

Download VMWare

<https://www.vmware.com/asean/products/workstation-player/workstation-player-evaluation.html>

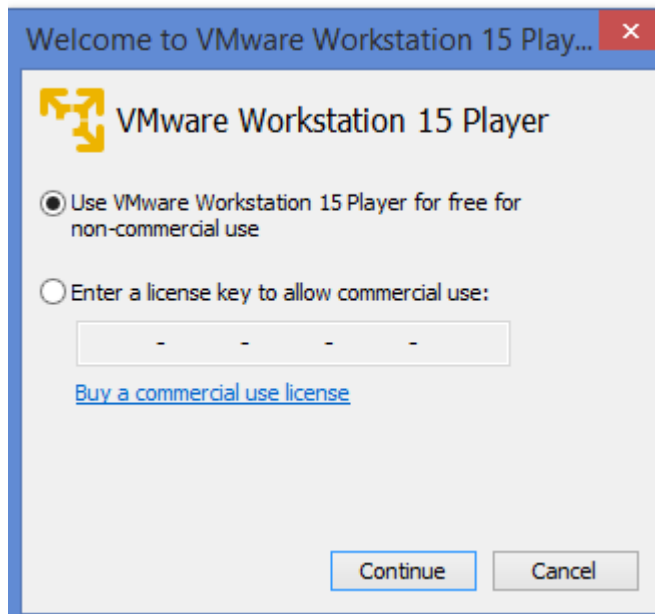
Download Windows Server 2012 **.iso**

<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2>

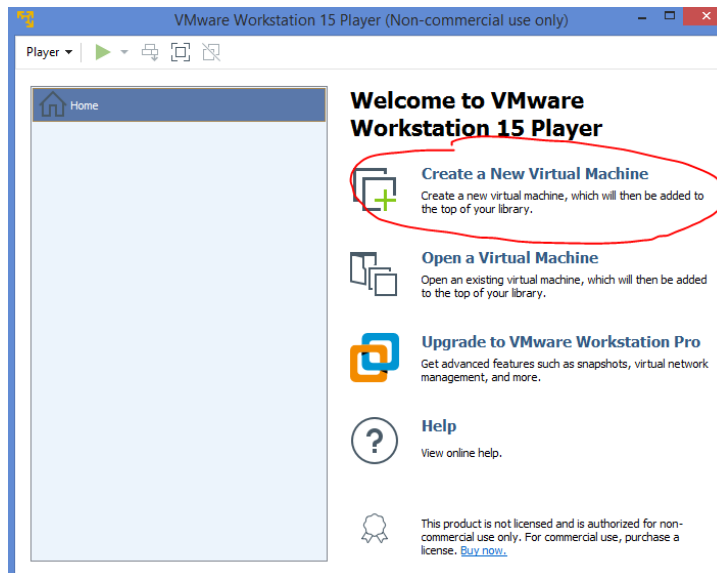
Install VMWare

Install Windows Server 2012 in VMWare

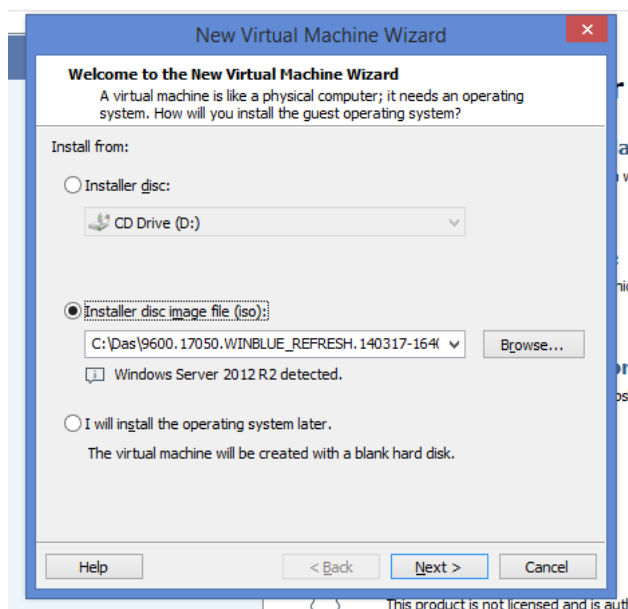
- A. Run VMWare Workstation 15
- B. Select use VMWare Workstation 15 player for free for noncommercial use and click continue



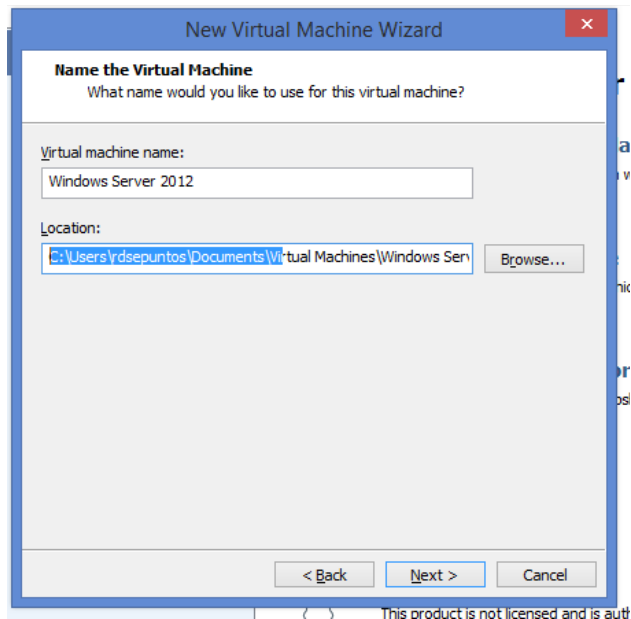
C. In virtual Machine menu click on create a new virtual machine



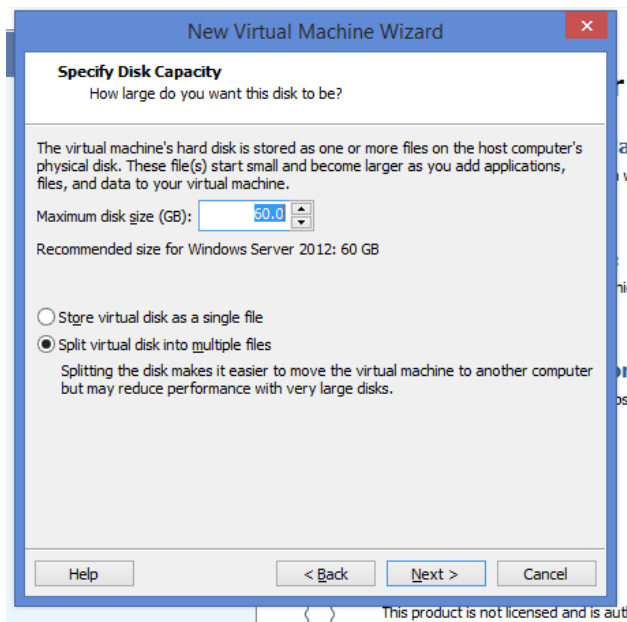
D. Installation form will be shown click on Installer disc image file (iso) and locate the downloaded Windows server 2012 and click on next



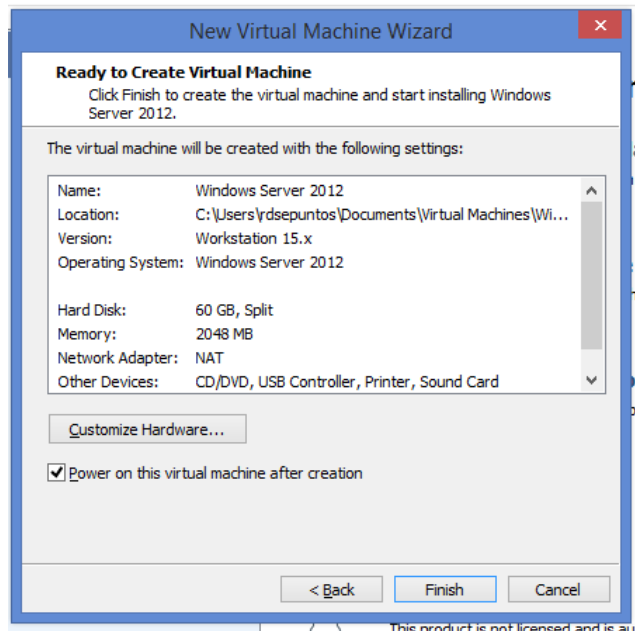
E. Set the name of the virtual machine and the location where it will be created.



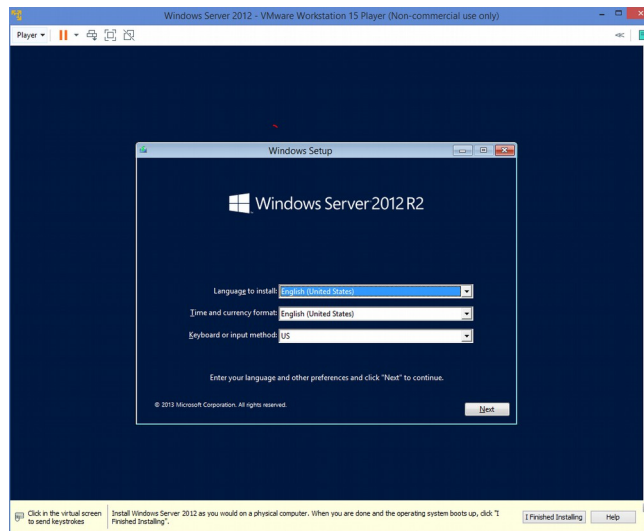
F. Set the allocated size of the virtual machine then click next



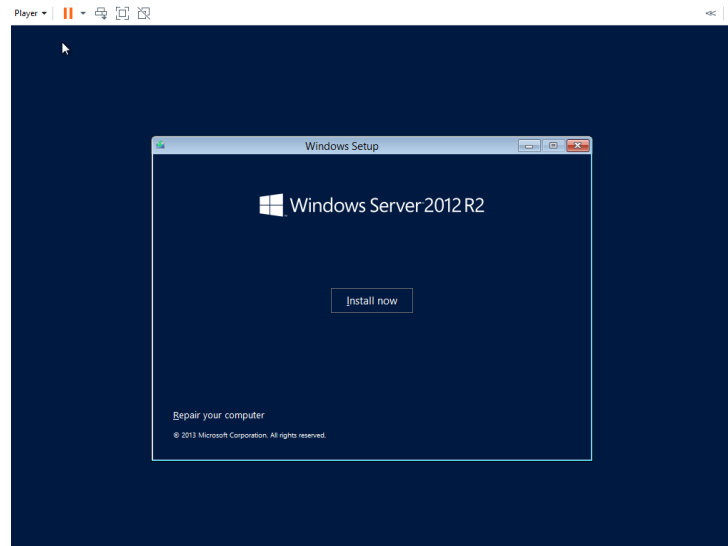
G. Click on finish



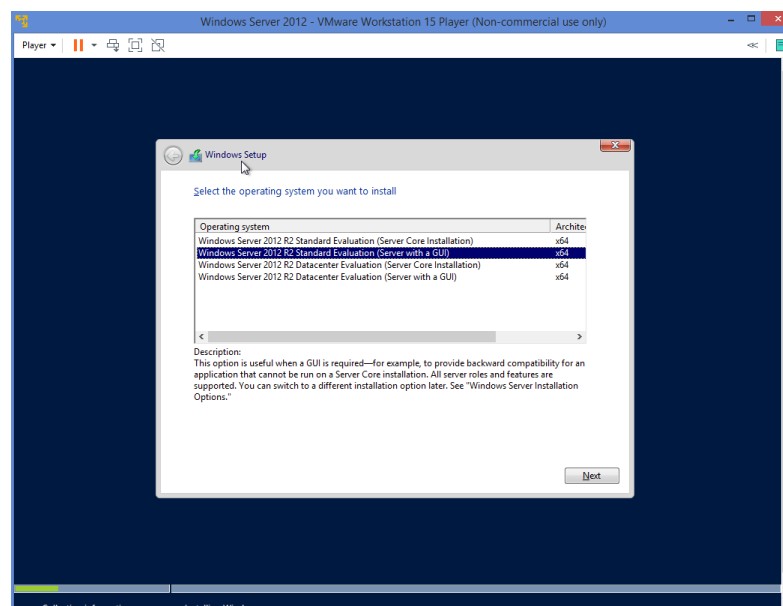
H. Virtual Machine should now run and will display installation of windows. Click Next



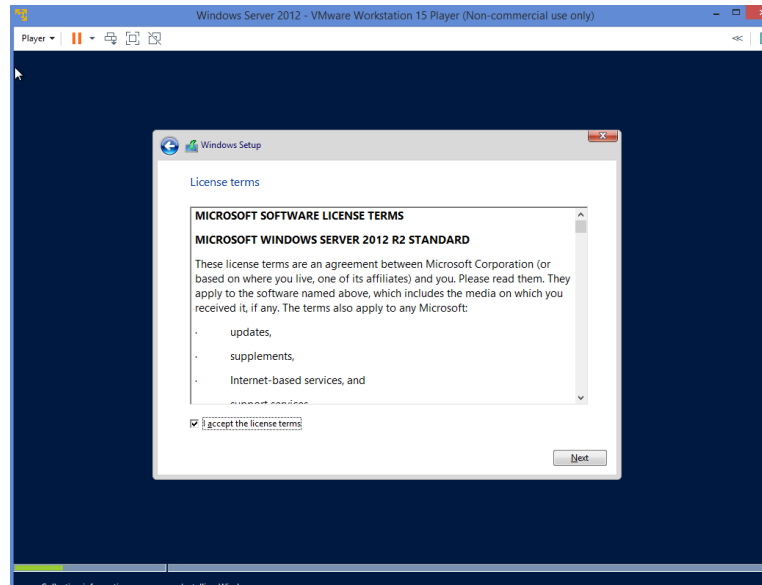
I. then click on install



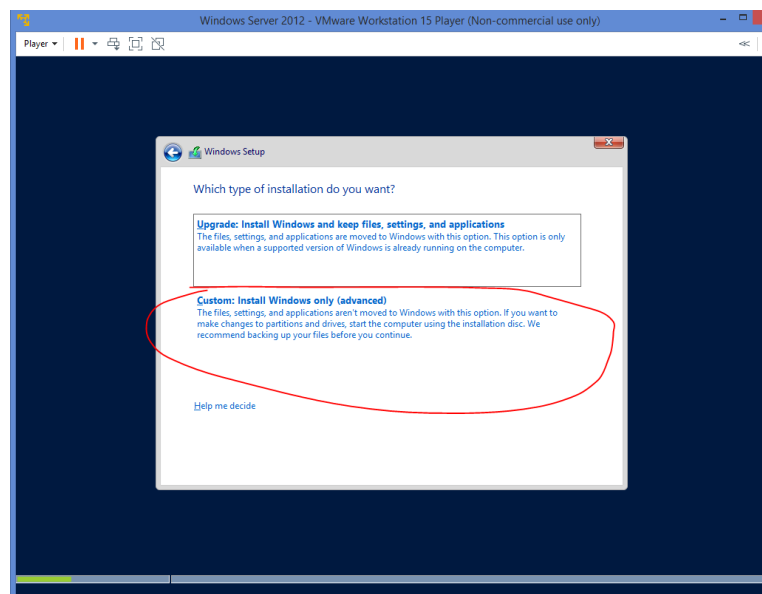
J. Select Windows Server 2012 Standard Evaluation (Server GUI) then click next



