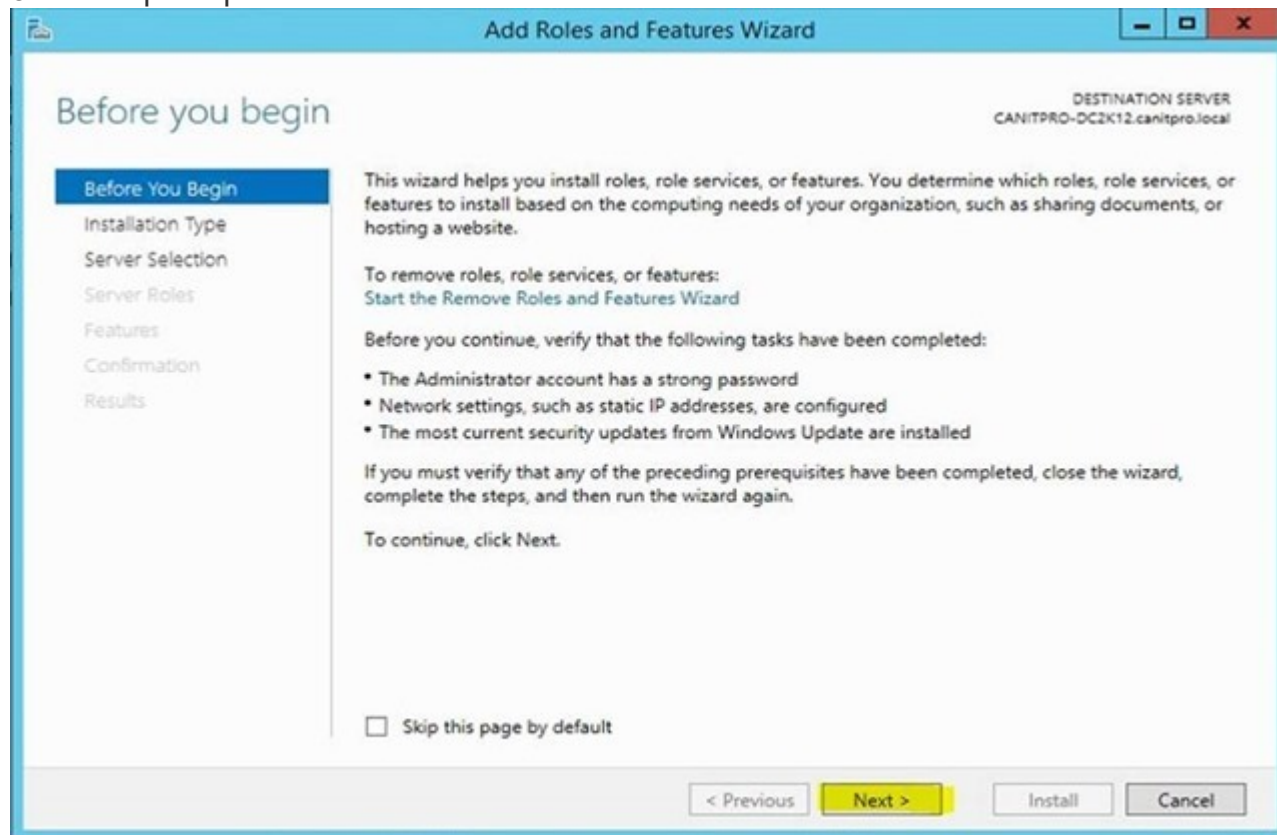
With it we done with Windows Server 2003 CA services and next step to get the Windows Server 2012 CA services install and configure.

Step 4: Install Windows Server 2012 R2 Certificate Services

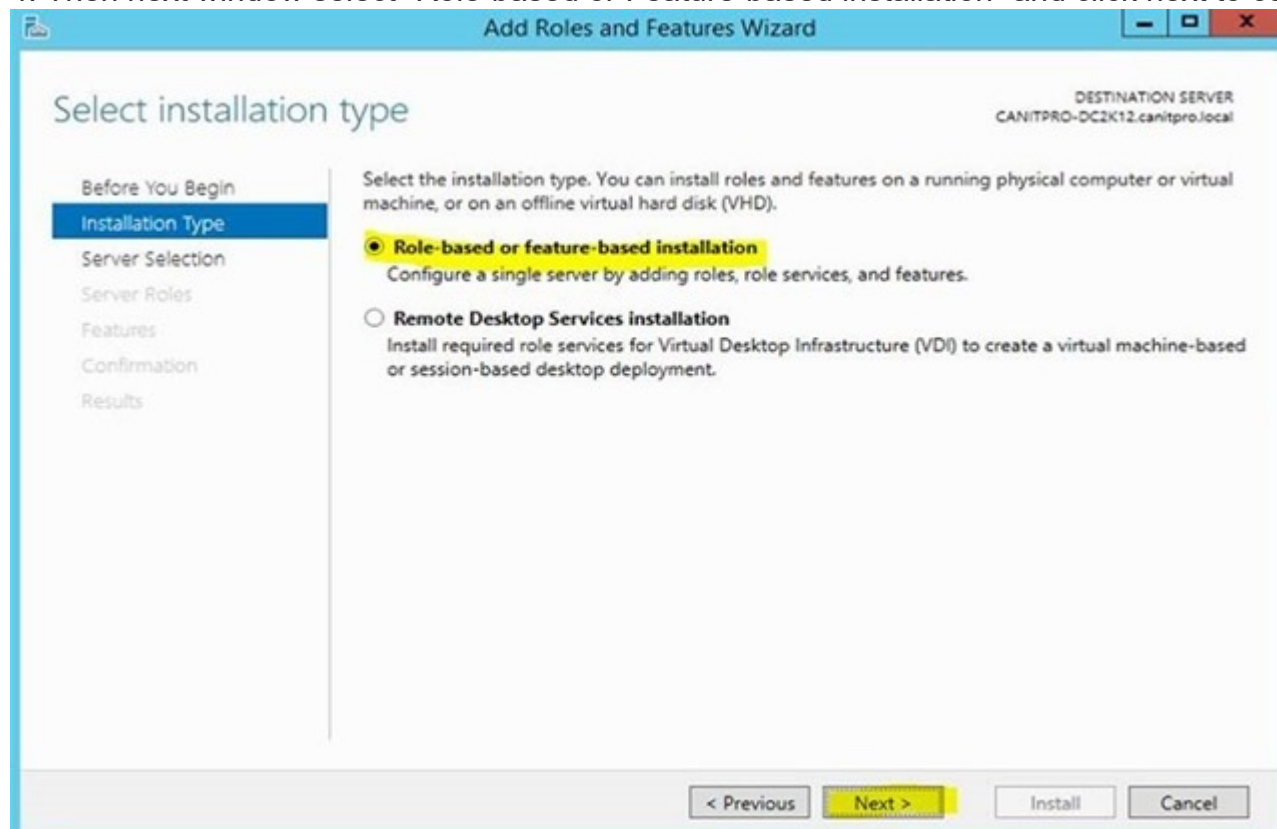
1. Log in to Windows Server 2012 as Domain Administrator or member of local administrator group
2. Go to Server Manager > Add roles and features



3. It will open up “Add roles and feature” wizard and click on next to continue



4. Then next window select “Role-based or Feature-based installation” and click next to continue



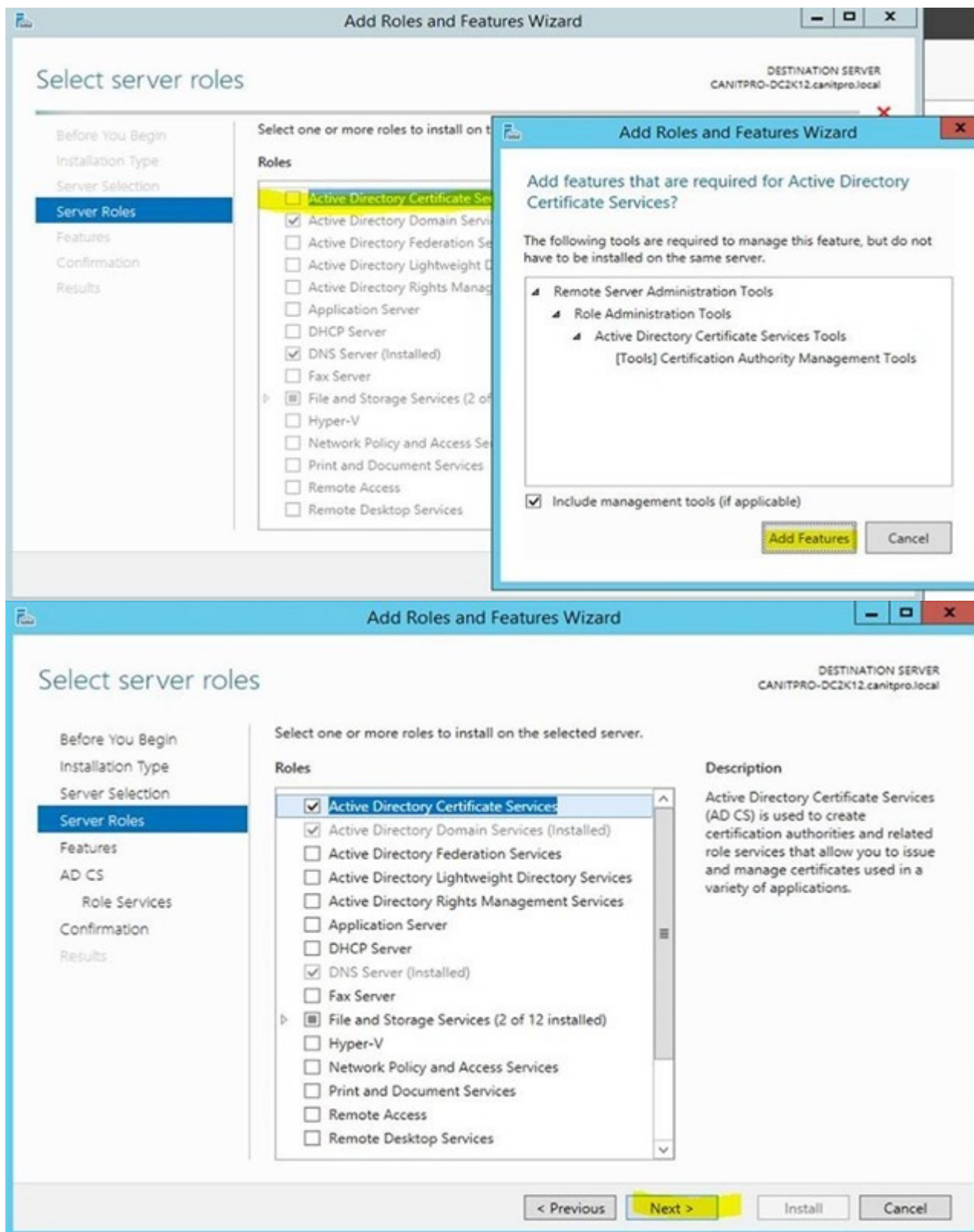
5. From the server selections keep the default selection and click on next to continue

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. In the top right corner, it says 'DESTINATION SERVER' and 'CANITPRO-DC2K12.canitpro.local'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection' (which is highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the text 'Select a server or a virtual hard disk on which to install roles and features.' Below this, there are two radio buttons: 'Select a server from the server pool' (which is selected) and 'Select a virtual hard disk'. Below the radio buttons is a section titled 'Server Pool'. It contains a 'Filter:' text box. Below the filter box is a table with the following data:

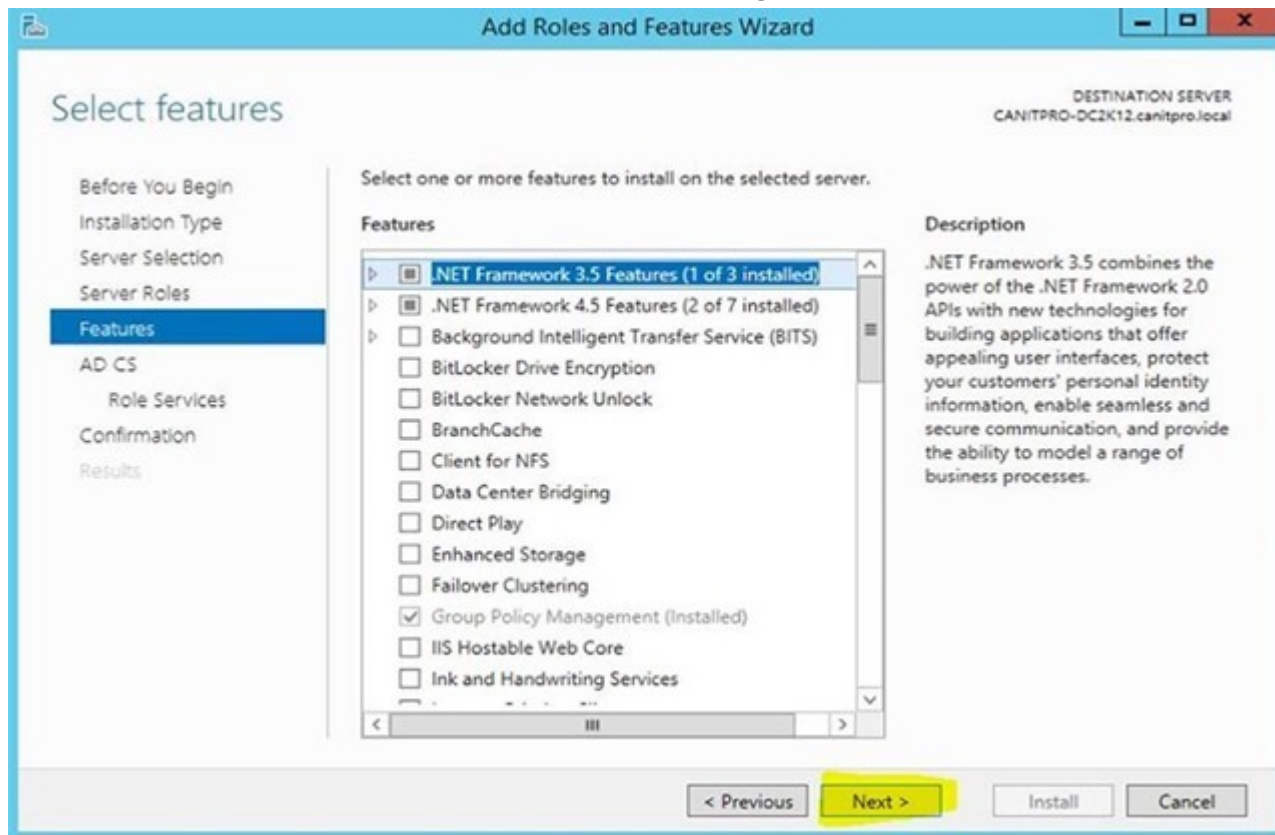
Name	IP Address	Operating System
CANITPRO-DC2K12.canitpro.local	38.117.80.124	Microsoft Windows Server 2012 R2 Standard

Below the table, it says '1 Computer(s) found'. Below that, it says 'This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom of the window, there are four buttons: '< Previous', 'Next >' (which is highlighted in yellow), 'Install', and 'Cancel'.

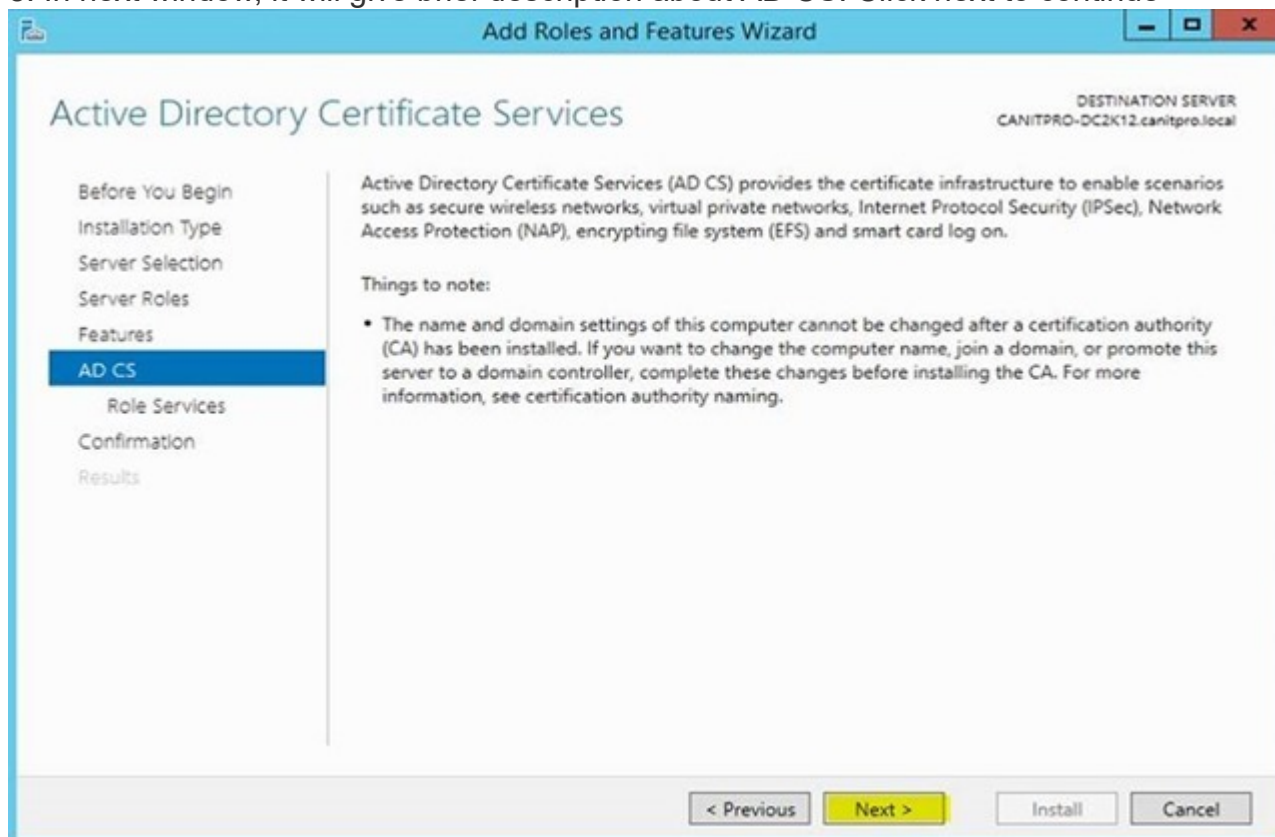
6. In next window click on tick box to select “Active Directory Certificate Services” and it will pop up with window to acknowledge about required features need to be added. Click on add features to add them



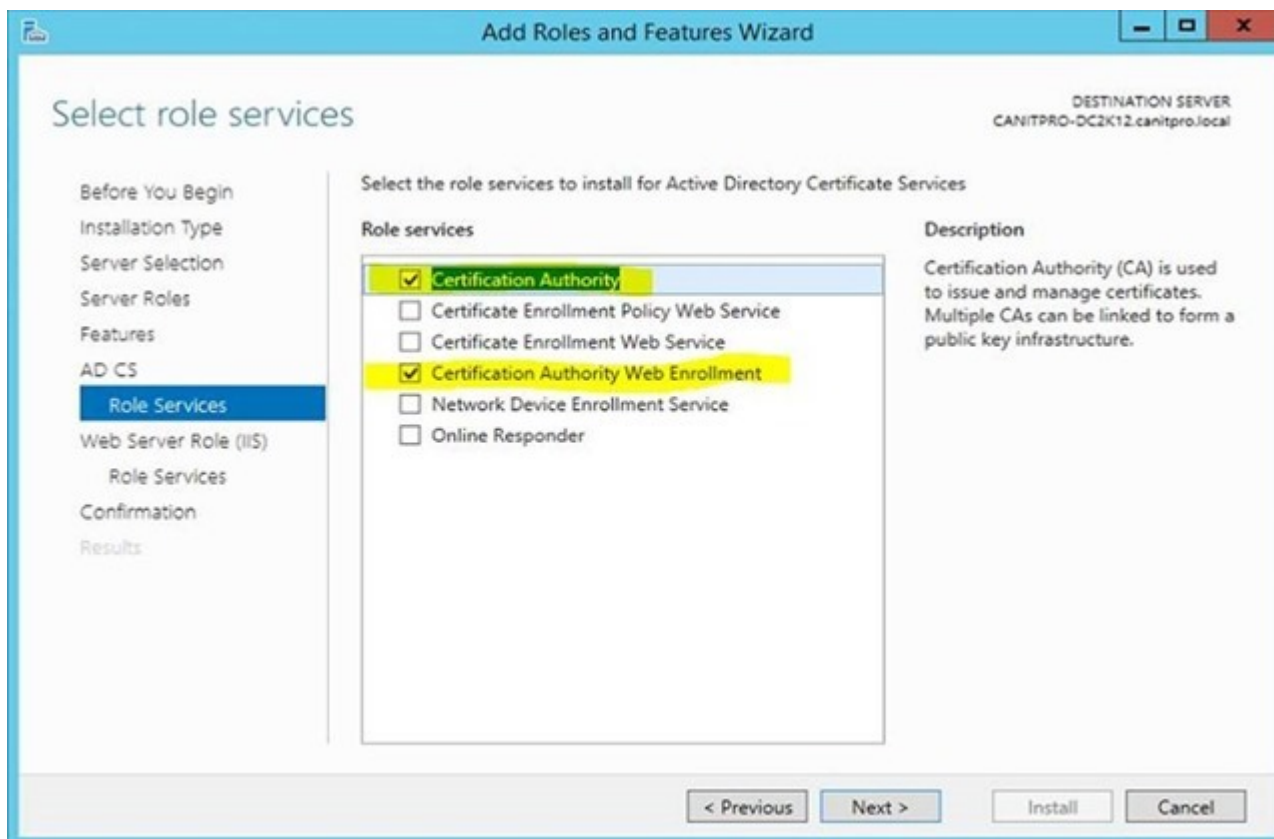
7. Then in features section will let it run with default. Click next to continue



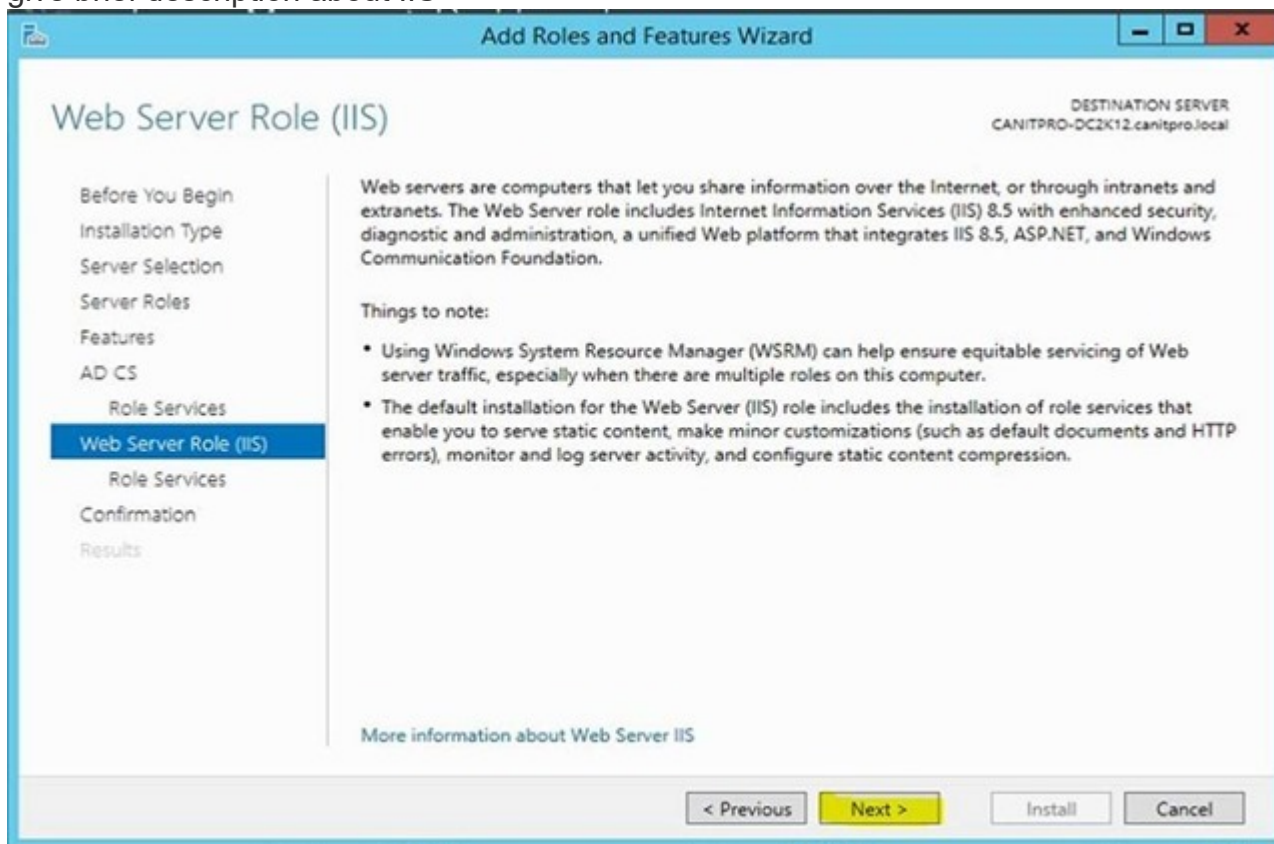
8. In next window, it will give brief description about AD CS. Click next to continue