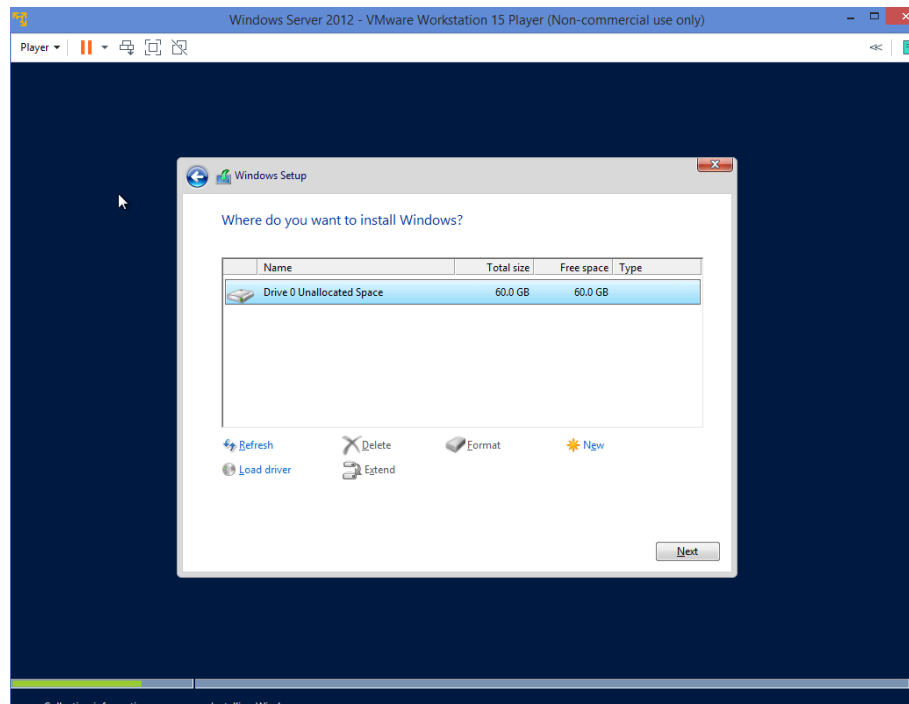
K. Accept the license Term agreement then click next



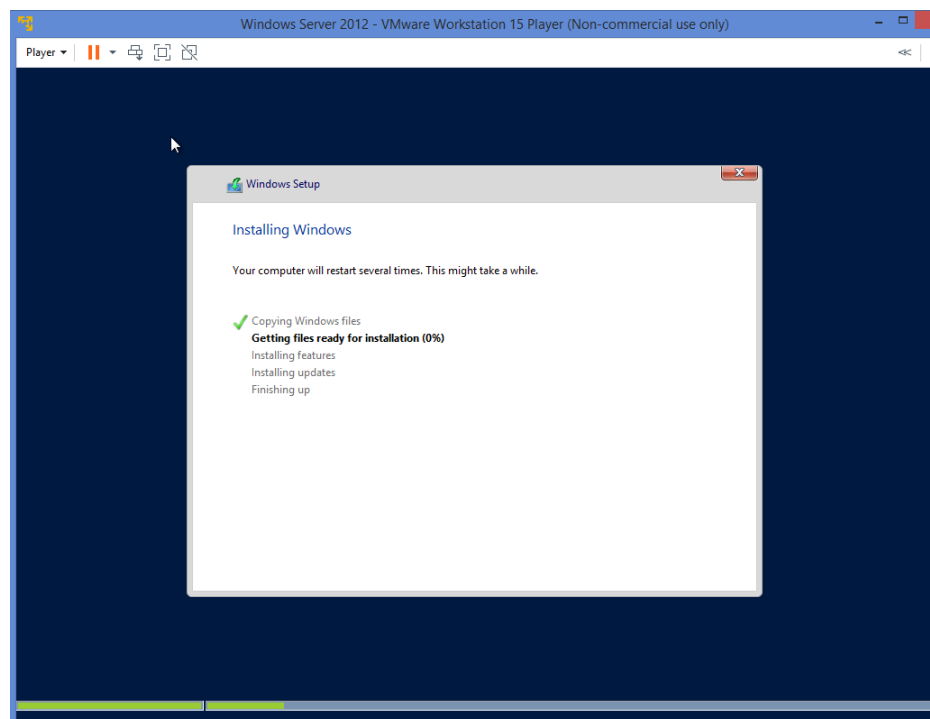
L. Select Custom: Install Windows Only (advanced)



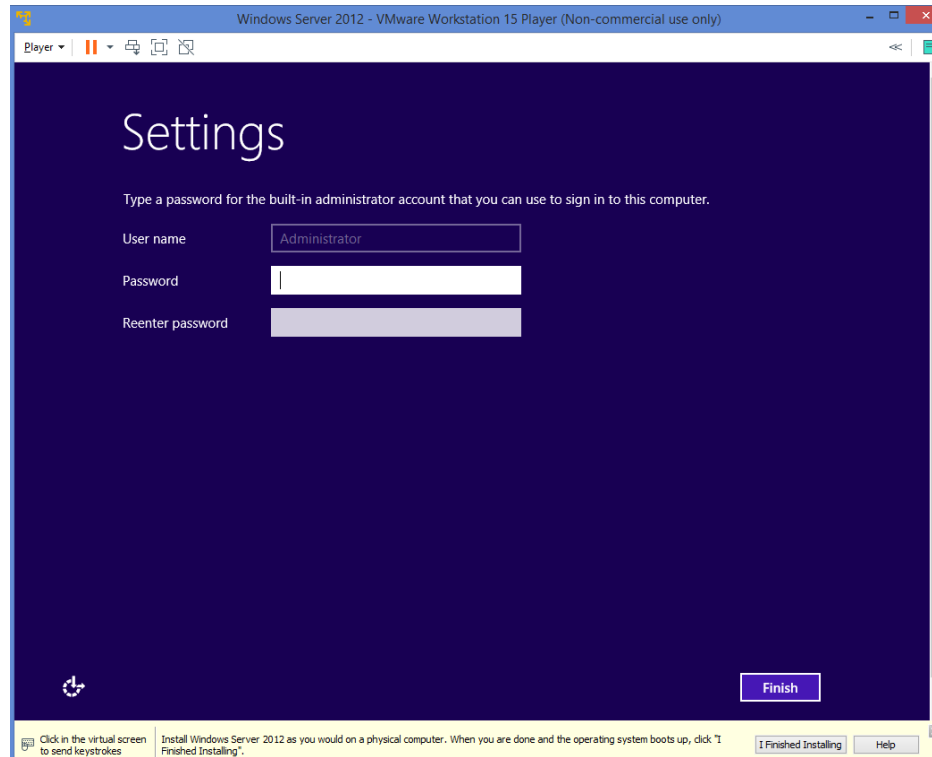
M. Select partition and click next



N. Wait for the installation to be finish

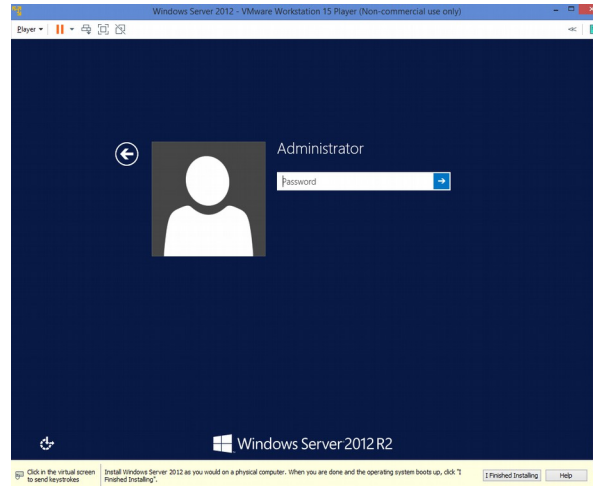


O. Set the password of the server

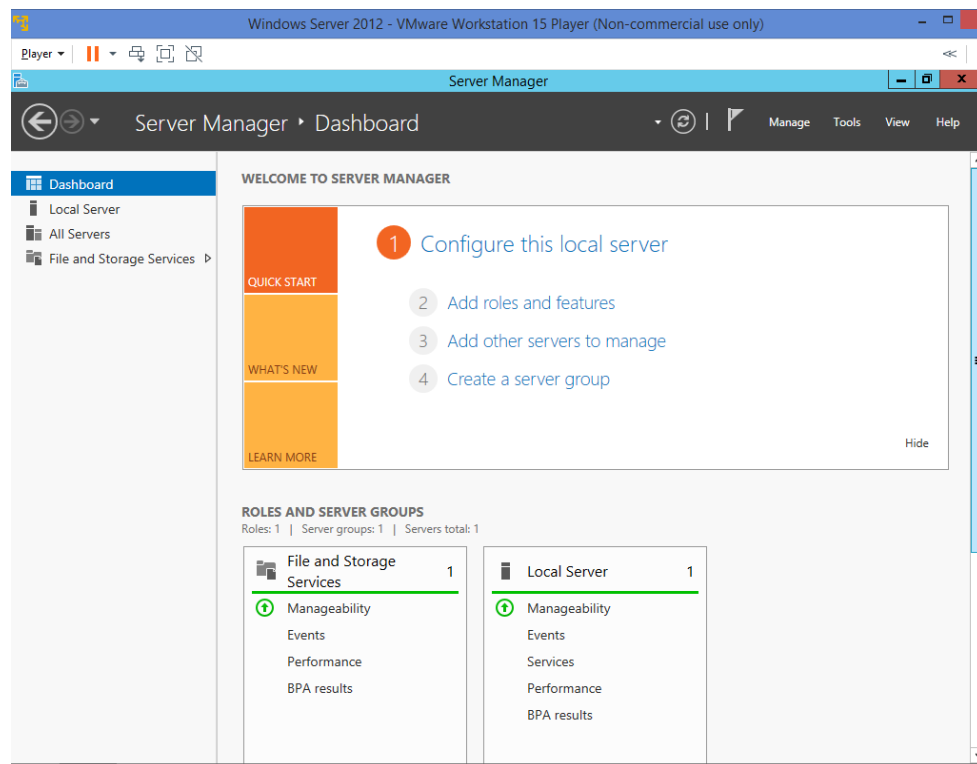


Install AD FS, AD and IIS

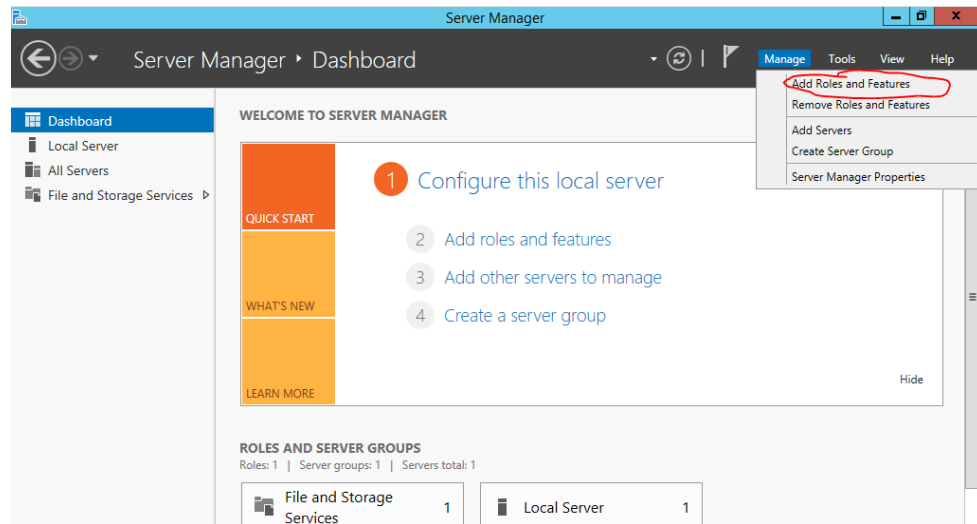
- A. Login to virtual machine windows server using ctrl + alt + insert
- B. Enter the password set earlier.



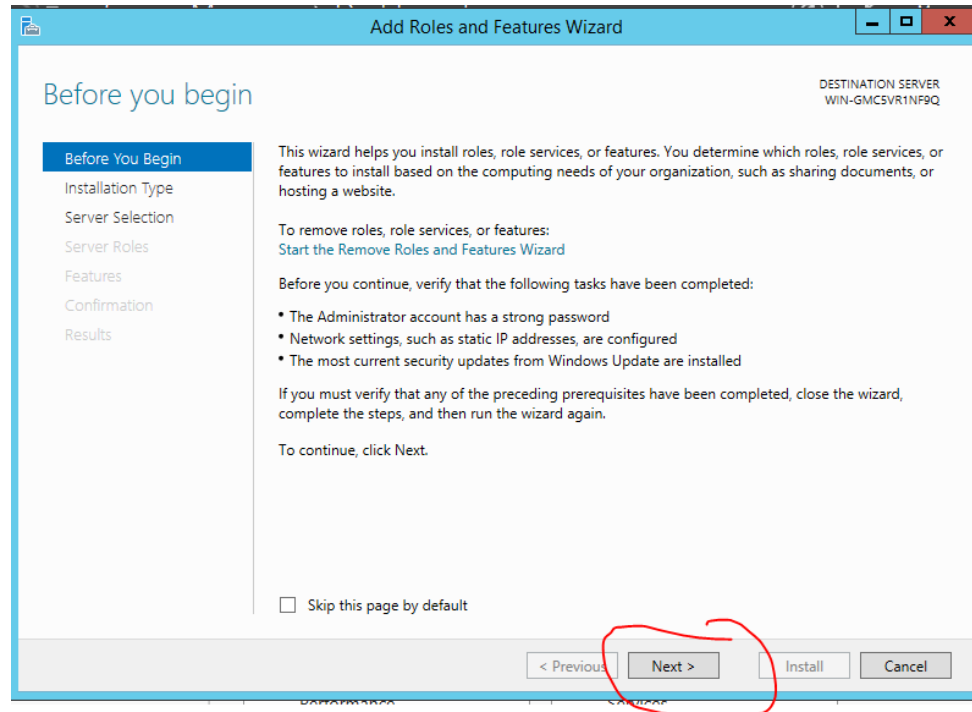
C. wait for the server manager to be loaded



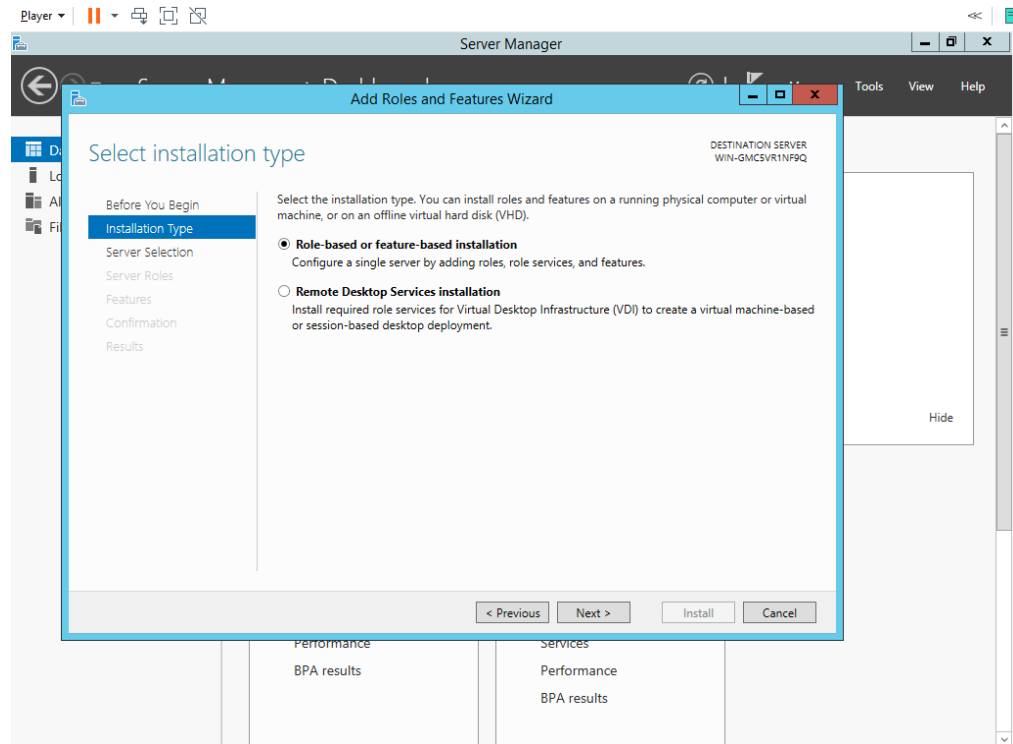
D. Click on add roles and features



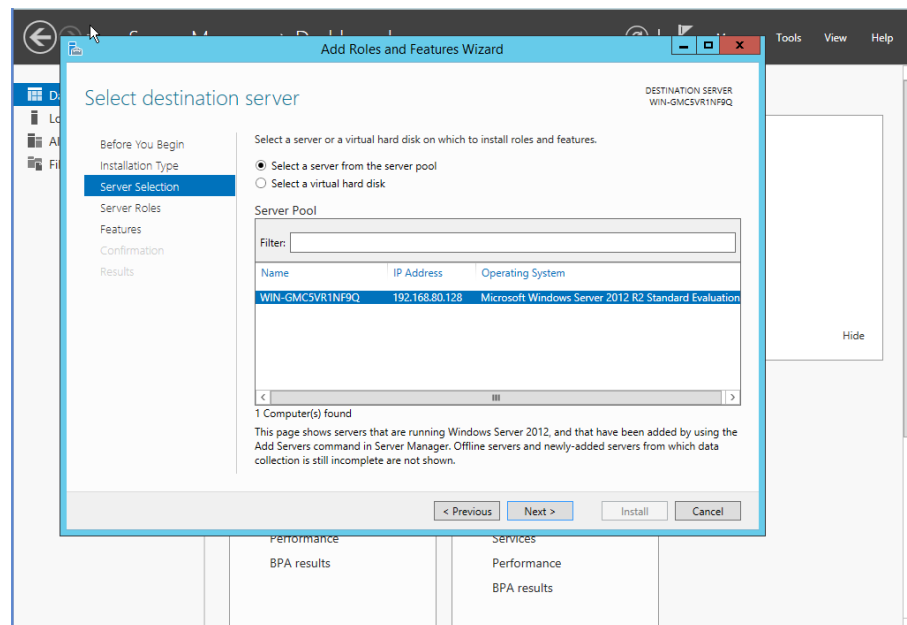
E. In add roles and features wizard click on next



F. Select Role based or feature-based installation

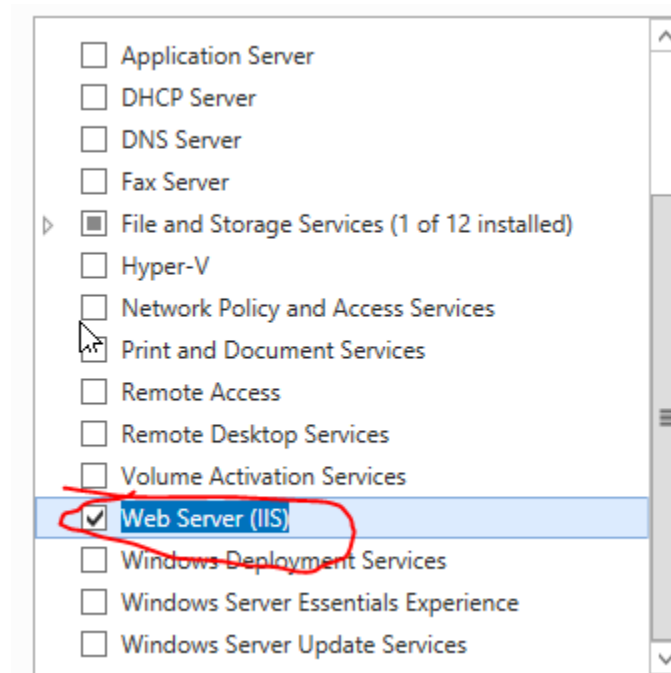
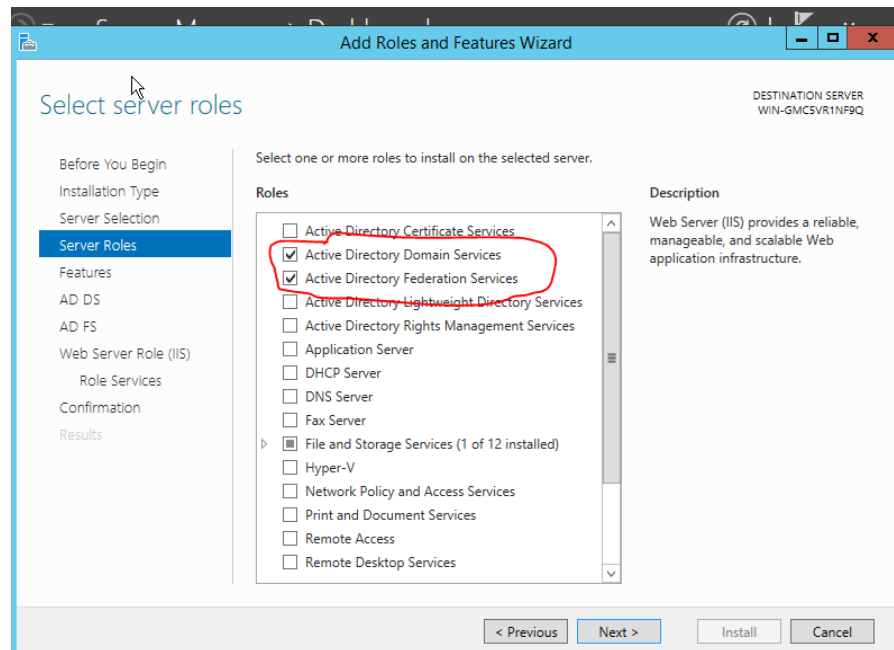