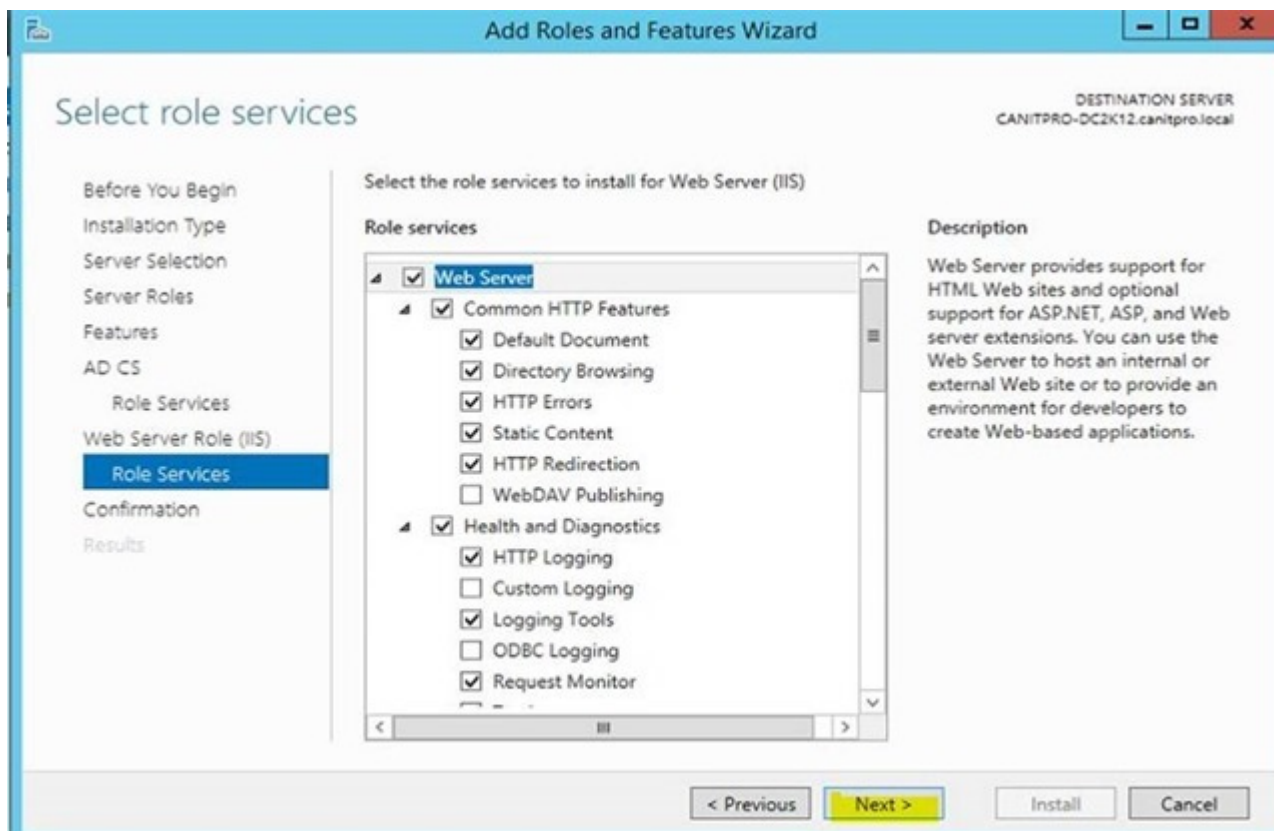
9. Then it will give option to select roles services. I have selected Certificate Authority and Certification Authority Web Enrollment. Click next to continue



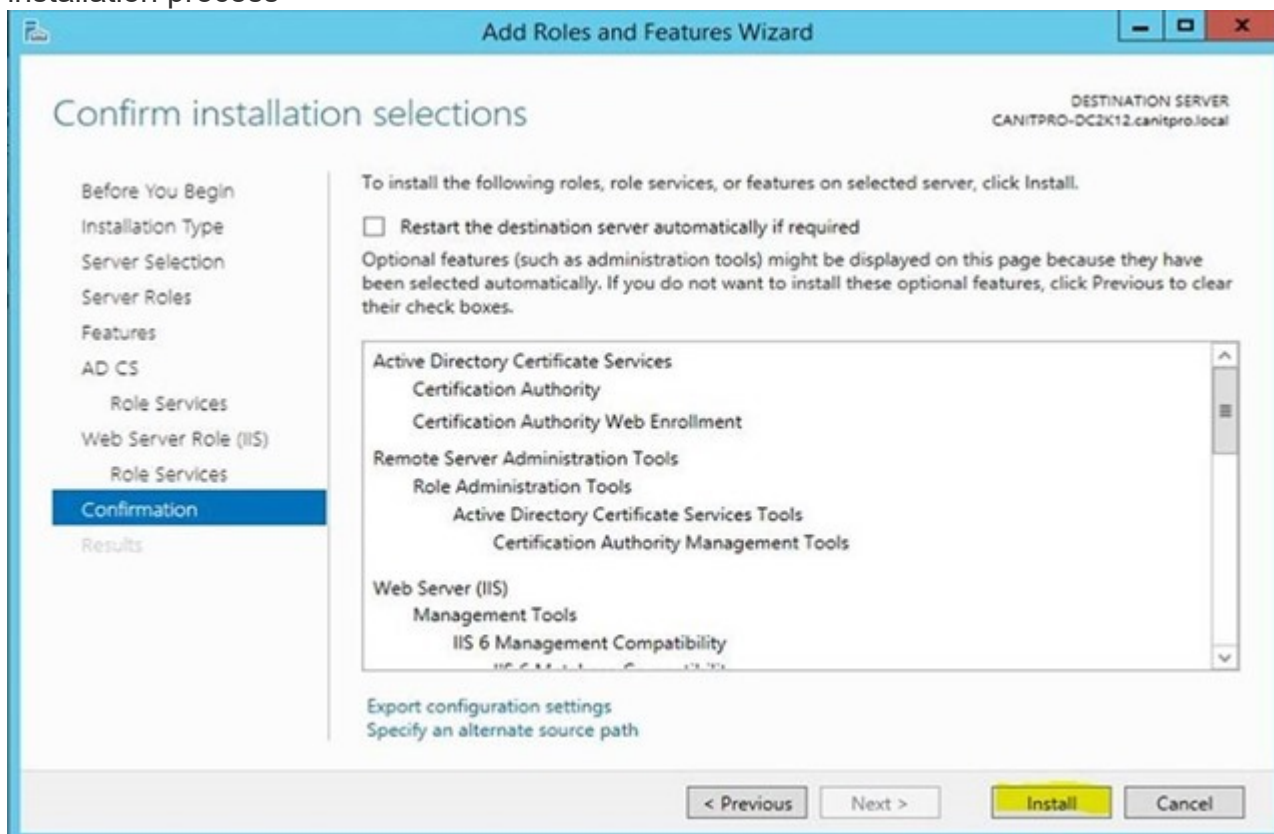
10. Since Certification Authority Web Enrollment selected it will required IIS. So next window it will give brief description about IIS



11. Then in next window it gives option to add IIS role services. I will leave it default and click next to continue



12. Next window will give confirmation about service install and click on “Install” to start the installation process

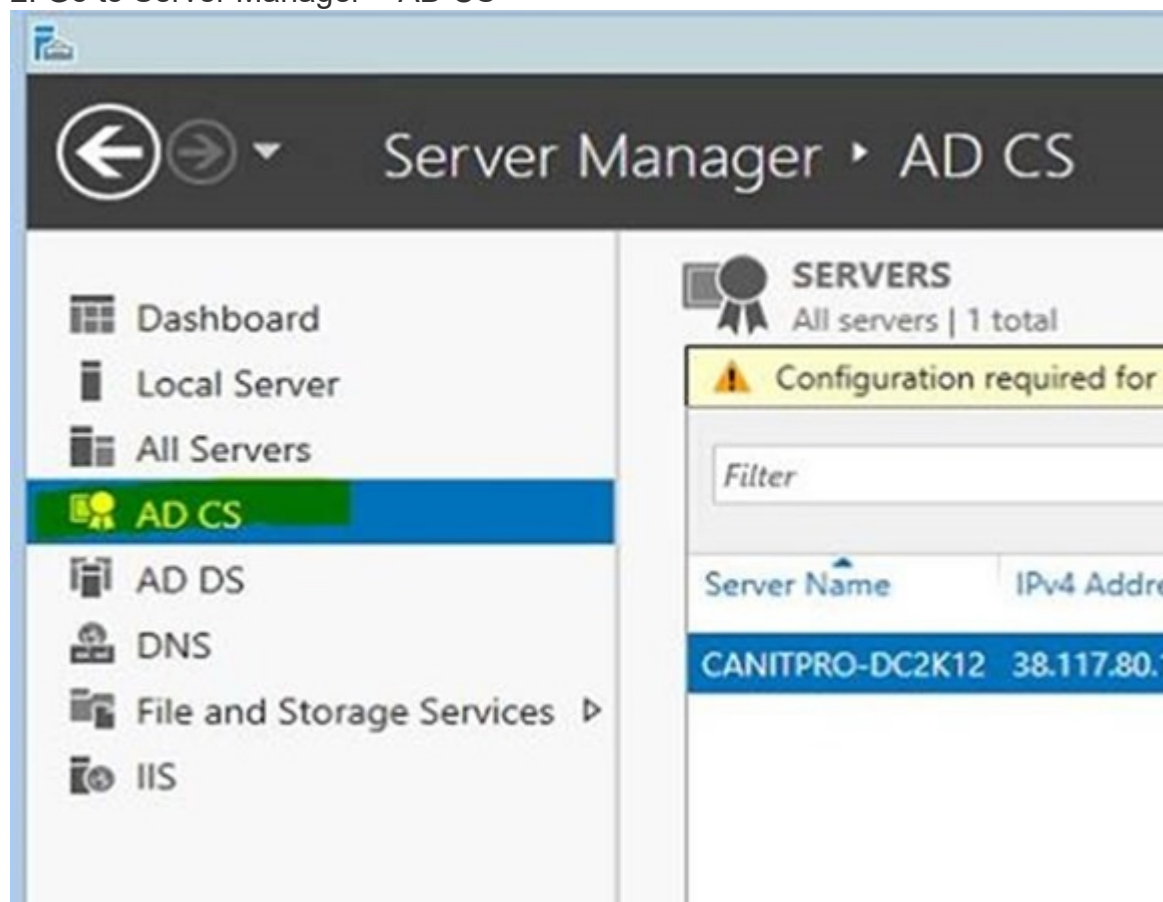


13. Once installation completes you can close the wizard.

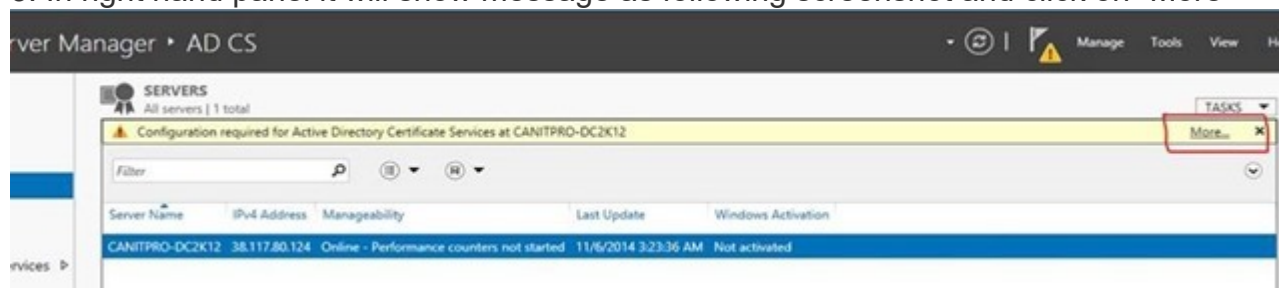
Step 5: Configure AD CS

In this step will look in to configuration and restoring the backup we created.