G. select "Select a server from the server pool" then click next

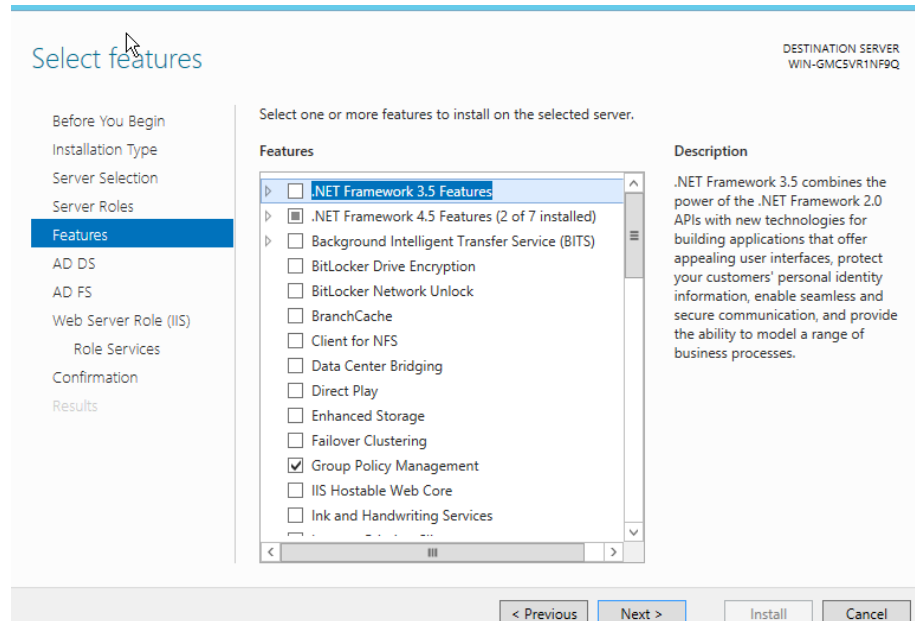


H. Select Active Directory Domain Services, Active Directory Federation Services

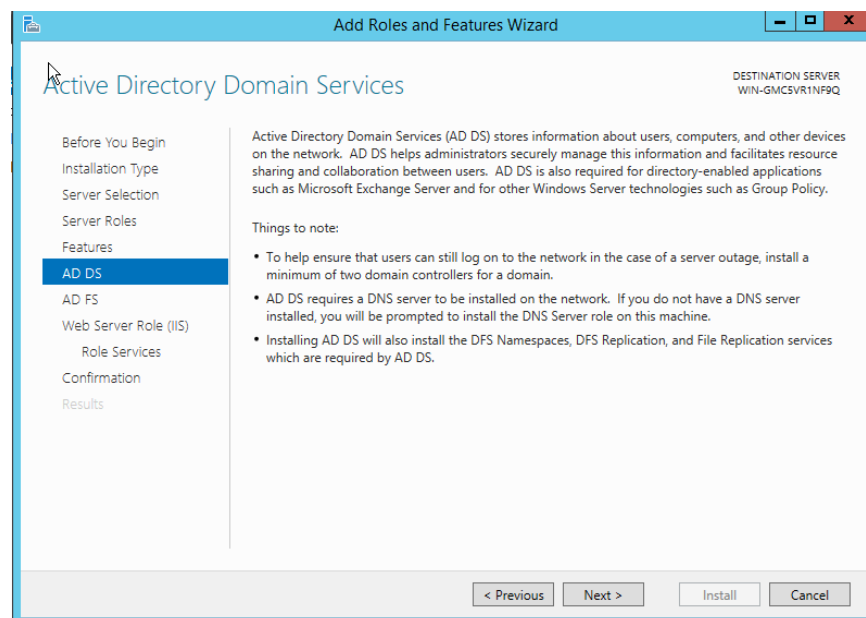
and Web IIS then click next



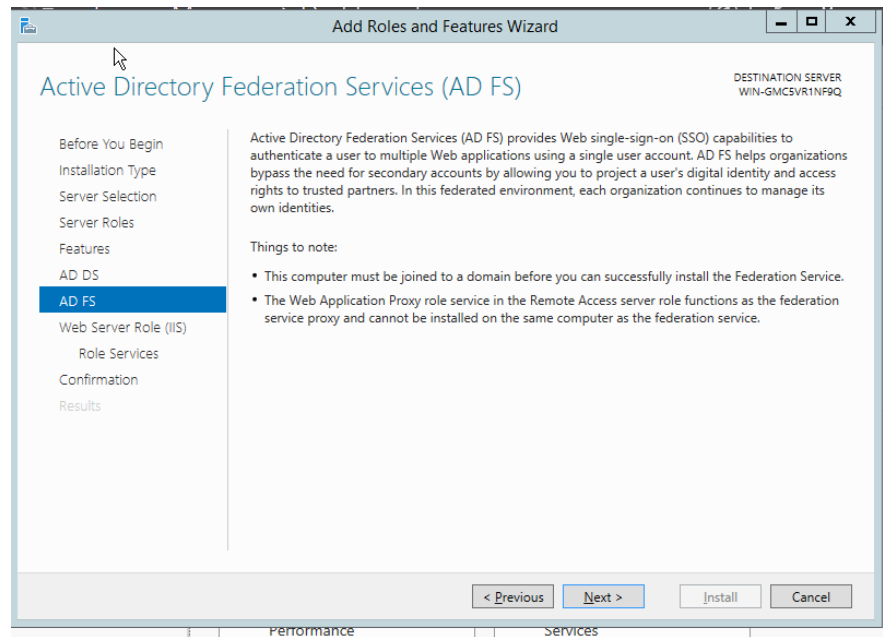
I. then in features click next



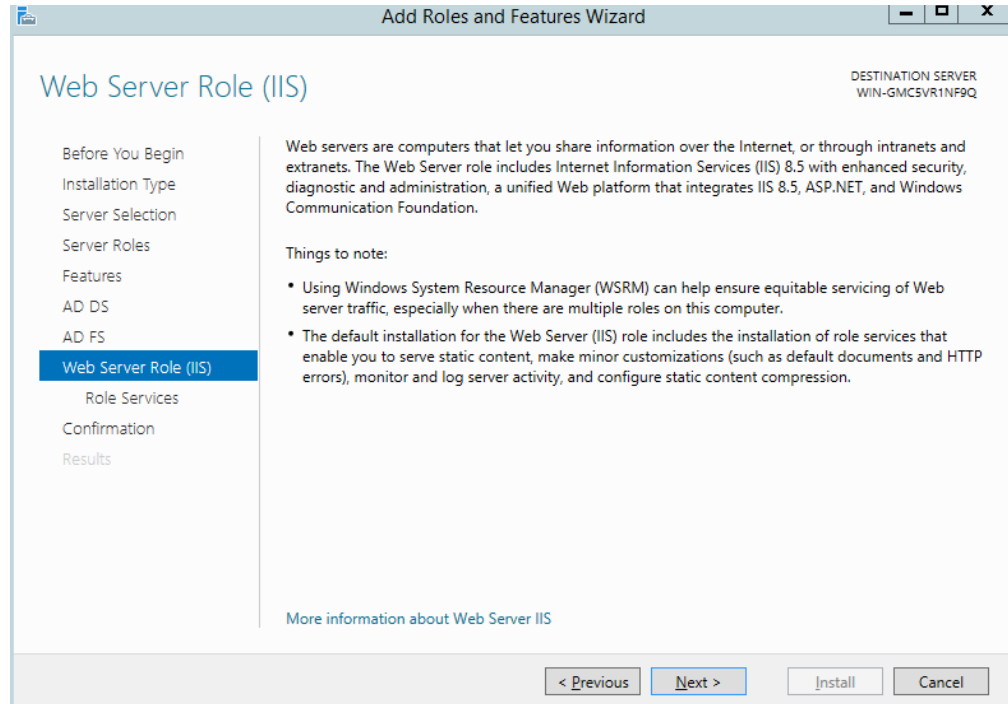
J. In AD DS click next



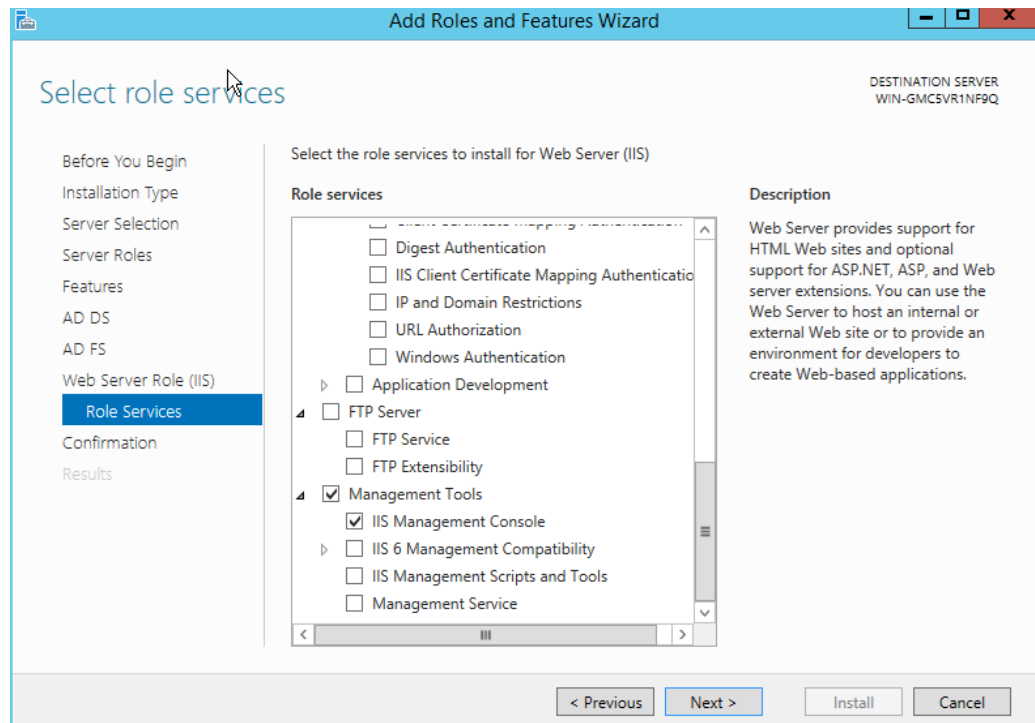
K. In AD FS click next



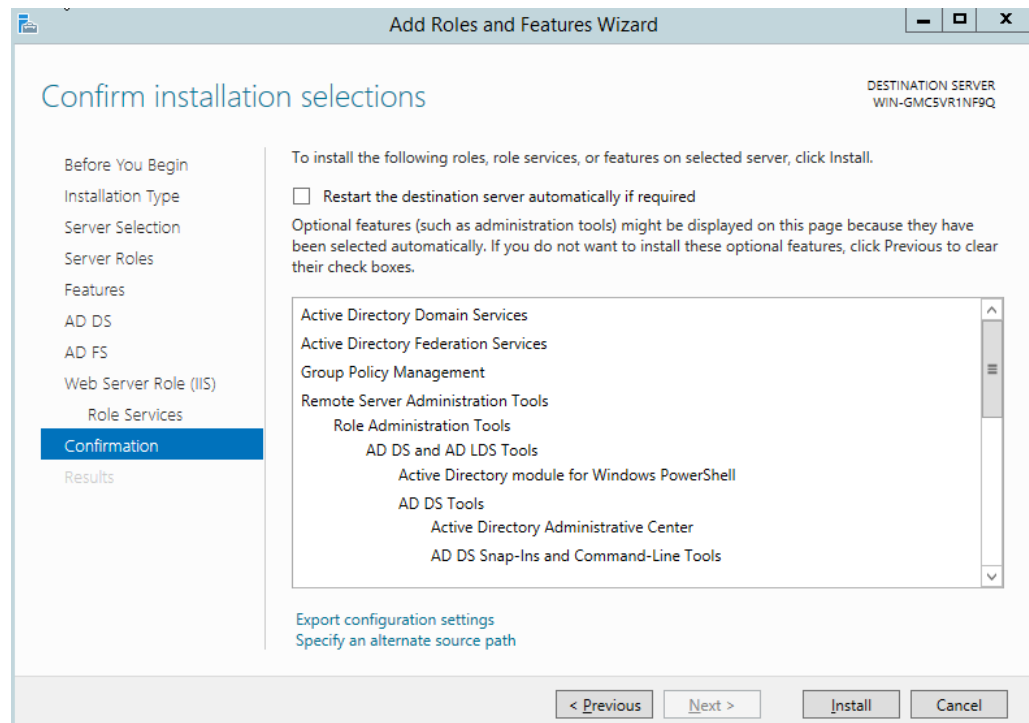
L. in Web Server Role (IIS) click next



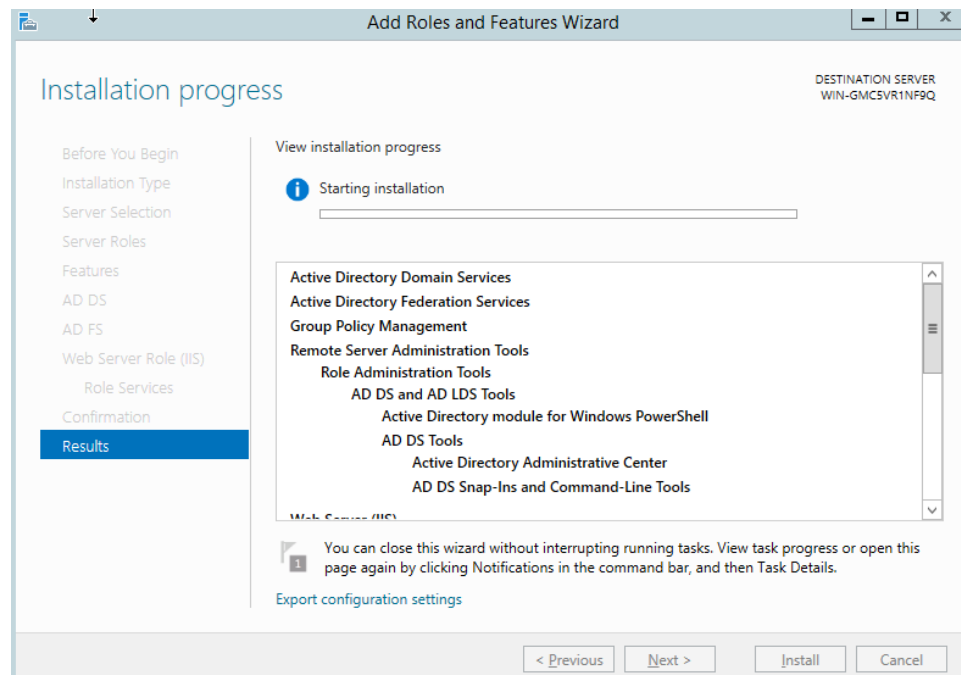
M. In role services click next



N. In confirmation click install

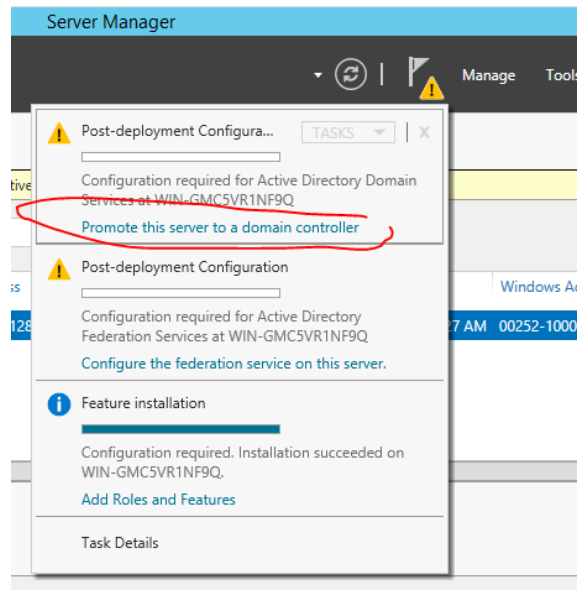


O. Wait for the installation to be finish then click close



Configuring Active Directory

- A. On the server management tool click on the flag and click on promote this server to domain controller



- B. On the deployment configuration select add a new forest and set Domain name “.” is required in specifying a domain name then click next

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes standard Windows window controls. The main title is 'Deployment Configuration'. On the left, a navigation pane lists steps: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area is titled 'Select the deployment operation' and contains three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected and circled in red). Below this, the section 'Specify the domain information for this operation' contains a text box for 'Root domain name:' with the value 'WHSADFS.com' entered (this text box is also circled in red). At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about deployment configurations' is located above the 'Next >' button.

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-GMCSVRINF9Q

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☐ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☒ Add a new forest

Specify the domain information for this operation

Root domain name: WHSADFS.com

More about deployment configurations

< Previous Next > Install Cancel

E. Specify a password for restore mode then click next

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window at the 'Domain Controller Options' step. The title bar is the same. The main title is 'Domain Controller Options'. The navigation pane on the left now has 'Domain Controller Options' selected. The main area is titled 'Select functional level of the new forest and root domain' and contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2012 R2'. Below this, the section 'Specify domain controller capabilities' contains three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). The section 'Type the Directory Services Restore Mode (DSRM) password' contains two password fields: 'Password:' and 'Confirm password:', both filled with dots. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about domain controller options' is located above the 'Next >' button.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-GMCSVRINF9Q

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

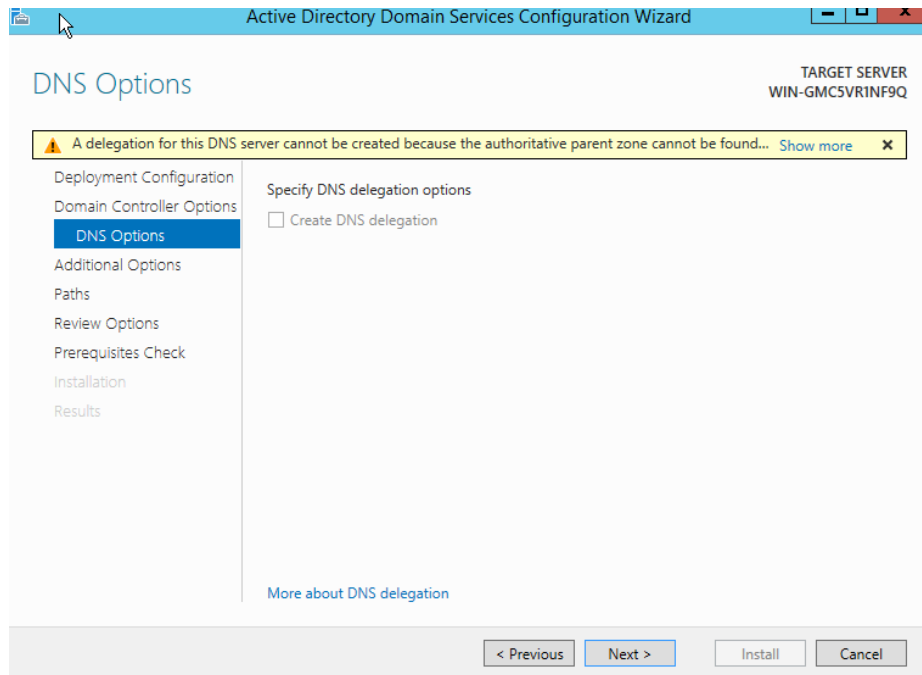
Password:

Confirm password:

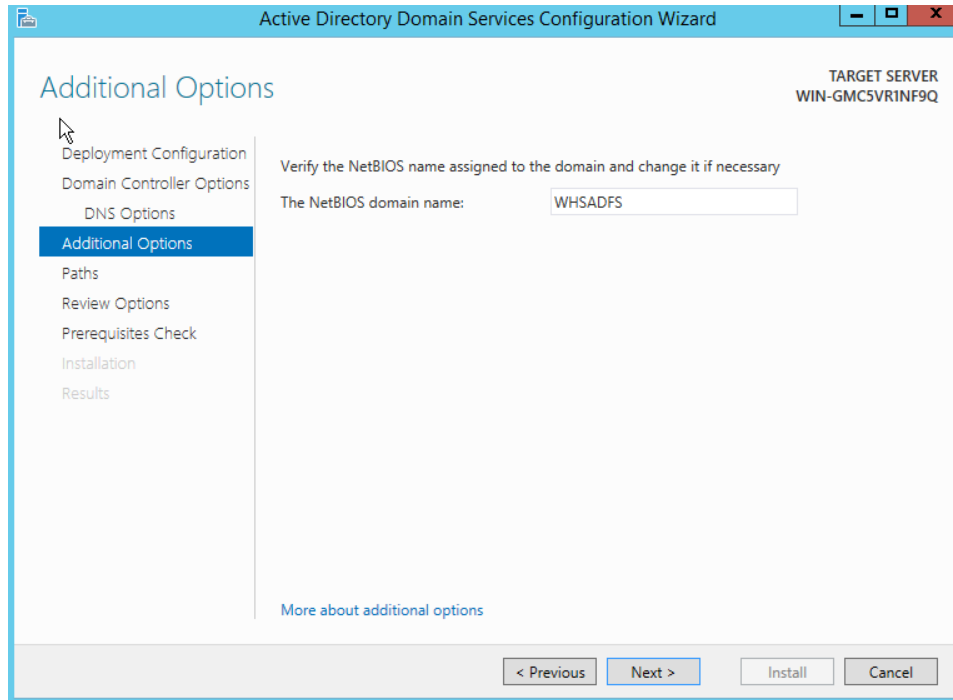
More about domain controller options

< Previous Next > Install Cancel

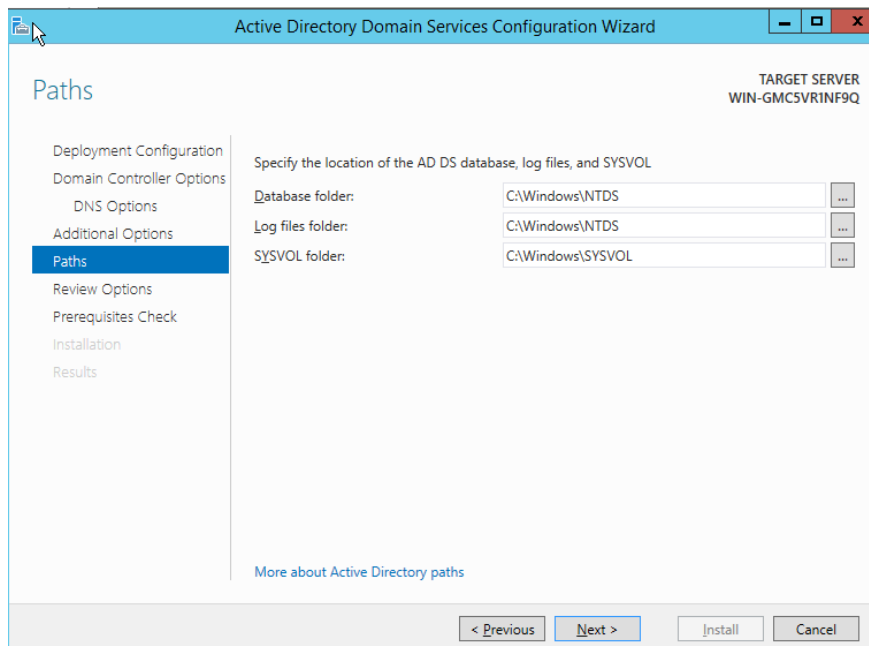
F. Click next on DNS options



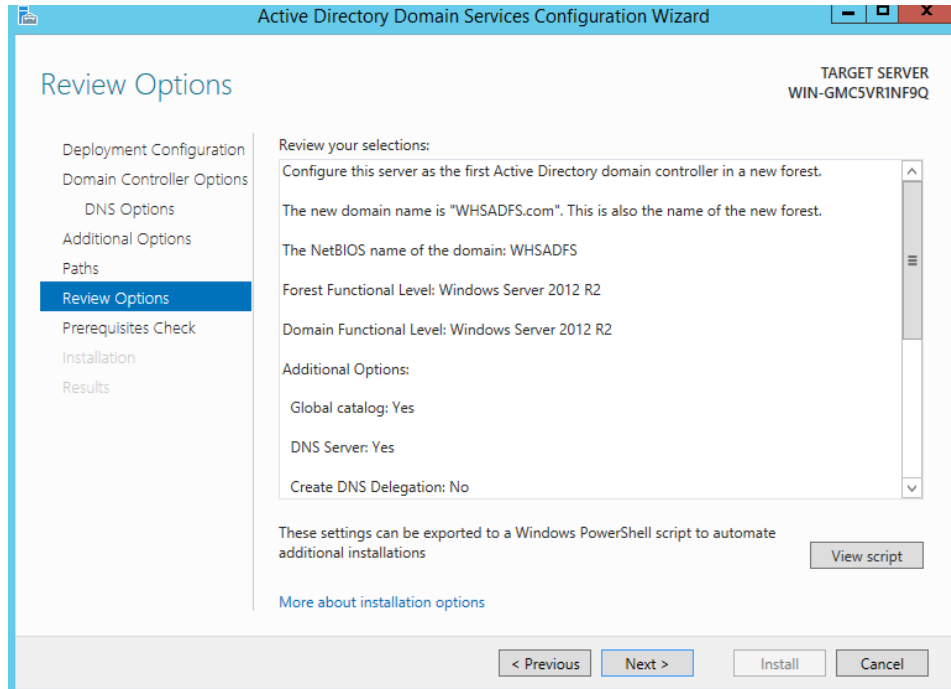
G. In Additional options click on Next



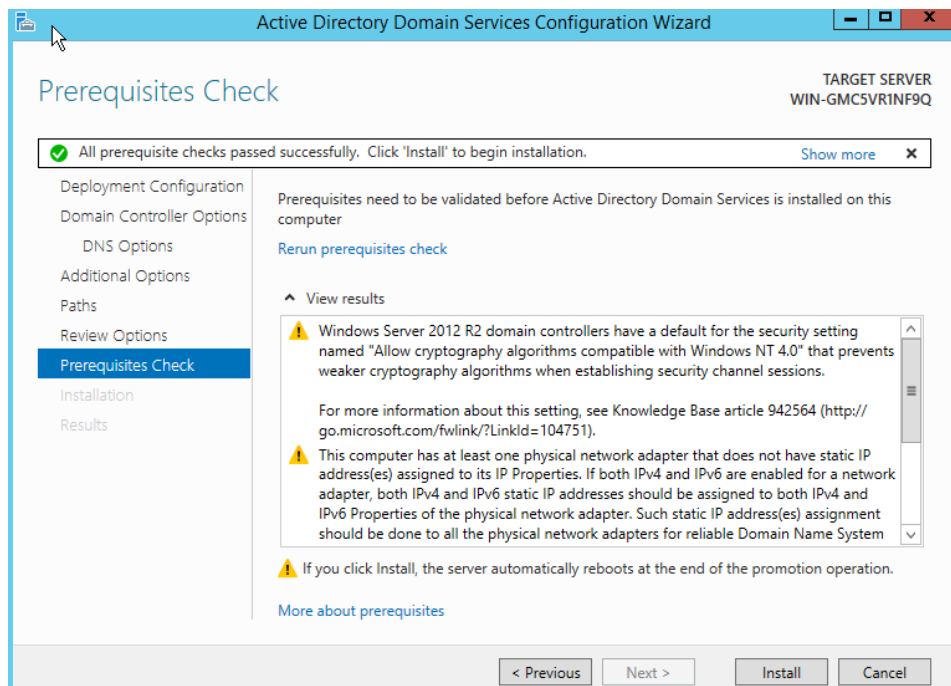
H. In specifying Paths click Next



I. In review options click Next



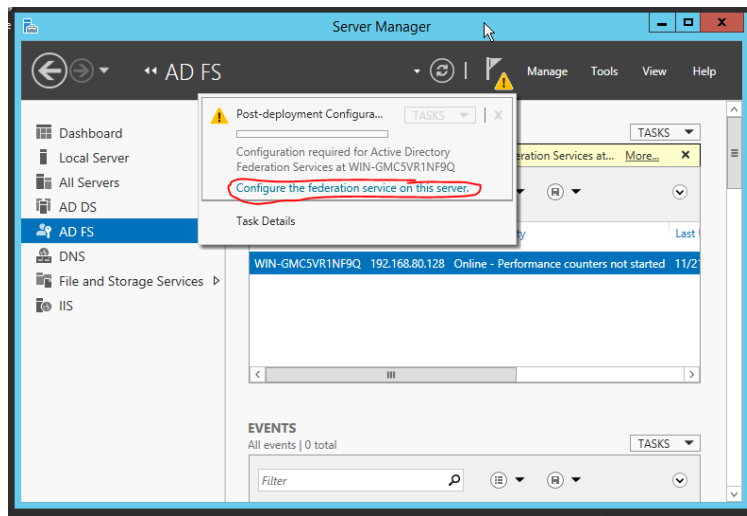
J. In prerequisites click on install



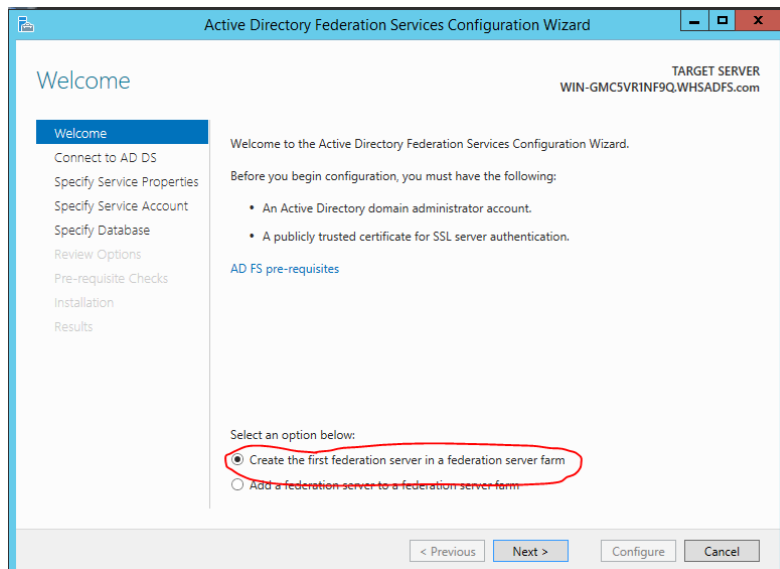
K. Wait for the installation to be completed and the server will restart automatically.

Configuring AD FS

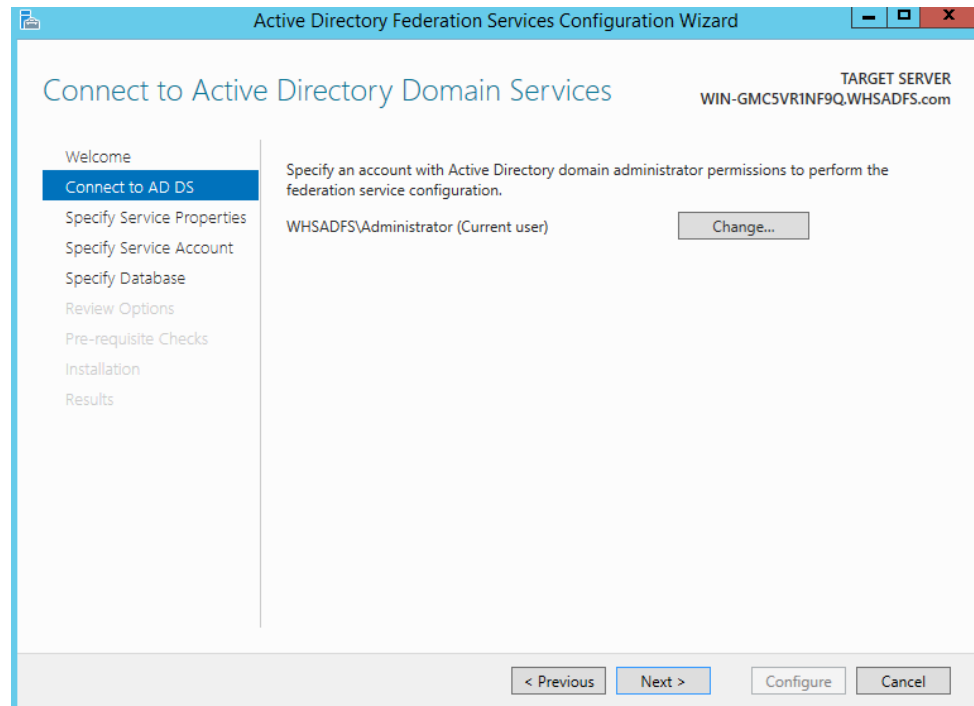
A. In server Manager click on the flag and you will see an post- deployment configuration for active directory federation services



B. This will redirected to Active Directory Federation Services Configuration Wizard. Select create the first federation server in federation server farm then click next

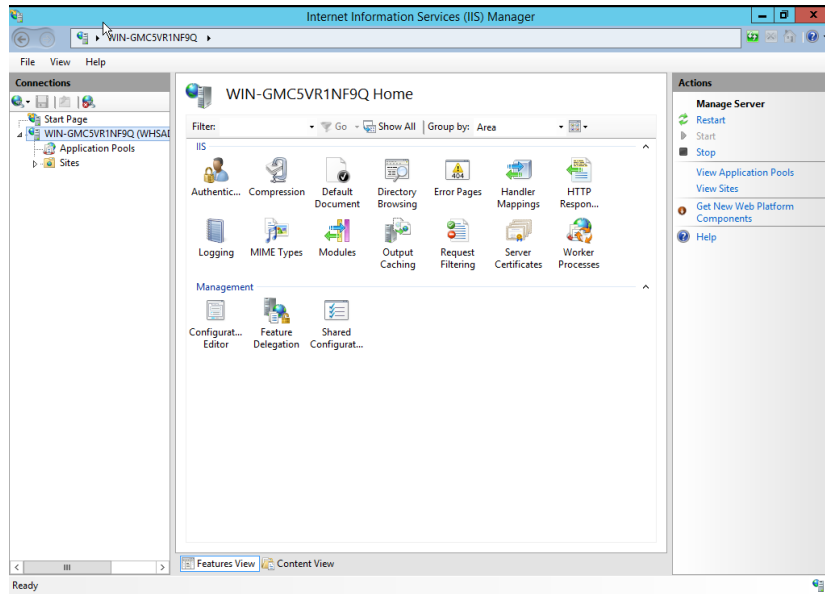


- C. Specify the admin we want to use to perform the federation services configuration
Then click next (we may use the account we created earlier)

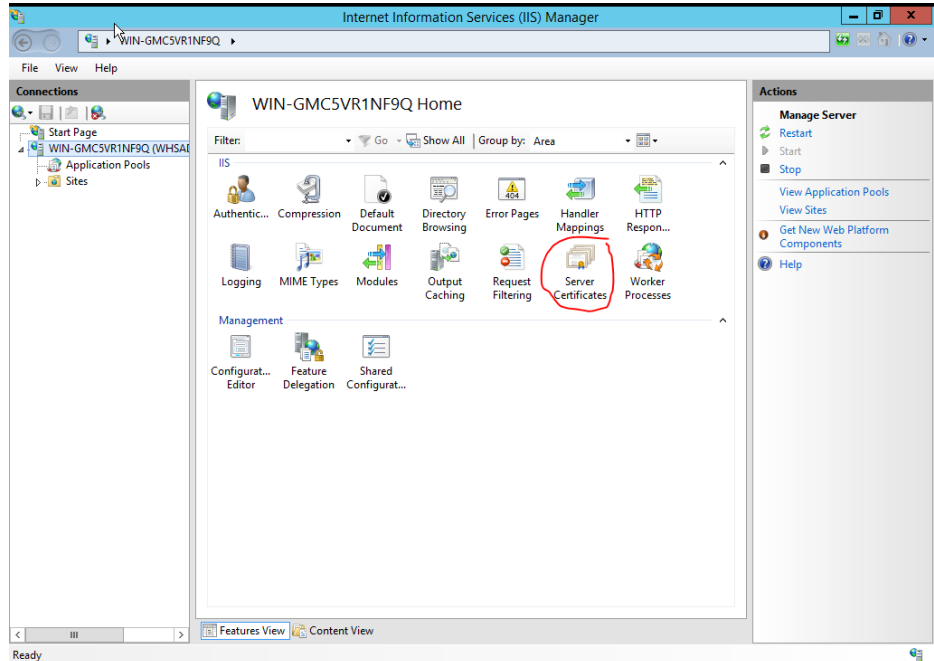


D. Importing SSL Certificate and assigning federation service name

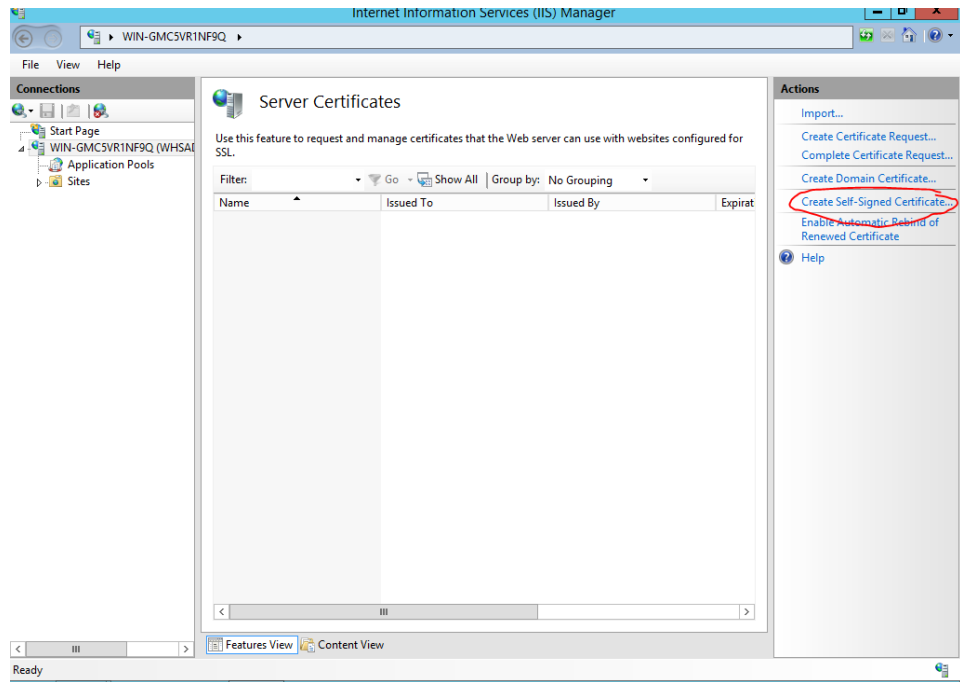
- To create an self sign SSL certificate go to IIS by searching IIS to windows search bar.