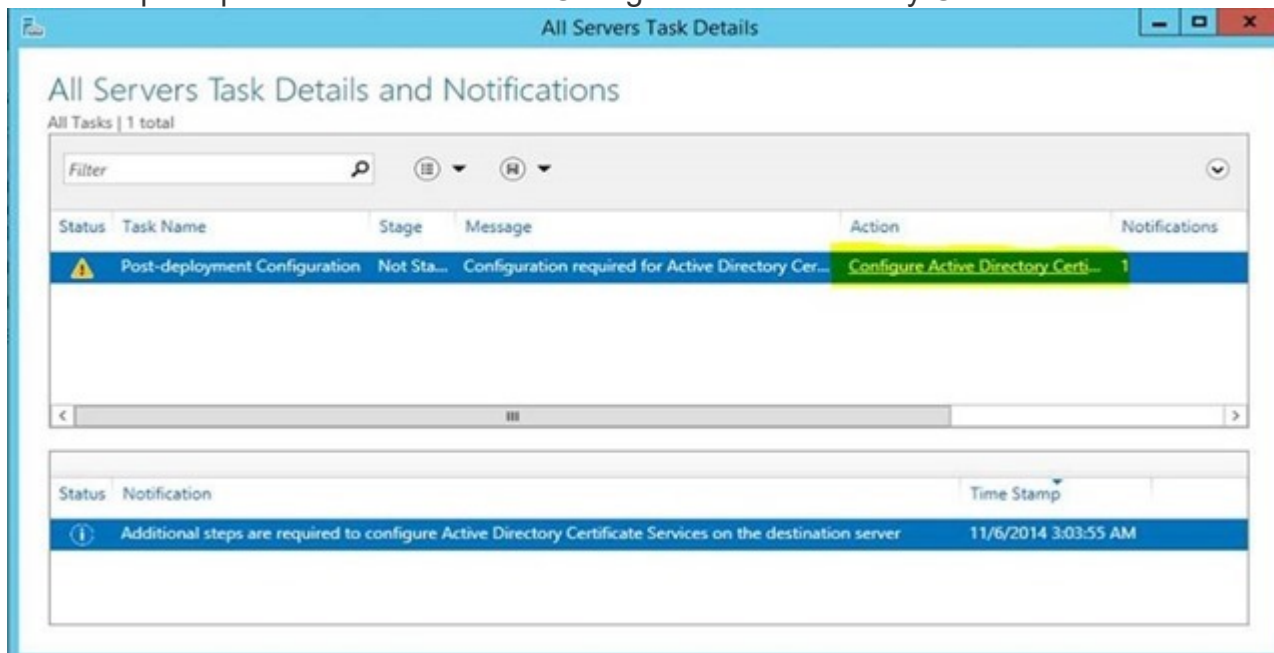
1. Log in to server as Enterprise Administrator
2. Go to Server Manager > AD CS



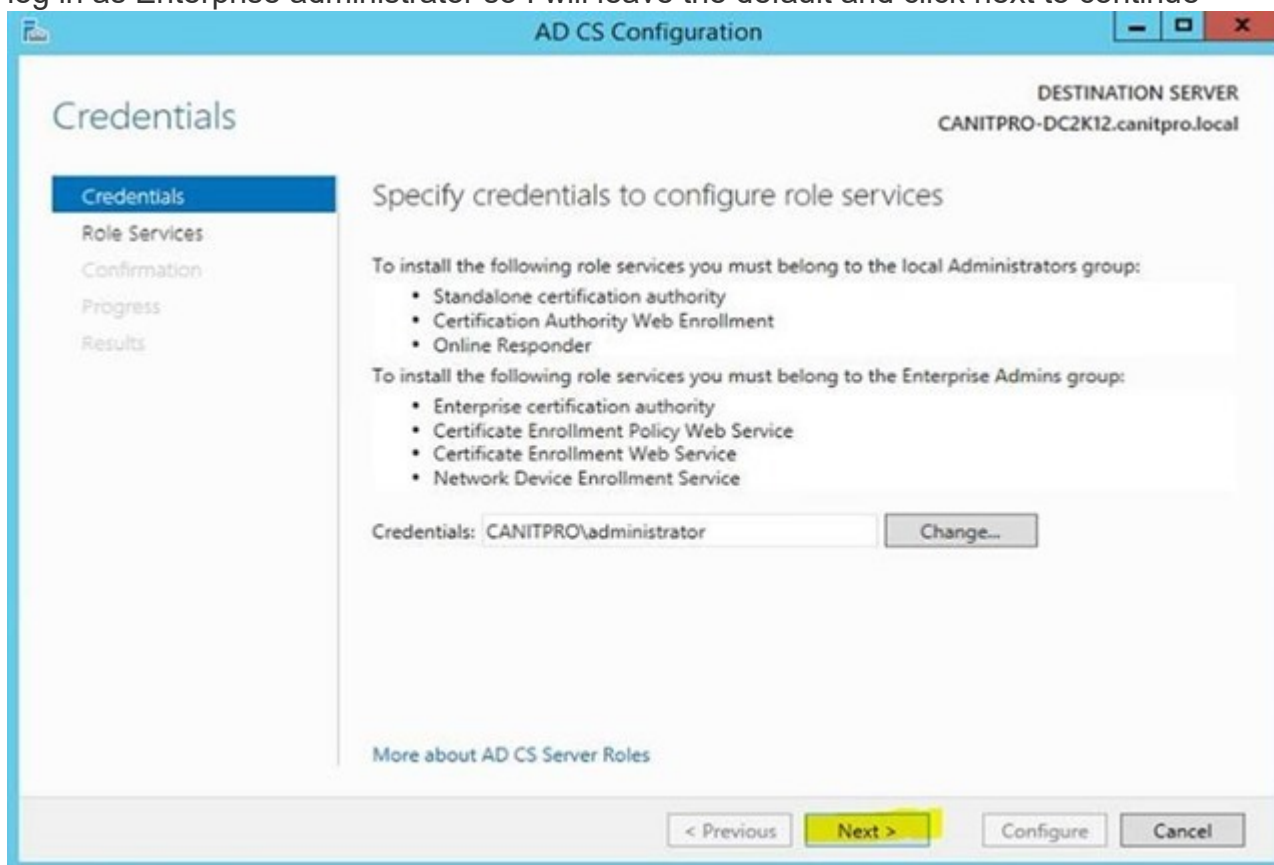
3. In right hand panel it will show message as following screenshot and click on “More”



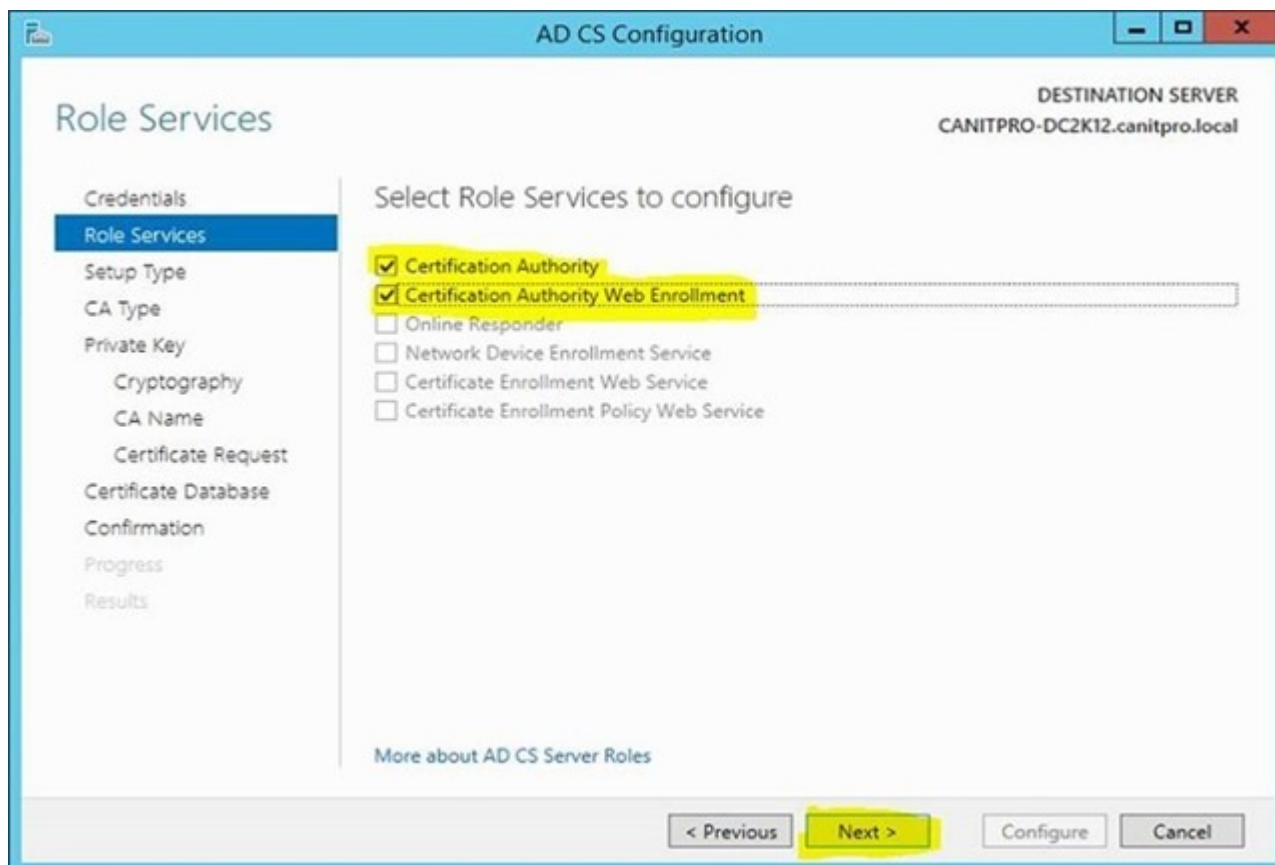
4. It will open up window and click on “Configure Active Directory Certificate Service



5. It will open role configuration wizard, it gives option to change the credential, in here I already log in as Enterprise administrator so I will leave the default and click next to continue



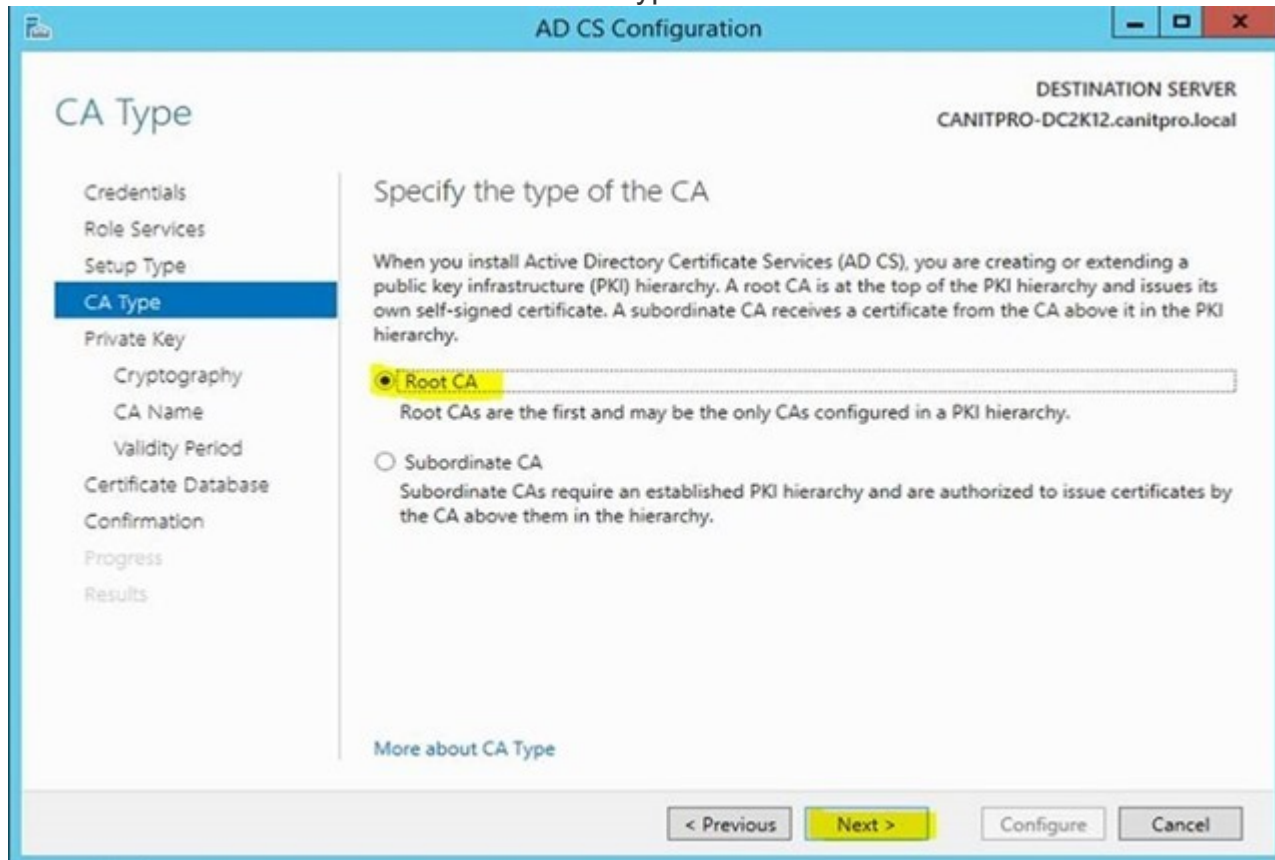
6. In next window it asking which service you like to configure. Select “Certification Authority”, “Certification Authority Web Enrollment” options and click next to continue



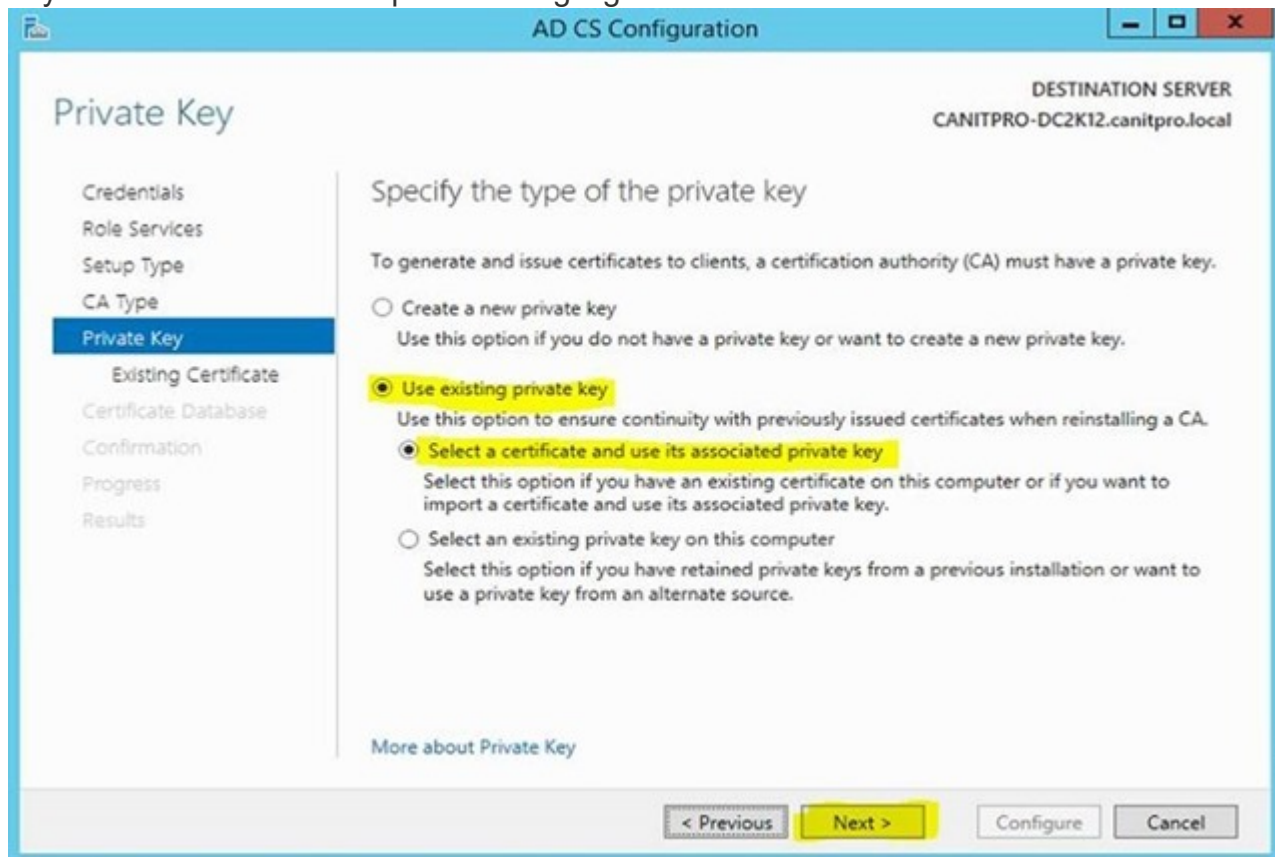
7. It will be Enterprise CA so in next window select the Enterprise CA as the setup type and click next to continue



8. Next window select “Root CA” as the CA type and click next to continue



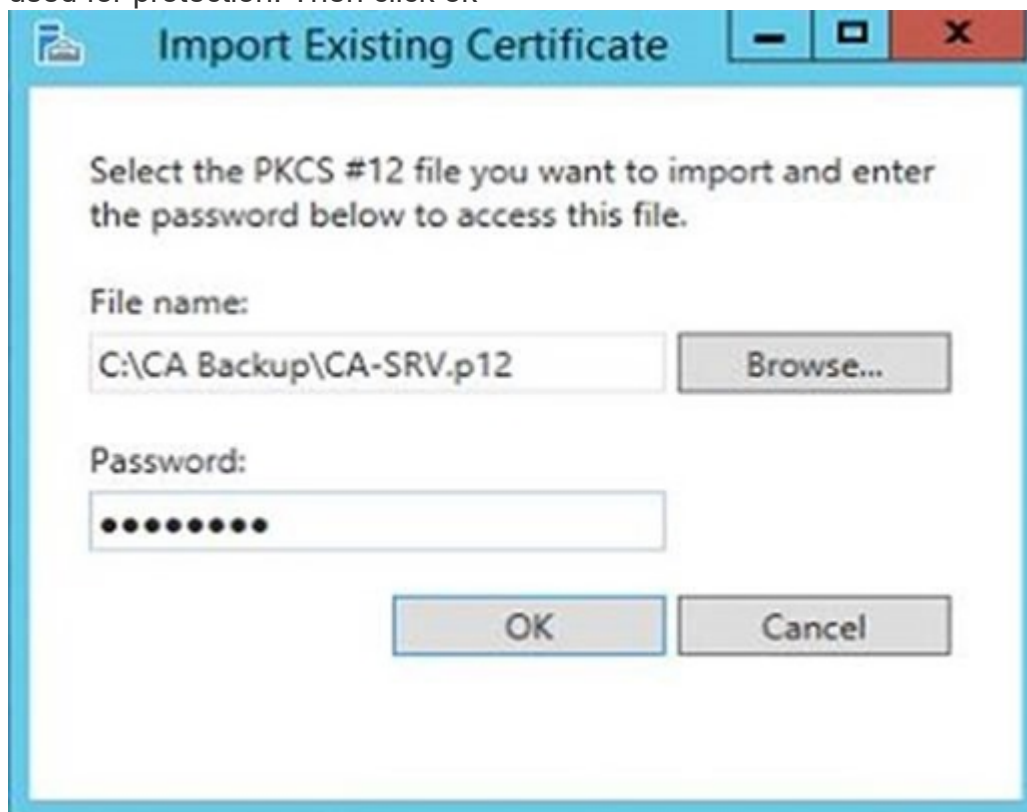
9. The next option is very important on the configuration. If its new installation we will only need to create new private key. But since it's a migration process we already made a backup of private key. So in here select the options as highlighted in screenshot. Then click on next to continue



10. In next window click on “Import” button



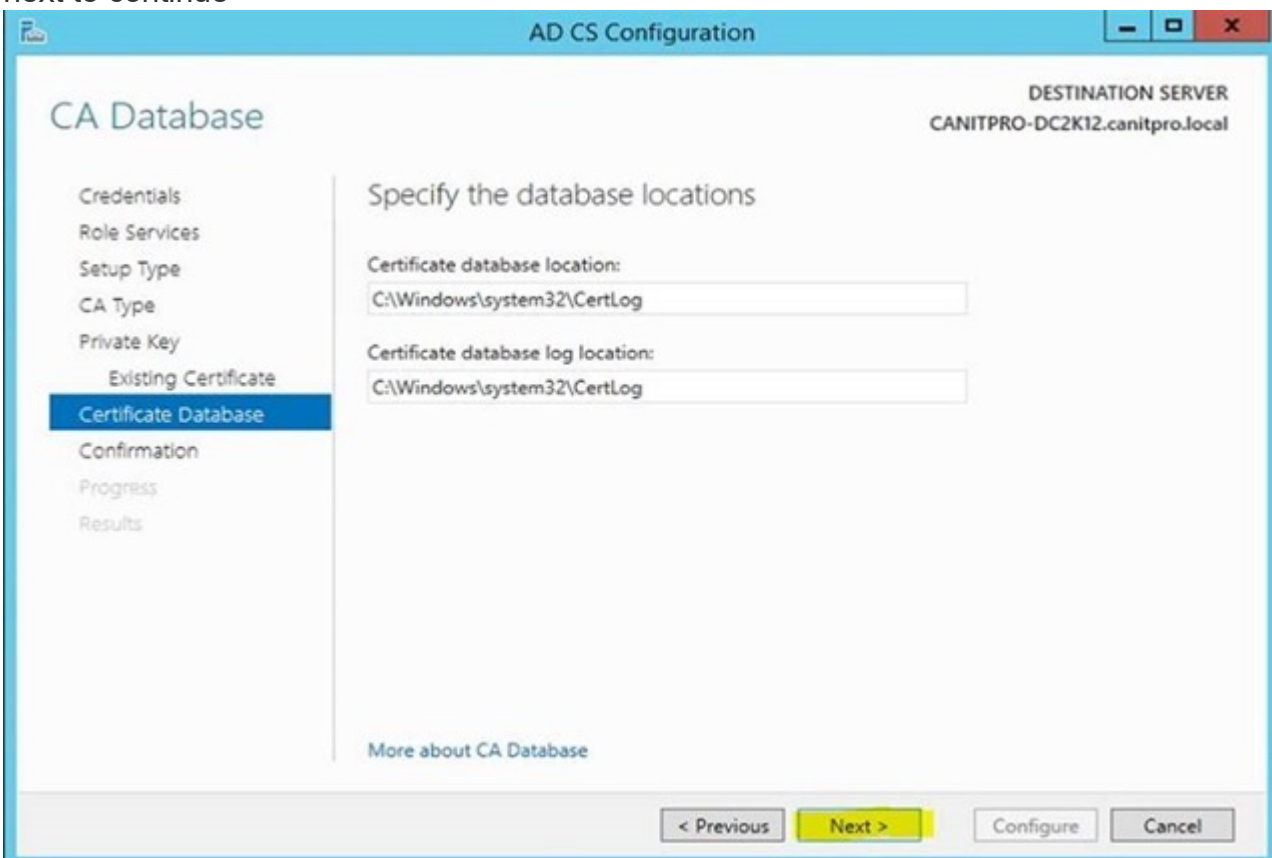
11. In here it will give option to select the key we backup during the backup process from windows 2003 server. Brows and select the key from the backup we made and provide the password we used for protection. Then click ok