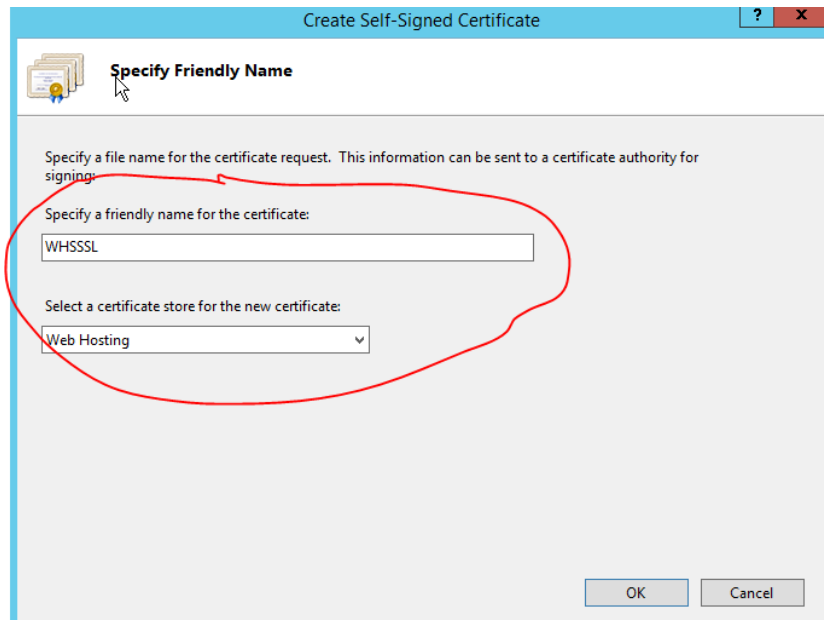
- In IIS manager click on Server Certificates



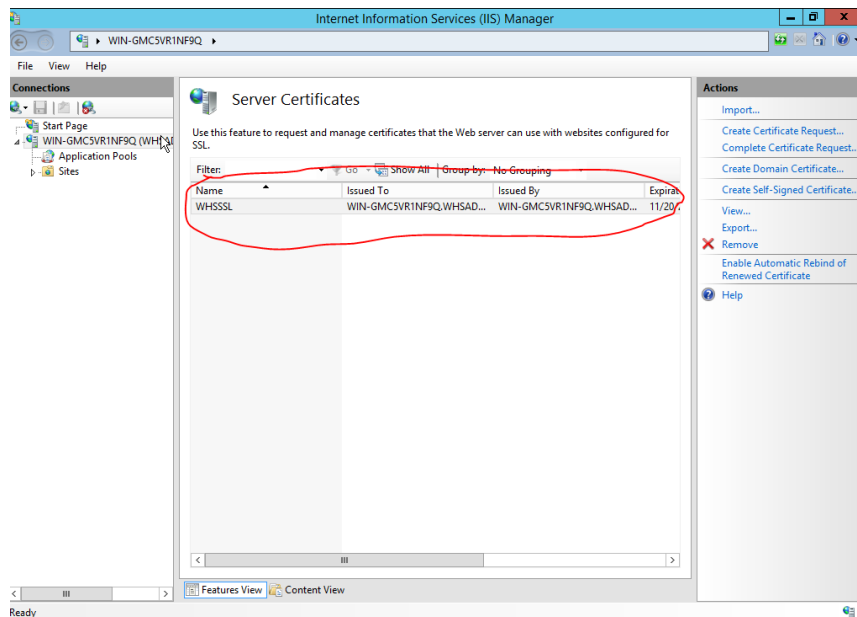
- On the right side of the IIS click on Create Self Signed Certificate



- Specify the name of certificate and select web hosting in select a certificate store for the new certificate. then click ok



- You will see that the certificate will be created in the Server Certificates.

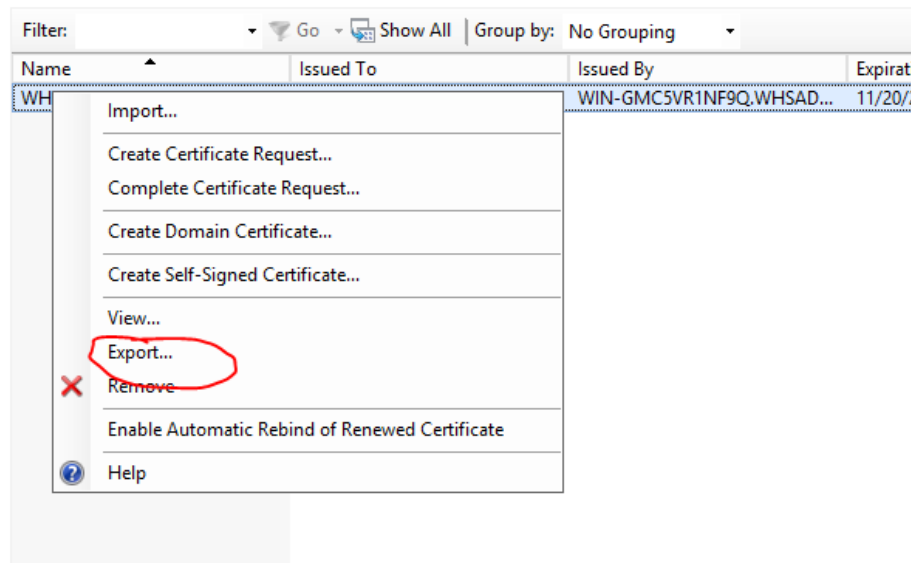


- Right click on the newly created SSL and click on export

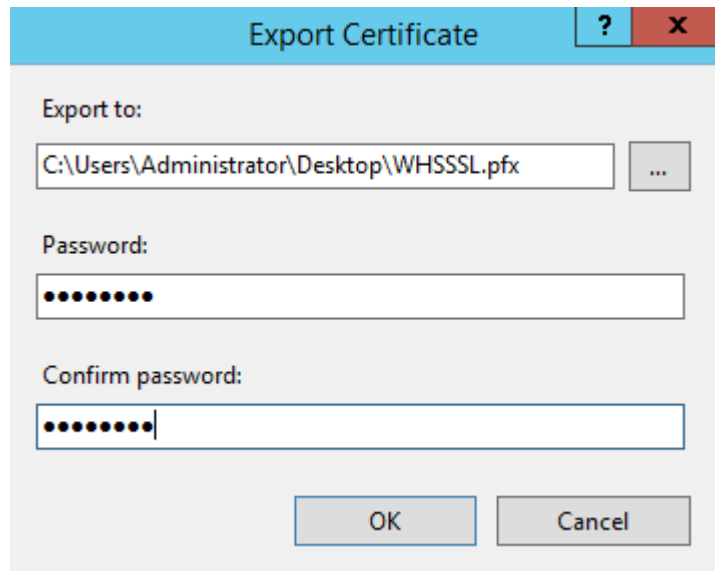


Server Certificates

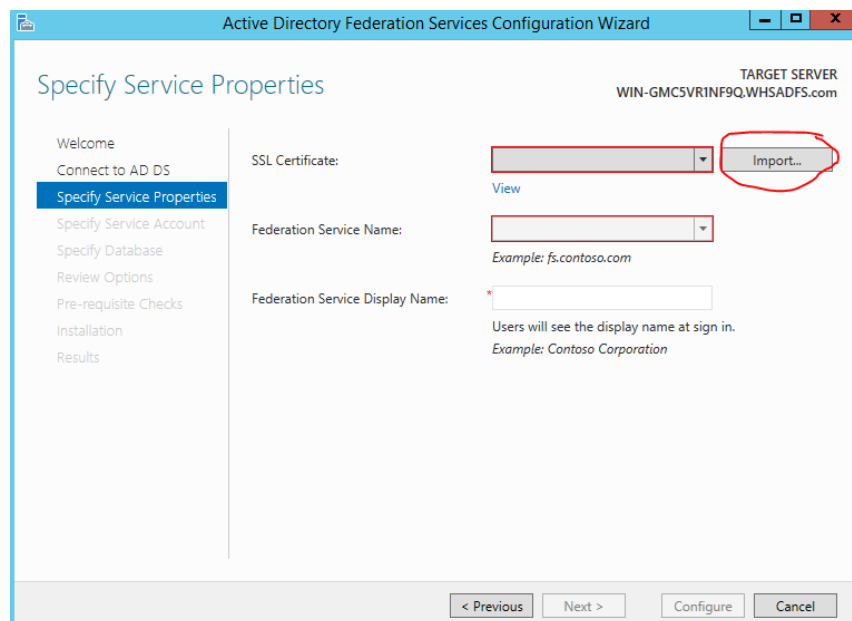
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

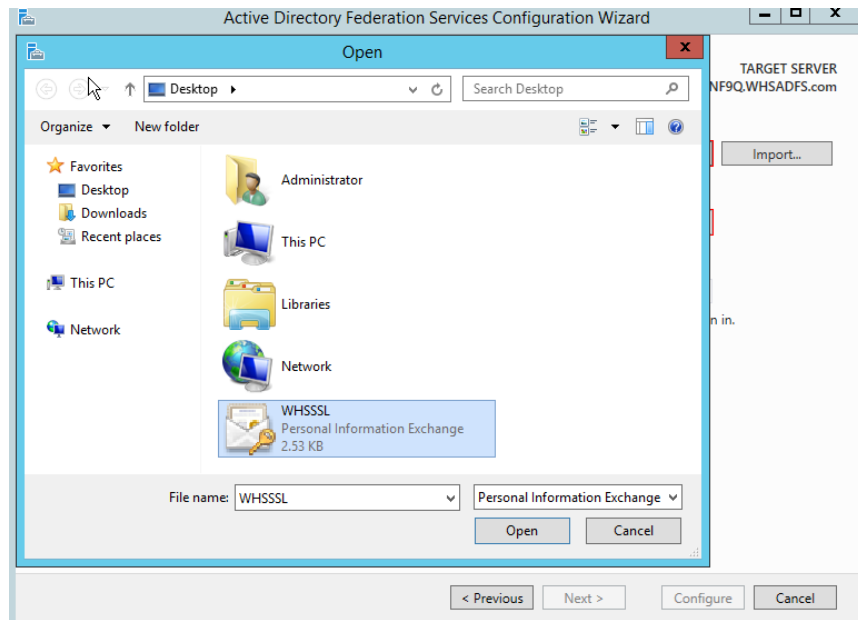


- A pop up will show and will ask to assign where will the SSL be exported to and will also ask for a password then click ok

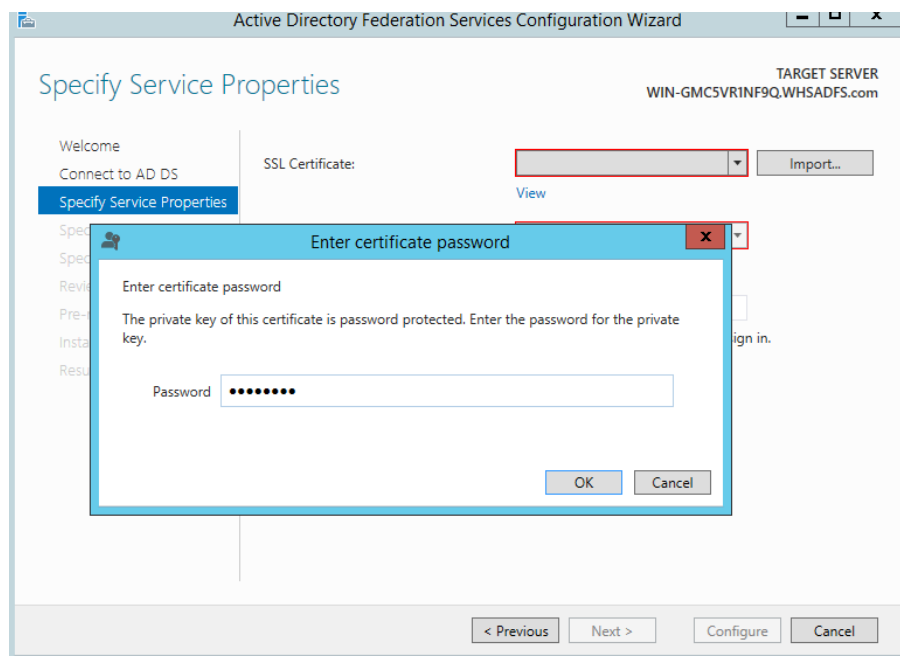


- Go back to the Active Directory Federation Services Configuration Wizard page on the SSL Certificate click on import and locate the directory where we put the exported SSL then click open.





- It will ask a password, just key in the password we assign earlier

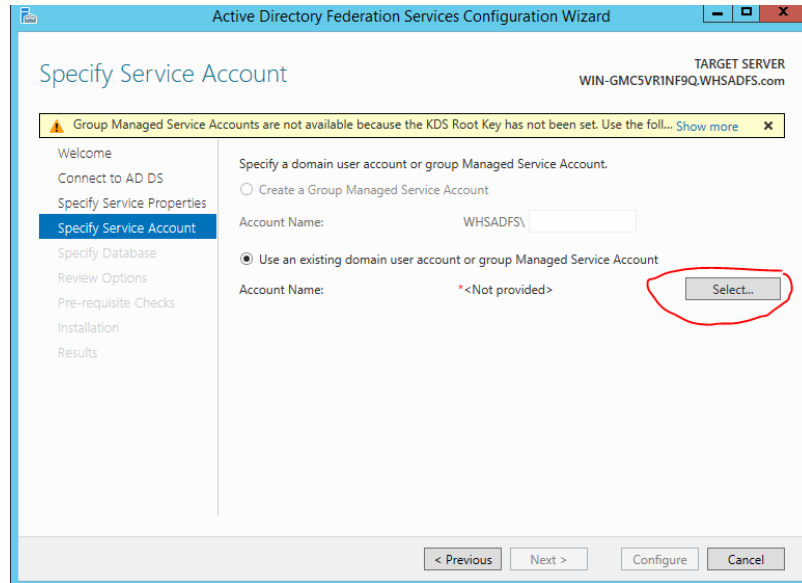


- Lastly assign the federation service display name then click next

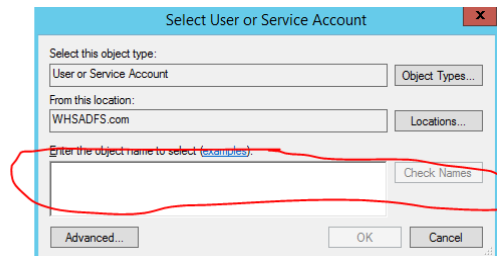
The screenshot shows the 'Active Directory Federation Services Configuration Wizard' window. The title bar reads 'Active Directory Federation Services Configuration Wizard'. The main window has a blue header with the title 'Specify Service Properties'. On the left is a navigation pane with the following items: 'Welcome', 'Connect to AD DS', 'Specify Service Properties' (highlighted in blue), 'Specify Service Account', 'Specify Database', 'Review Options', 'Pre-requisite Checks', 'Installation', and 'Results'. On the right, the 'TARGET SERVER' is listed as 'WIN-GMC5VR1NF9Q.WHSADFS.com'. Below this, there are three fields: 'SSL Certificate:' with a dropdown menu showing 'WIN-GMC5VR1NF9Q.WHSADFS' and an 'Import...' button; 'Federation Service Name:' with a dropdown menu showing 'WIN-GMC5VR1NF9Q.WHSADFS' and a 'View' link below it; and 'Federation Service Display Name:' with a text box containing 'WHS ADFS'. Below the text box is a note: 'Users will see the display name at sign in. Example: Contoso Corporation'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'Next >' button is highlighted in blue.

E. Specify a service account just like earlier we can use the admin account we created when we install the windows server.

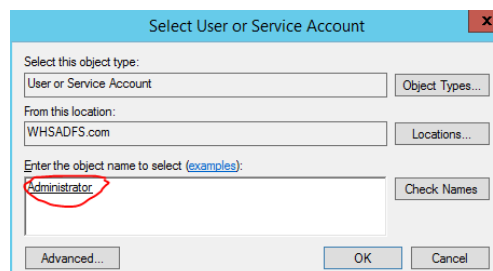
- Click on select



- Specify the account we will use on the enter the object name to select



- Key in the user we will be using we can type in admin then click on check name so that it will automatically put the user on the text area. Please ensure that there is an underline with in the username then click ok.



F. Specify service account will ask for a account password. Then click next

Active Directory Federation Services Configuration Wizard

TARGET SERVER
WIN-GMC5VRINF9Q.WHSADFS.com

Specify Service Account

Group Managed Service Accounts are not available because the KDS Root Key has not been set. Use the following options. [Show more](#)

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a domain user account or group Managed Service Account.

☐ Create a Group Managed Service Account

Account Name: WHSADFS\

☒ Use an existing domain user account or group Managed Service Account

Account Name: WHSADFS\Adminis...

Account Password:

< Previous Next > Configure Cancel

G. Specify Configuration of database. Select create a database on this server using windows internal database. Then click next.

Active Directory Federation Services Configuration Wizard

TARGET SERVER
WIN-GMC5VRINF9Q.WHSADFS.com

Specify Configuration Database

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a database to store the Active Directory Federation Service configuration data.

☒ Create a database on this server using Windows Internal Database.

☐ Specify the location of a SQL Server database.