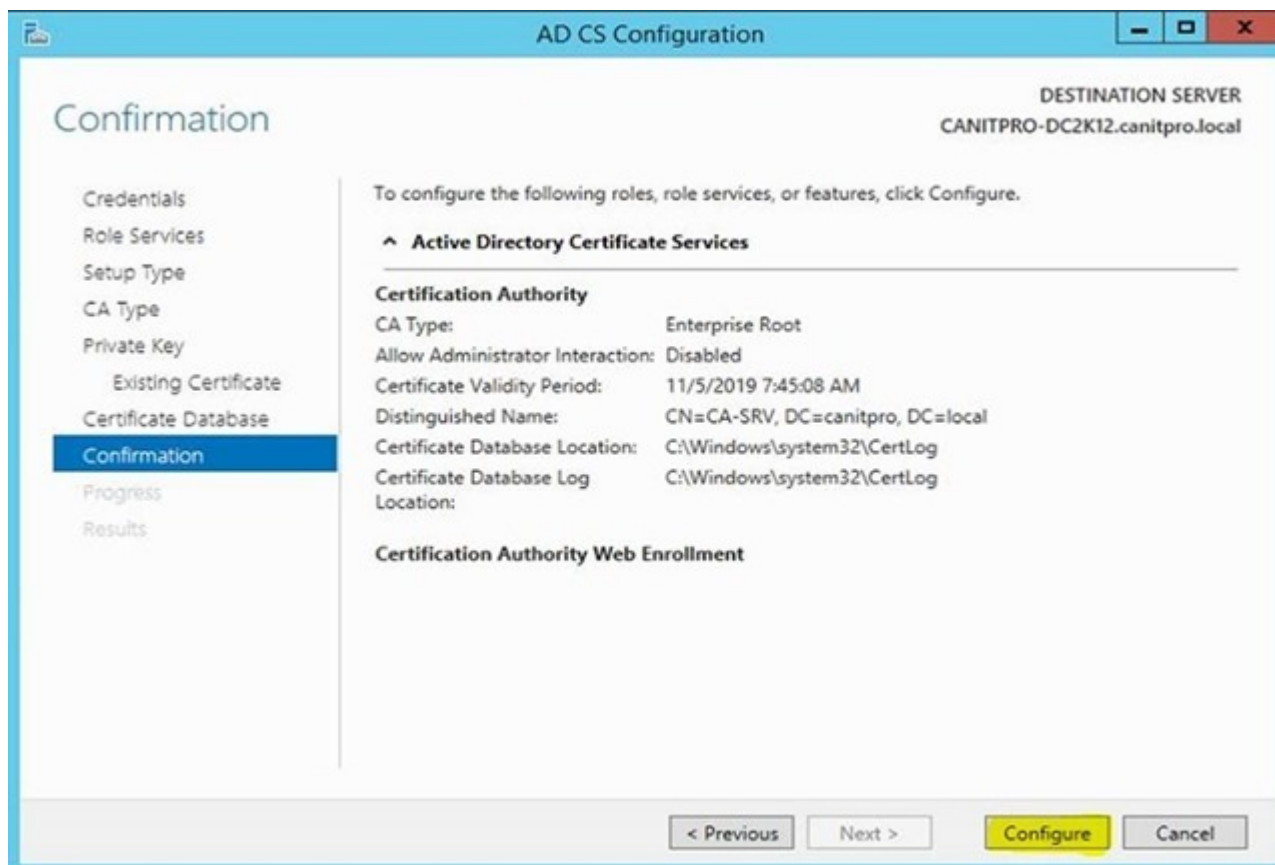
12. Then it will import the key successfully and in window select the imported certificate and click next to continue



13. Next window we can define certificate database path. In here I will leave it default and click next to continue



14. Then in next window it will provide the configuration confirmation and click on configure to proceed with the process

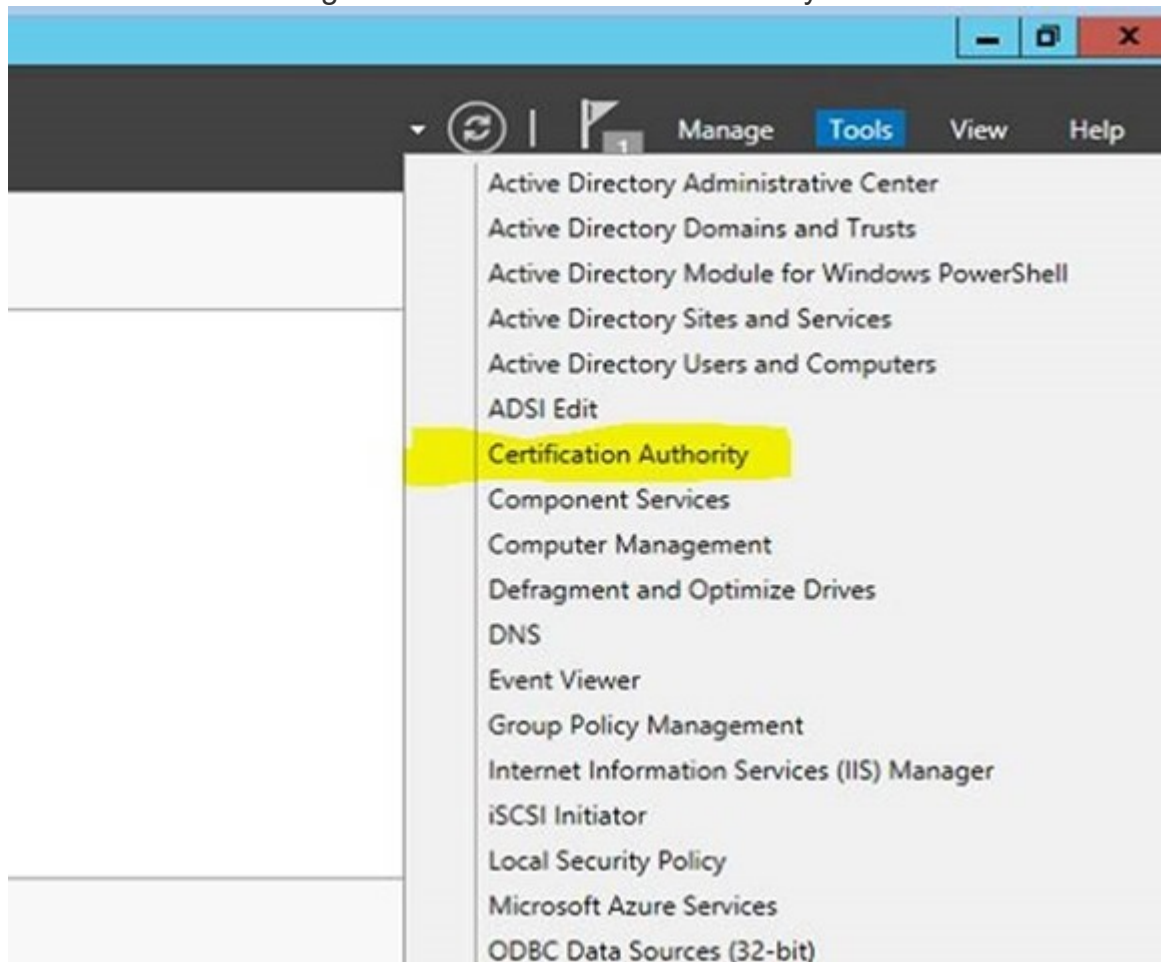


15. Once its completed click on close to exit from the configuration wizard

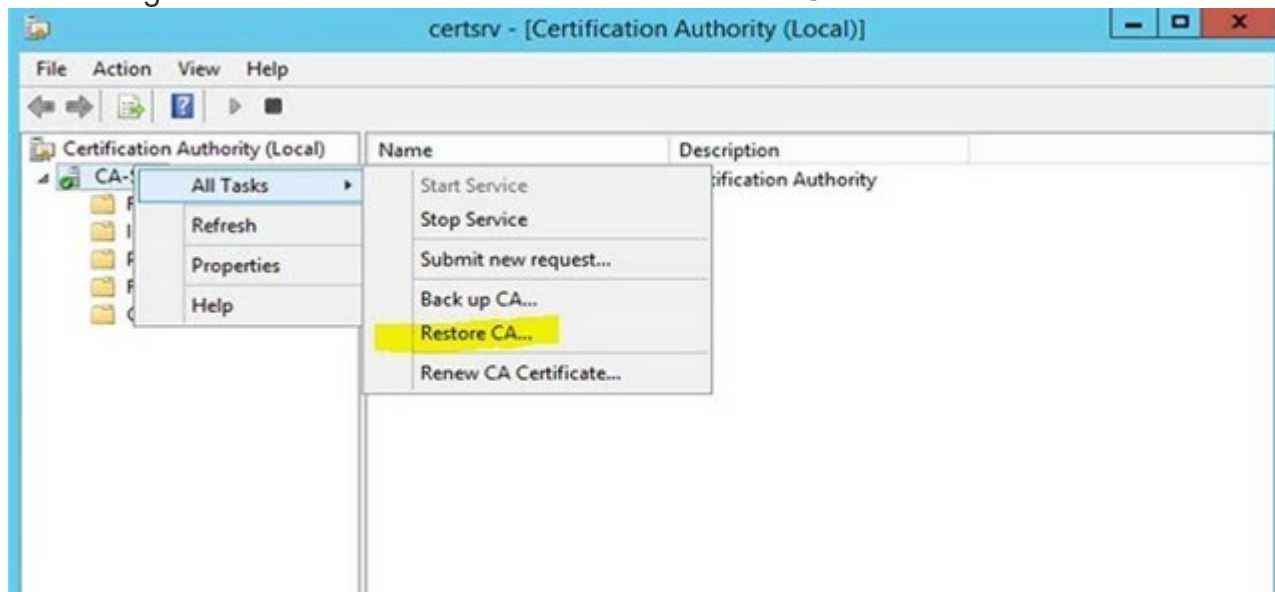
Step 6: Restore CA Backup

Now it's comes to the most important part of the process which is to restore the CA backup we made from Windows Server 2003.