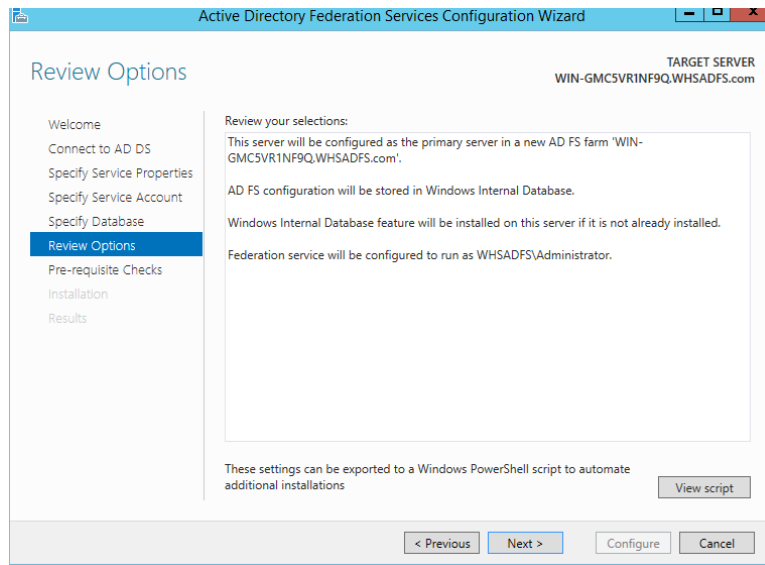
Database Host Name:

Database Instance:

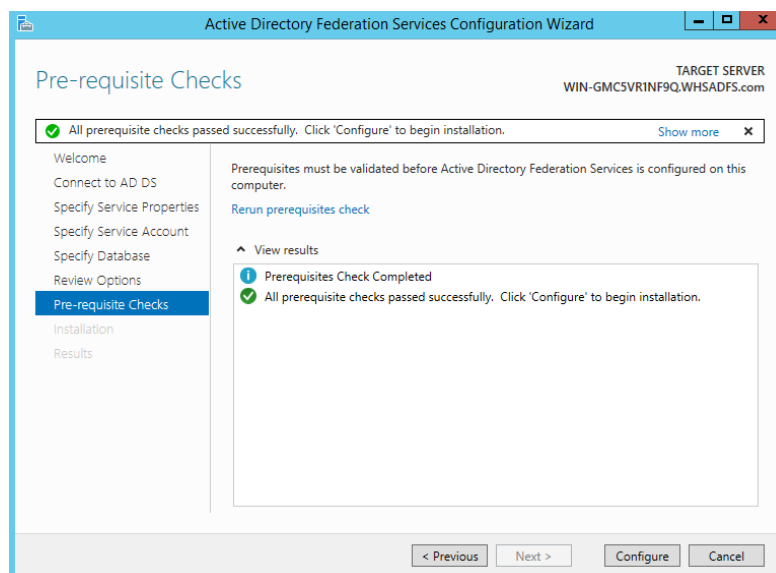
To use the default instance, leave this field blank.

< Previous Next > Configure Cancel

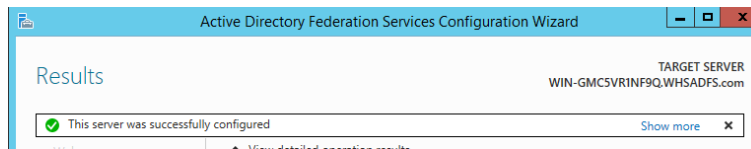
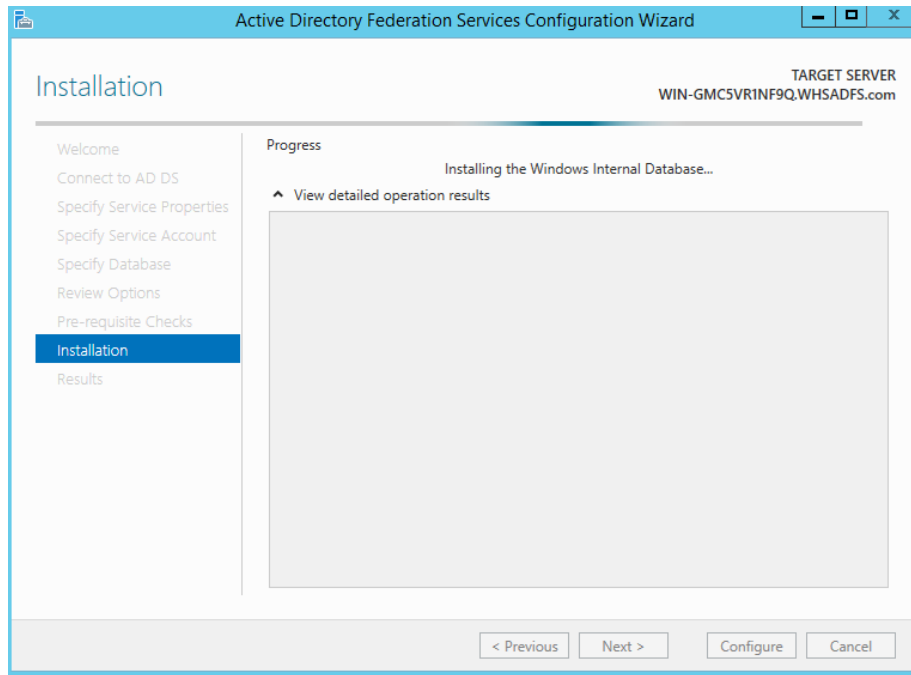
H. Review Options, click on next



I. Prerequisite check, click on configure

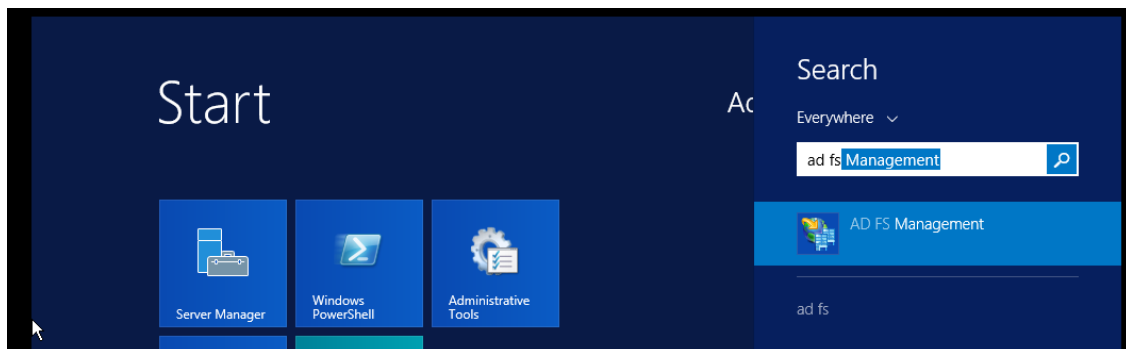


J. wait for the installation to be finish.

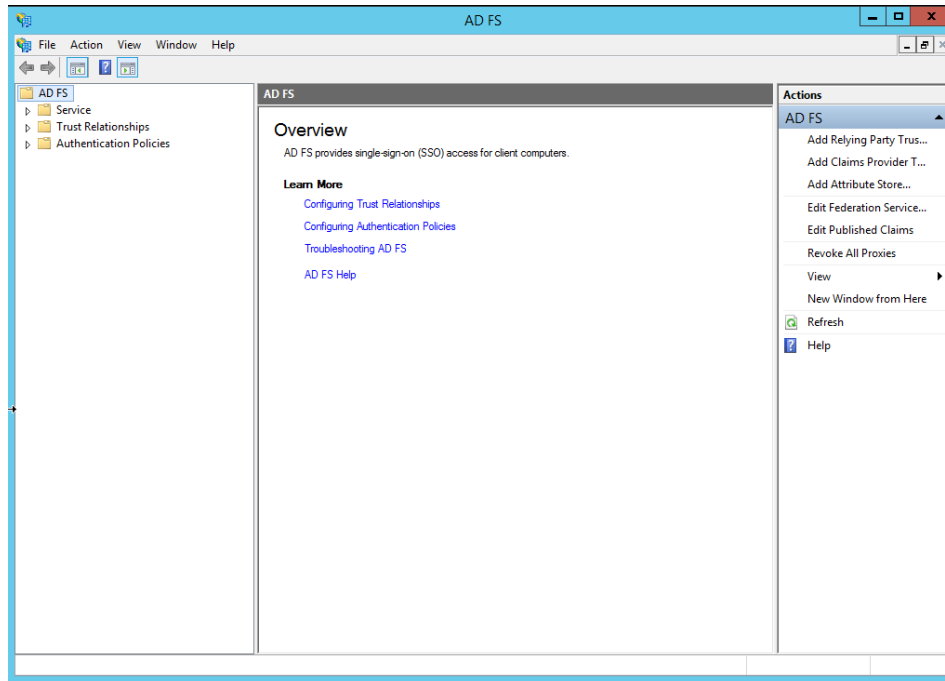


Specifying Relying Party Trusts

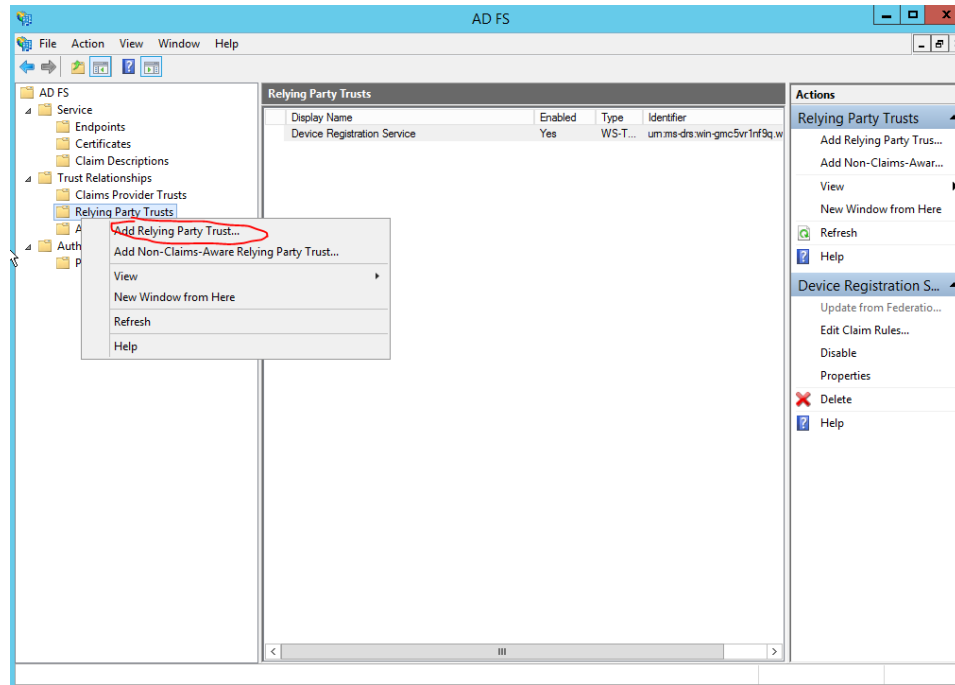
A. In windows search type in ad fs, AD FS Management will be shown then click it.



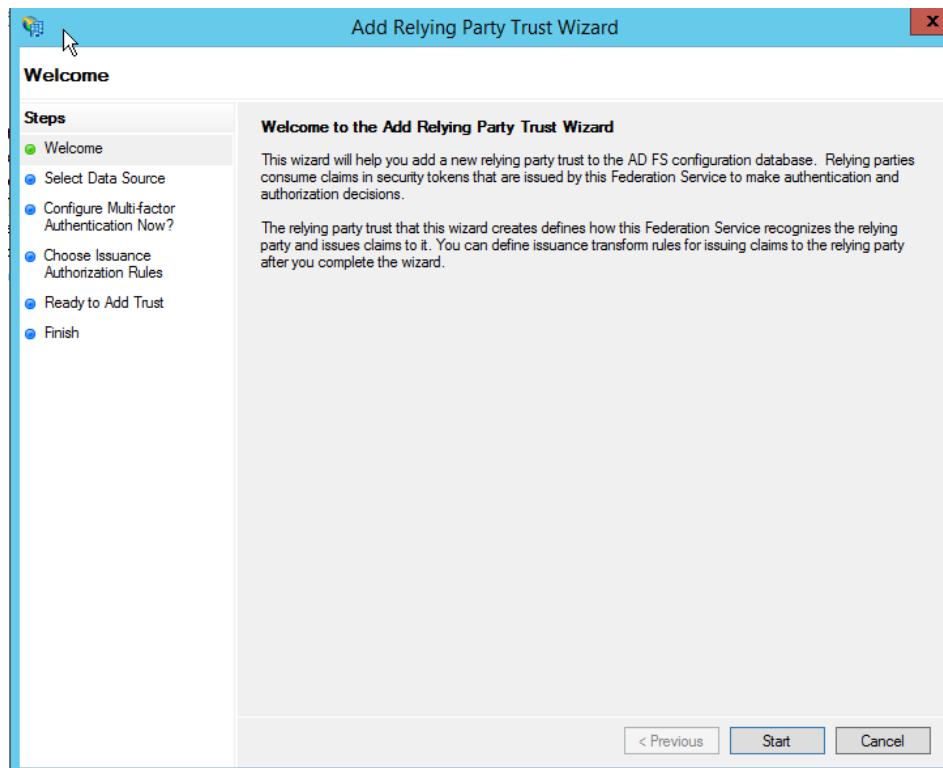
B. AD FS management will be shown



C. on the left side right click Trust Relationships > Relying Party Trusts then click Add Relying Party Trust



D. Add Relying Party Trust wizard will be shown then click start.



enter

E. Select data

about the relying party manually.then click next

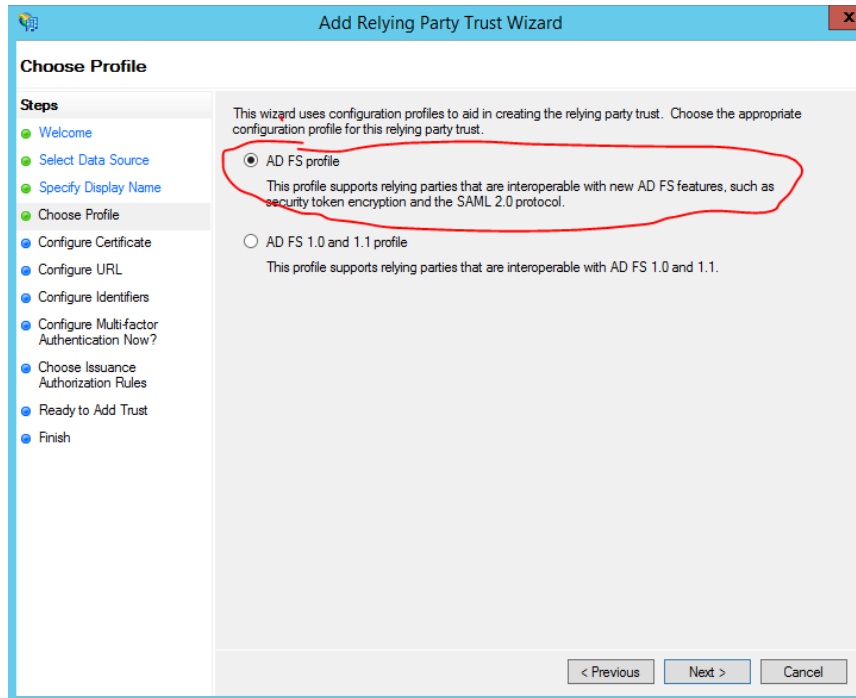
The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Select Data Source' step. On the left, a 'Steps' pane lists the wizard's progression: Welcome, Select Data Source (current), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains three radio button options. The first option, 'Import data about the relying party published online or on a local network', is unselected. The second option, 'Import data about the relying party from a file', is also unselected. The third option, 'Enter data about the relying party manually', is selected and circled in red. Below the selected option is a text box for 'Federation metadata file location' and a 'Browse...' button. At the bottom of the window are '< Previous', 'Next >', and 'Cancel' buttons.