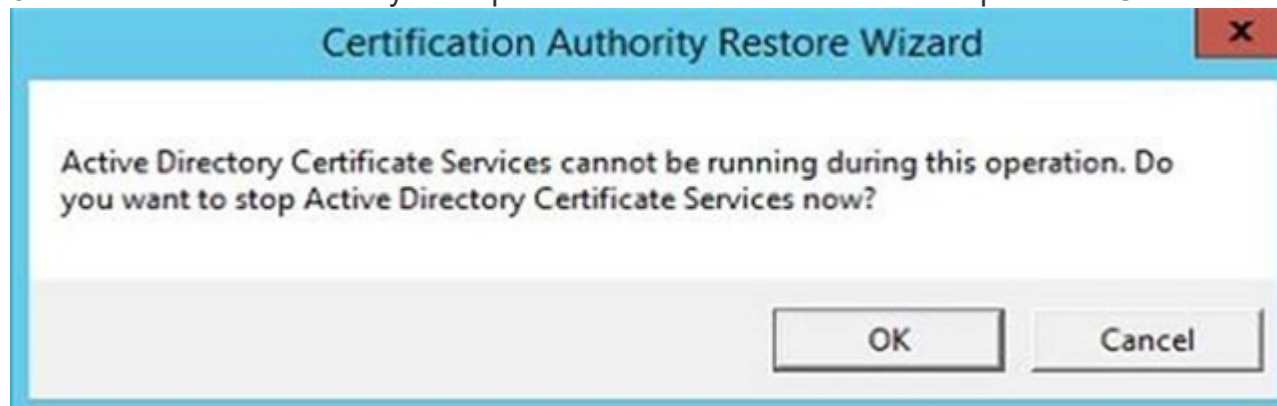
1. Go To Server Manager > Tools > Certification Authority



2. Then right click on server node > All Tasks > Restore CA



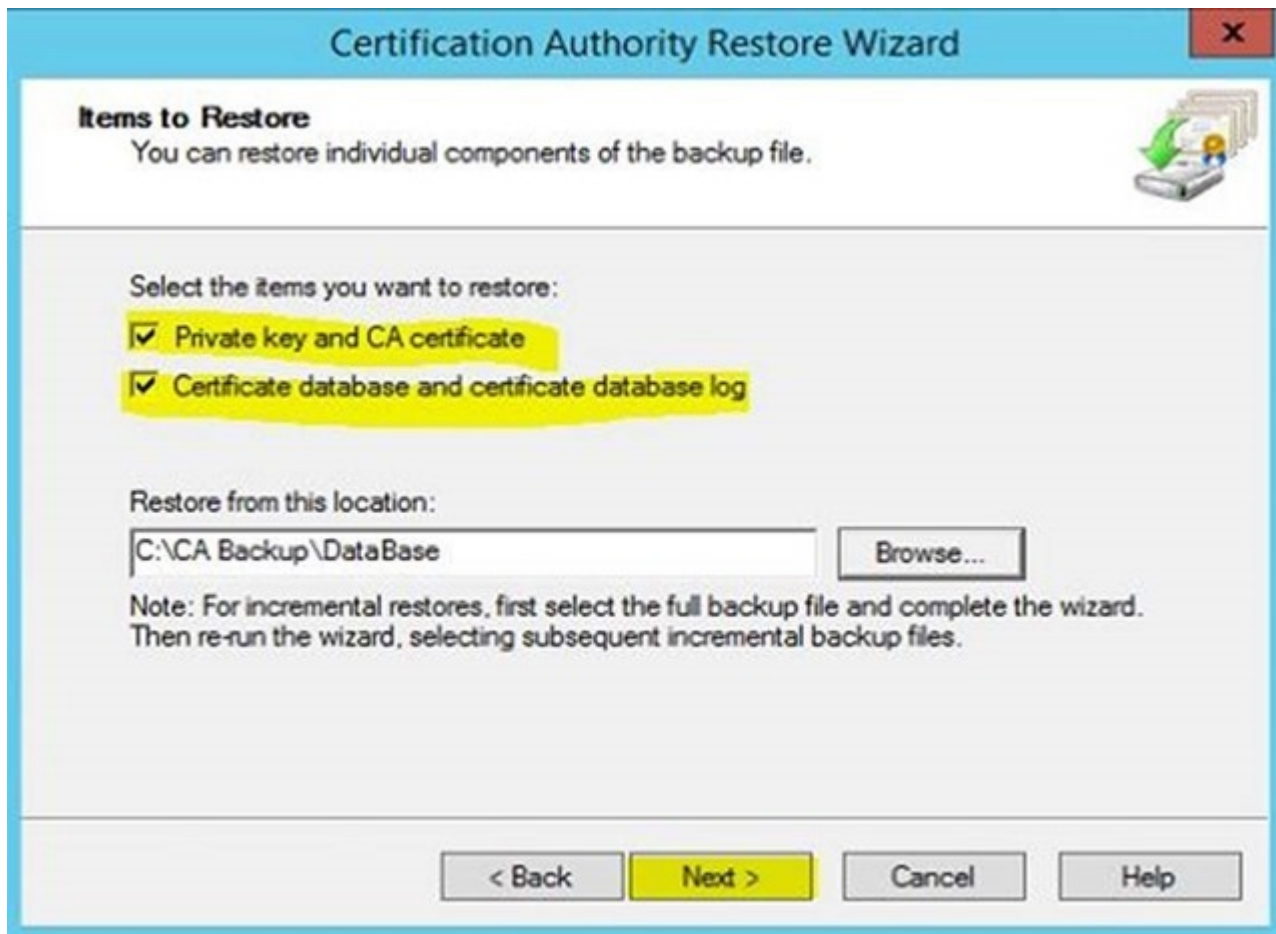
3. Then it will ask if it's okay to stop the certificate service in order to proceed. Click ok



4. It will open up Certification Authority Restore Wizard, click next to continue



5. In next window brows the folder where we stored backup and select it. Then also select the options as I did in below. Later click next to continue



Certification Authority Restore Wizard

Items to Restore
You can restore individual components of the backup file.

Select the items you want to restore:

- ☒ Private key and CA certificate
- ☒ Certificate database and certificate database log

Restore from this location:

C:\CA Backup\DataBase Browse...

Note: For incremental restores, first select the full backup file and complete the wizard. Then re-run the wizard, selecting subsequent incremental backup files.

< Back **Next >** Cancel Help

6. Next window give option to enter the password we used to protect private key during the backup process. Once its enter click next to continue



Certification Authority Restore Wizard

Provide Password
For encryption and decryption of messages, both a public key and a private key are required. You must provide the password for the private key.

This password is required to gain access to the private key and the CA certificate file.

Password:
[password field]

To maintain private key security, do not share your password.

< Back **Next >** Cancel Help

7. In next window click “Finish” to complete the import process

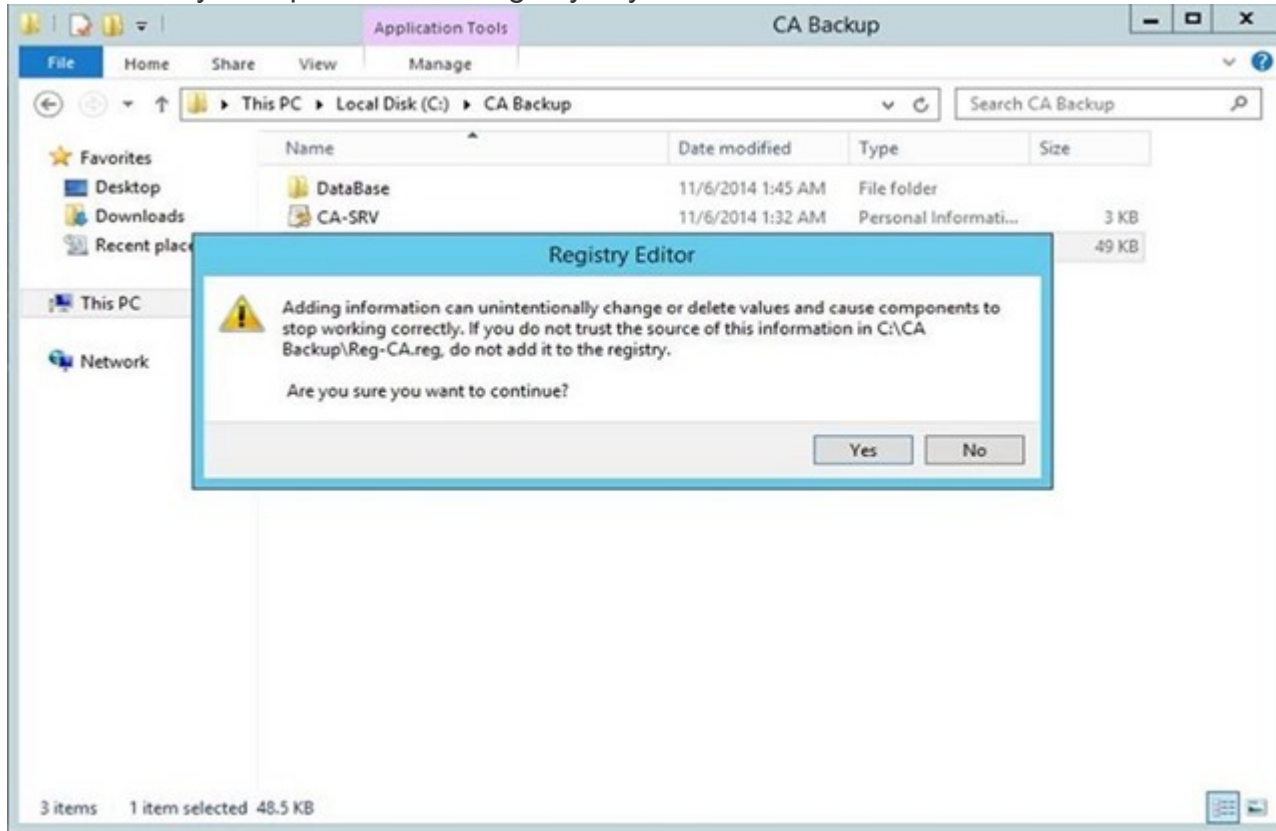


8. Once its completed system will ask if it's okay to start the certificate service again. Please proceed with it to bring service back online

Step 7: Restore Registry info

During the CA backup process we also backup registry key. It's time to restore it. To do it open the folder which contains the backup reg key. Then double click on the key.

1. Then click yes to proceed with registry key restore



2. Once completed it will give confirmation about the restore

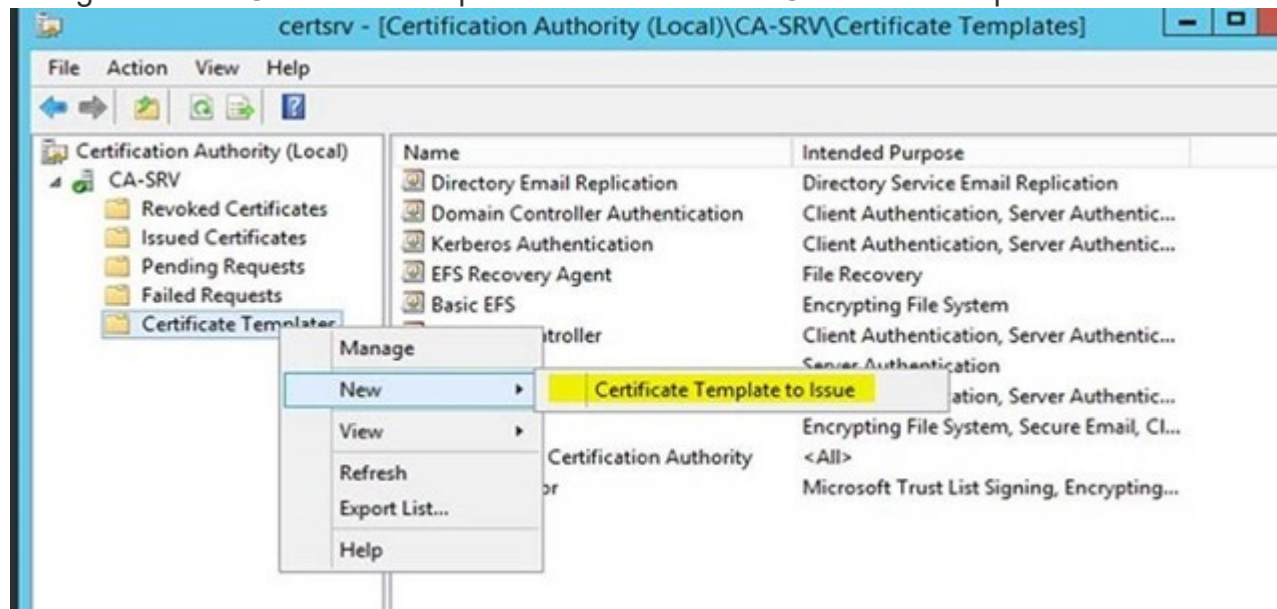


Step 8: Reissue Certificate Templates

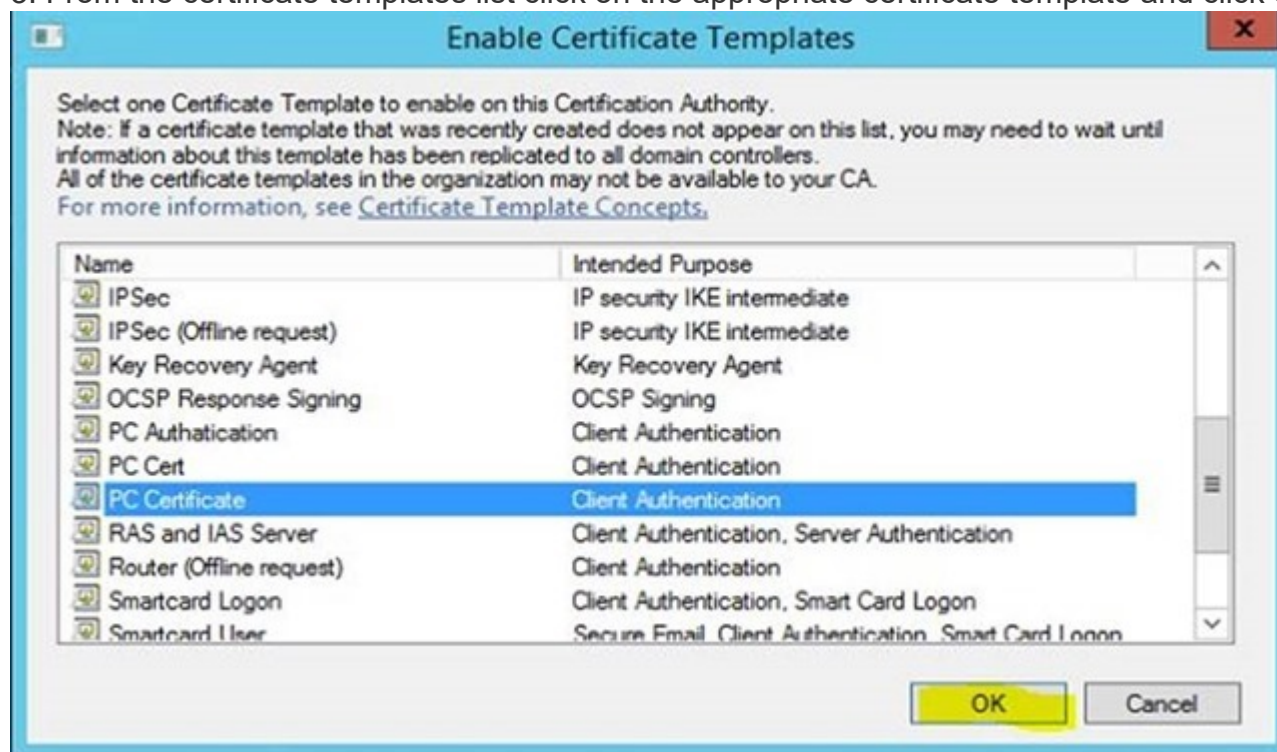
We have done with the migration process and now it's time to reissue the certificates. I had template setup in windows 2003 environment called "PC Certificate" which will issue the certificates to the domain computers. Let's see how I can reissue them.

1. Open the Certification Authority Snap-in

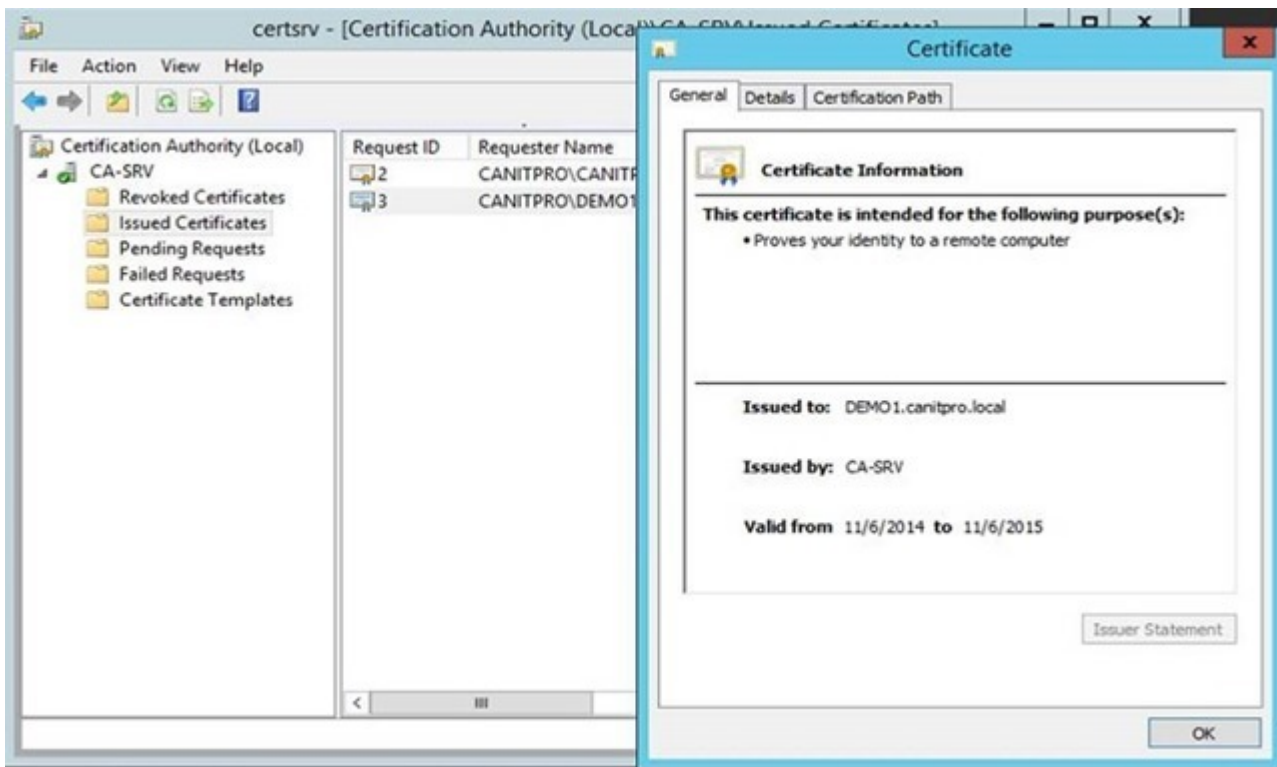
2. Right click on Certificate Templates Folder > New > Certificate Template to Reissue



3. From the certificate templates list click on the appropriate certificate template and click ok

**Step 9: Test the CA**

In here I already had certificate template setup for the PC and set it to auto enroll. For the testing purposes I have setup windows 8 pc called **demo1** and added it to canitpro.local domain. Once it's loaded first time in server I open certification authority snap in and once I expanded the "Issued Certificate" section I can clearly see the new certificate it issued for the PC.



So this confirms the migration is successful.

Tags [Active Directory](#) [How-To](#) [MVP](#) [Step-By-Step](#) [Windows Server 2003](#) [Windows Server 2012](#) [Windows Server 2012 R2](#)

Comments (17)

Name *

Email *

Website

[Post Comment](#)



[Brian Wing](#)

[June 27, 2016 at 9:02 pm](#)

There are other options, role features that are enabled in 2012R2. Is it best to complete the steps as you described, then add the new services, or does it matter when you add these additional services, ex. network device, certificate web enrollment, etc.

[Reply](#)

Jon



July 28, 2016 at 9:45 pm

Thank you for the article. I have several questions that I can't seem to find an answer to. Your old and new CA servers have different names as mine to however, the server name in your console matches neither and appears to be a CName. The certificate issued matches that CName "CA-SRV". Unfortunately, in my environment the certificates issued have the name of the legacy server that I wish to replace. The articles that I have found mention to have the new server match the name of the old sever. I'm not sure how to move forward with the name mismatch, please advise.

Thank you,
Jon

[Reply](#)



ITGuy

August 1, 2016 at 9:41 pm

Dear Dishan,

Thank you very much for this invaluable article. I have 2 questions that I wanted to clarify.

(1) The scenario that you described above, does it apply only in the situation where there is a single Enterprise CA server that houses both Ent Root CA and Ent Subordinate CA? For example, we have an Enterprise Root CA server (Windows 2003, 32-bit) and Enterprise Subordinate CA server (Windows 2008 R2, 64-bit). Need to upgrade only Enterprise Root CA server from Windows 2003 to Windows 2012 R2.

(1.a) The Enterprise Root CA server also has a domain controller role (we want to remove that role), will the domain controller role need to be removed prior to doing migration, or after?

(2) Is there a rollback plan that can be used with this migration in case if there are issues with the migration?

[Reply](#)



shy

August 21, 2016 at 10:50 am

Thanks for a great article, is there any roll back option?

[Reply](#)



Shadab Ahmad

August 4, 2016 at 1:04 pm

Good Article

[Reply](#)



ITOFC

October 3, 2016 at 12:28 am

I read in many places you cannot import a x86 database to a x64. It throws the error "The expected data does not exist in this directory. Please choose a different directory." How did you get yours to restore without issue?

[Reply](#)



Paul Rixon

August 23, 2016 at 3:25 pm

Great walkthrough and will definitely follow this when moving mine next month. Will existing certificates break if I'm moving to a different hostname? A few articles I've read suggest you need to keep the same name?

[Reply](#)*Venom*[September 11, 2016 at 9:35 am](#)

Great Article,

Have anyone done this and can say what happens to old certs that have been issued to AD clients member and also the ones we have issued to other resources. The CA on 2003 is named as the server, will that cause problems if the old 2003 server will be alive for another 3-6months?

[Reply](#)*bhupalan*[November 29, 2016 at 2:46 pm](#)

I dont think so, but have you tried 😊

[Reply](#)*ITOFc*[October 3, 2016 at 12:28 am](#)

I read in many places you cannot import a x86 database to a x64. It throws the error "The expected data does not exist in this directory. Please choose a different directory."
How did you gets yours to restore without issue?

[Reply](#)*Miguel*[February 9, 2017 at 10:40 pm](#)

I selected the level above database, where the .ip2 certificate is located and it went through without problems

[Reply](#)*Richard*[October 27, 2016 at 11:12 am](#)

Just the article I needed.

One thing worth mentioning. I migrated my CA from 2003 to 2012R2. The registry export from 2003 contains the paths to the CertLog folder in System32. But 2003 still uses C:\WINNT as the %systemroot%. Since 2008, this folder is no longer called WINT but Windows. So when you import the .reg file, the wrong path is added to the registry. This causes the ADCS service to fail with a PATH_NOT_FOUND error.

I manually edited the registry and replaced C:\WINT with C:\WINDOWS in the \HKLM\SYSTEM\Currentcontrolset\Services\CertSvc\Configuration after which the services starts succesfully.

Greetings

[Reply](#)*Stryker*[November 1, 2016 at 6:58 pm](#)

You're missing the step where the DBDirectory FQDN needs to be changed if the hostname changes.

[Reply](#)



Reginald Johnson

[November 16, 2016 at 4:01 pm](#)

I'm having a problem. When I get to the part of restoring the CA on the 2012 server, I keep getting this error message: "The unexpected data does not exist in this directory. Please choose a different directory. The system cannot find the file specified. 0x800700002 (WIN32: 2)"; which is weird because the files are there in backup folder, and they have been altered in any way that I can think of. What am I doing wrong?

[Reply](#)



no more x86

[February 2, 2017 at 9:39 pm](#)

This guide is great, nice and detailed, but it fails to mention that you can't migrate x86 CA to an x64 machine.

[Reply](#)



Sadanand Velechi

[February 9, 2017 at 8:52 pm](#)

Very good explanation.

I have one query, if I want to migrate IA Server from window 2003 to 2012, what are the steps for that?

Regards,
Sadanand Velechi

[Reply](#)



Schattenberg

[May 29, 2017 at 12:15 am](#)

Great Great Great Article, thank you so much 😊

[Reply](#)

Follow Us

Video of the Week

Sharing of thoughts and information is what blogging is all about. This way we can learn from each other.
Post A Comment!

These postings are provided "AS IS" with no warranties, and confers no rights. You assume all risk for your use.

[Subscribe to TechNet E-Newsletter](#) 

Resident Bloggers



Anthony Bartolo
[Twitter](#) | [LinkedIn](#)



Pierre Roman
[Twitter](#) | [LinkedIn](#)

[Privacy & Cookies](#) [Terms of Use](#) [Trademarks](#)

Microsoft

© 2018 Microsoft