F. Specify the

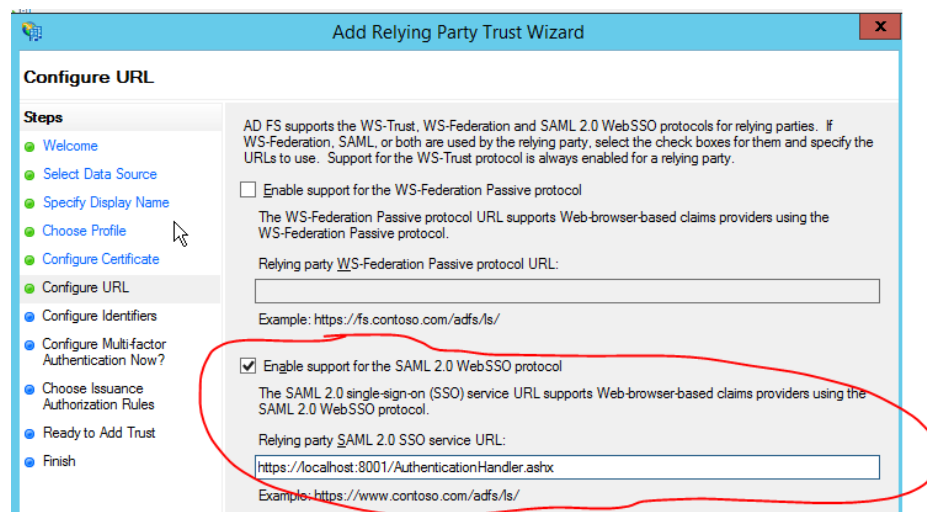
name we want to be display on the SSO login page. Then click next

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The 'Steps' pane on the left shows the progression, with 'Specify Display Name' now highlighted. The main area has a heading 'Specify Display Name' and a sub-instruction 'Enter the display name and any optional notes for this relying party.' Below this is a 'Display name:' label followed by a text box containing the text 'WHS', which is circled in red. Underneath the text box is a 'Notes:' label followed by a large text area. At the bottom of the window are '< Previous', 'Next >', and 'Cancel' buttons.

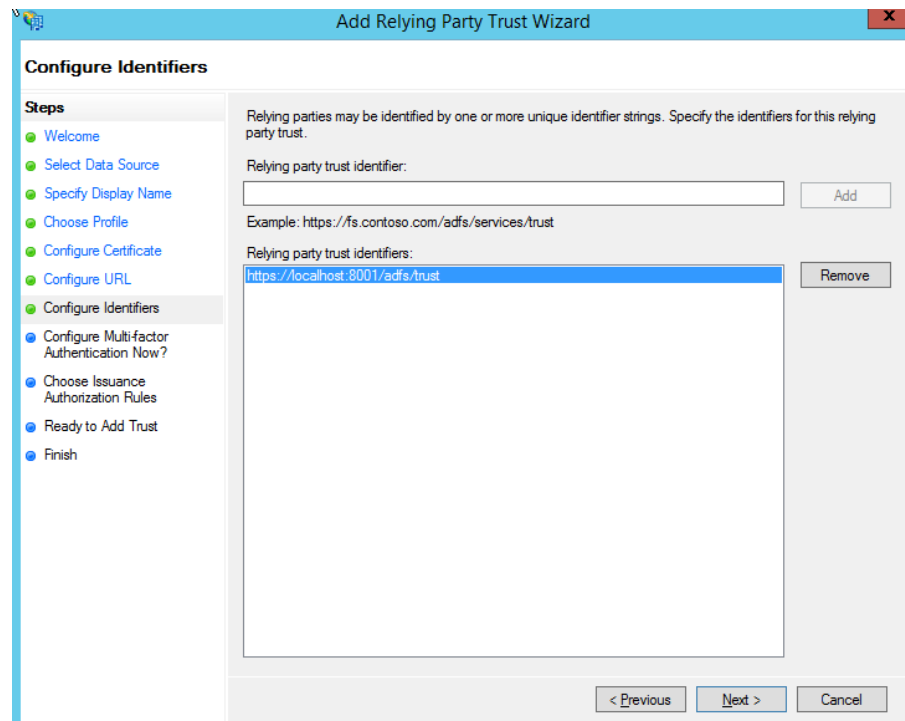
G. Select AD FS profile then click next.



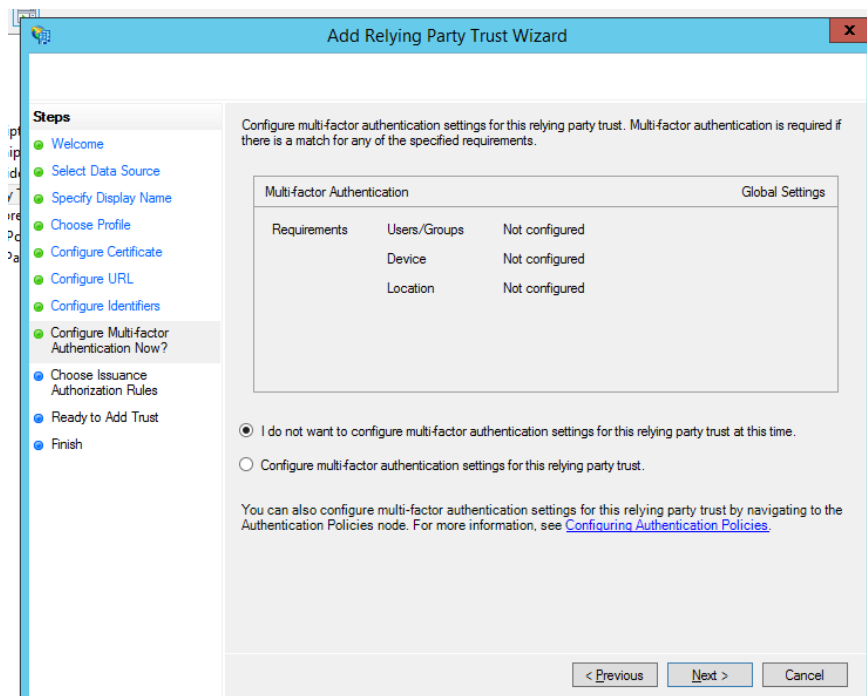
H. Configure Url check enable support SAML 2.0 WebSSO protocol and key in the application url we need to specify the url of WHS in this then click next



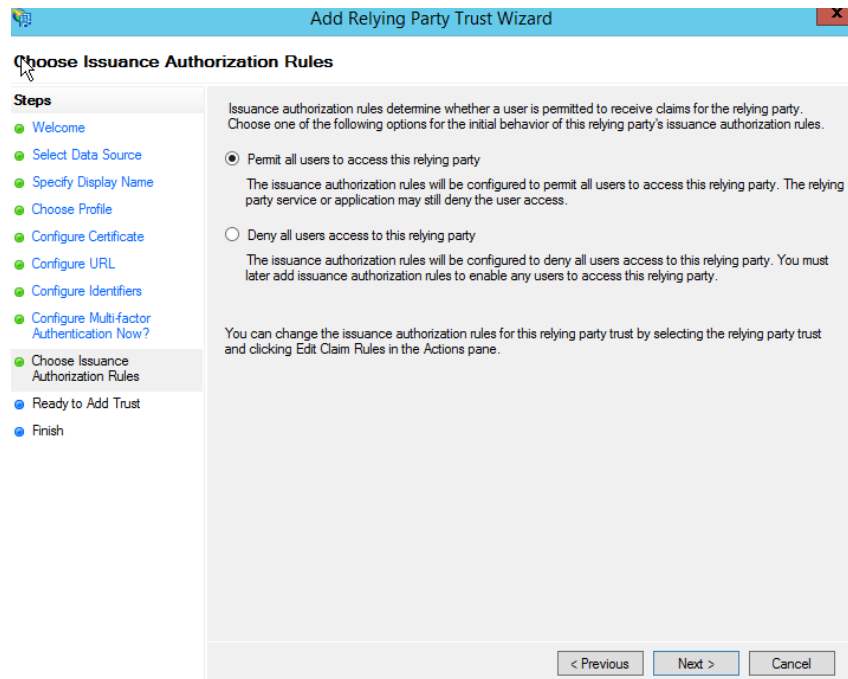
I. Add trust url this is also WHS application url. Then click next



J. Selects I do not want to configure multi-factor authentication settings then click next



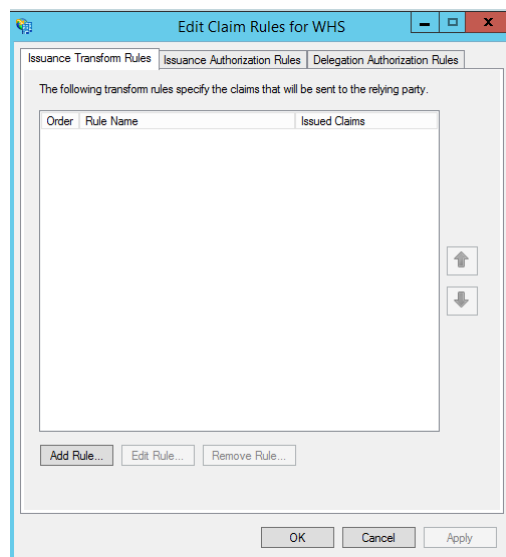
K. Click on Permit all users to access the relying party.



The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Choose Issuance Authorization Rules' step. On the left, a 'Steps' pane lists the wizard's progression: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules (the current step), Ready to Add Trust, and Finish. The main area contains instructions: 'Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.' Two radio buttons are present: 'Permit all users to access this relying party' (which is selected) and 'Deny all users access to this relying party'. Below these, explanatory text states that the 'Permit' option allows all access, while the 'Deny' option restricts access, requiring further rule configuration. A note at the bottom mentions that rules can be changed later via the 'Edit Claim Rules' action. Navigation buttons at the bottom right include '< Previous', 'Next >', and 'Cancel'.

L. Click on Next then Click on finish

M. Edit claim rules for WHS will be displayed



The screenshot displays the 'Edit Claim Rules for WHS' window. It features three tabs: 'Issuance Transform Rules', 'Issuance Authorization Rules' (the active tab), and 'Delegation Authorization Rules'. The active tab contains the text: 'The following transform rules specify the claims that will be sent to the relying party.' Below this is a table with columns 'Order', 'Rule Name', and 'Issued Claims'. The table is currently empty. To the right of the table are up and down arrow buttons for reordering. At the bottom of the table area are buttons for 'Add Rule...', 'Edit Rule...', and 'Remove Rule...'. The bottom of the window has 'OK', 'Cancel', and 'Apply' buttons.

M. Click on add rule add transformation claim rule wizard will be shown. Select Send LDAP Attributes as claim in claim rule template, then click next.

Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule**

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:
Send LDAP Attributes as Claims

Claim rule template description:
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous Next > Cancel

N. Set claim rule name and the items we want to use as authentication module in WHS. then click finish

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule**

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Username claim

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

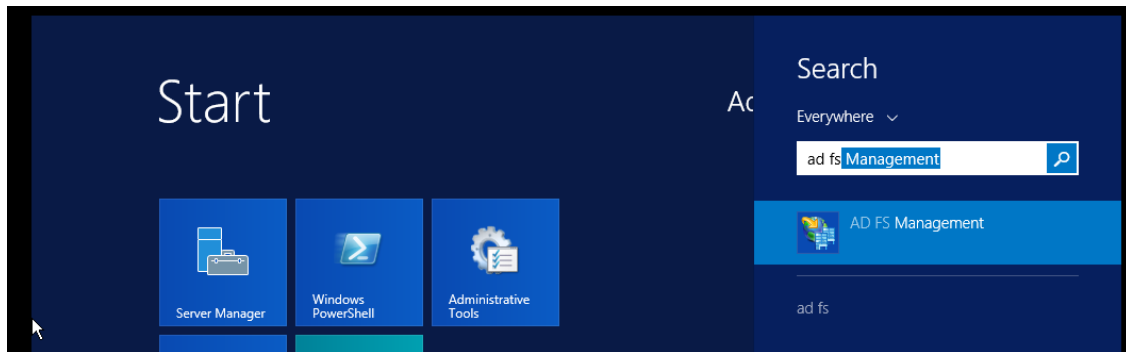
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

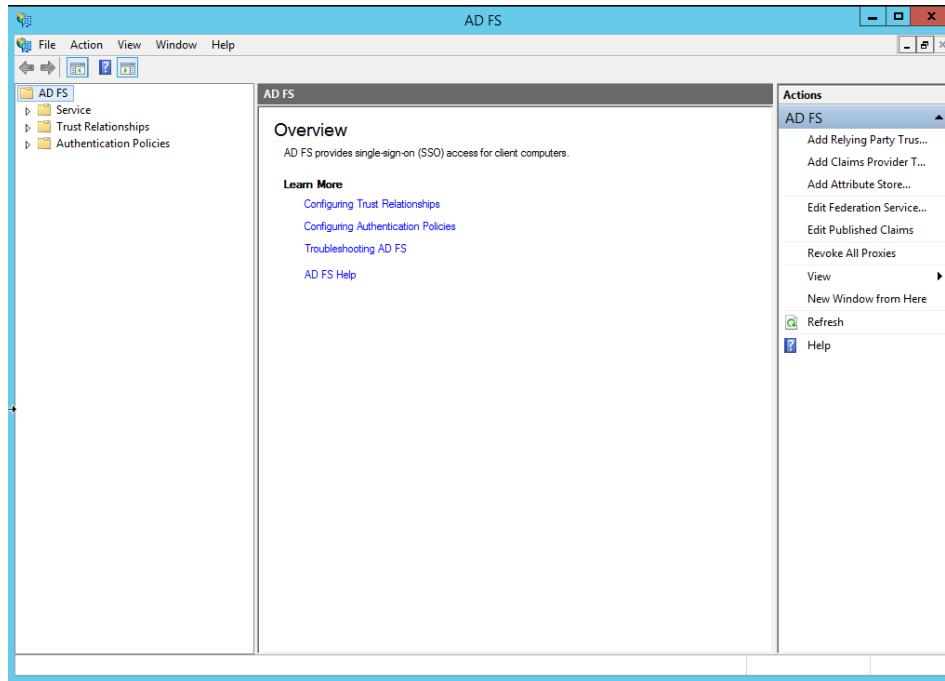
O. Click on restart.

Trying AD FS

A. In windows search type in ad fs, AD FS Management will be shown then click it.



B. AD FS management will be shown



C. check

the following if enable on the left side click on Service > Endpoint check on
/adfs/ls and /federationMetadata/2007-06/FederationMetadata.xml

Enabled	Proxy Enabled	URL Path	Type
Token Issuance			
Yes	Yes	/adfs/ls/	SAML 2.0/WS-F
No	No	/adfs/services/trust/2005/windows	WS-Trust 2005
No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005
Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005
No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005
Yes	Yes	/adfs/services/trust/mex	WS-MEX
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metac
Yes	No	/adfs/ls/federationsservice.asmx	ADFS 1.0 Metad

D. In the pc that is hosting the VMWare try to access the adfs/ls and
/federationMetadata/2007-06/FederationMetadata.xml by using the
https://{pcname}/adfs/ls or
https://{pcname}/federationMetadata/2007-06/FederationMetadata.xml