**Lab - Install a Read-Only Domain Controller (RODC) 2012R2**

**Overview**

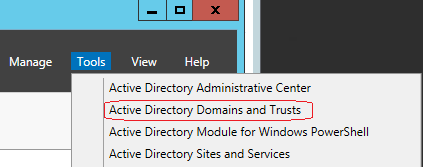
Read-only domain controllers (RODC) are ideal in a remote location where system security cannot be guaranteed. They allow the remote site to have local authentication point, without storing vulnerable data about objects in the domain. The only information stored on a read-only domain controller is that of users and computers it has been authorized to authenticate. Any other object that is queried or authorized against is forwarded by the read-only DC to writable domain controller.

**Lab Requirements**

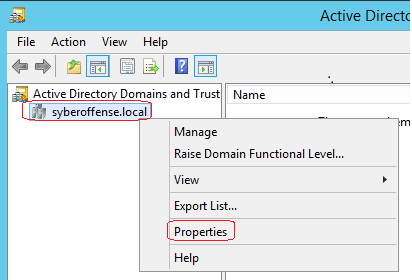
* A fresh install of Server 2012 R2 as a virtual machine joined to an existing domain.
* Forest function level should be windows 2003 server or higher
* **A**t least one writable domain controller running windows server 2008 or higher

**Check the forest function level**

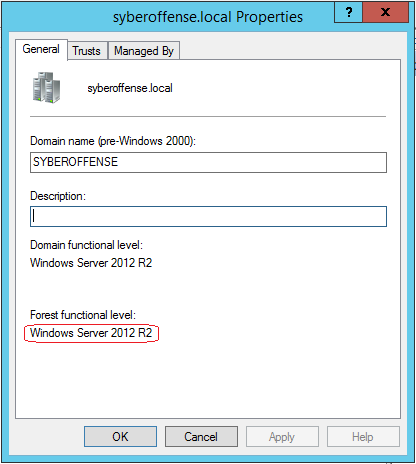
Open Server Manager and click on tools. From the context menu, select Active Directory Domain and Trusts.

****

Right-click on the name of your domain and select properties.

****

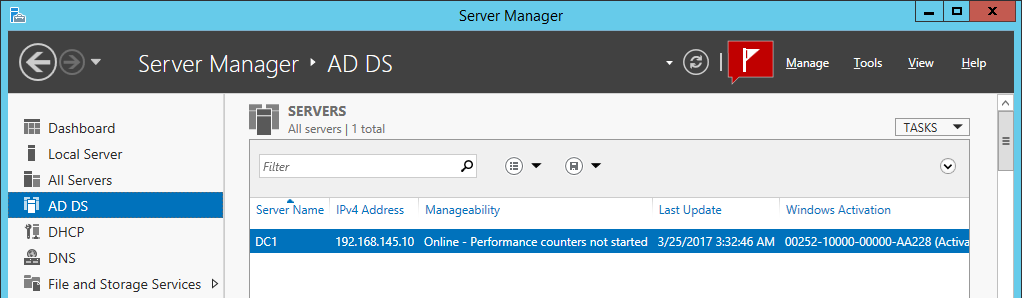
On the domain properties page, you can check the forest functional level. This means no additional domain prep is needed.

****

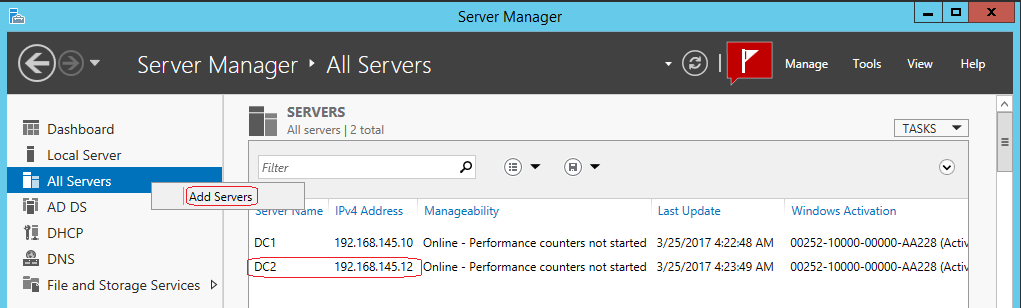
I have joined my new server DC2, to the domain as a member server. Joining a Windows machine to the domain was covered in a previous lab.



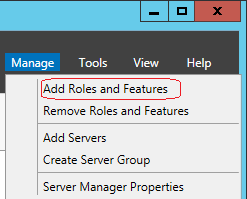
Ensure that you are logged onto to a domain controller in your existing domain using your domain administrator account. For this lab, I have logged on to my root domain controller, DC1.



Right-click on **All Servers** and select **Add Servers**. Find all and select your new member server and add to the existing server pool.

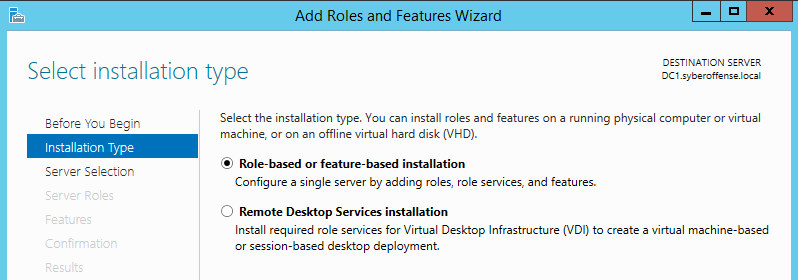
****

Open Server Manager and click on **Manage** and select, **Add roles and Features**.

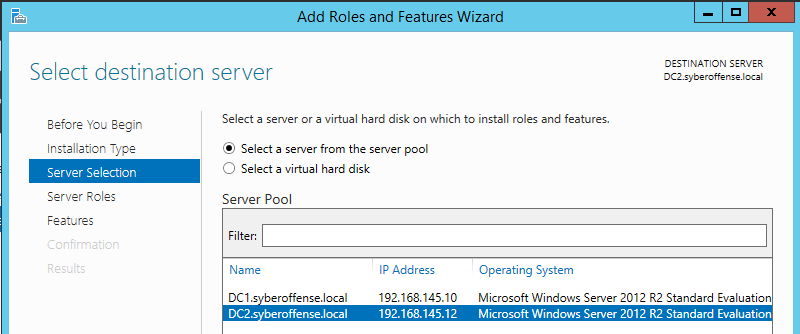
****

The **Add Roles and Features Wizard** opens. Click **next** to continue.

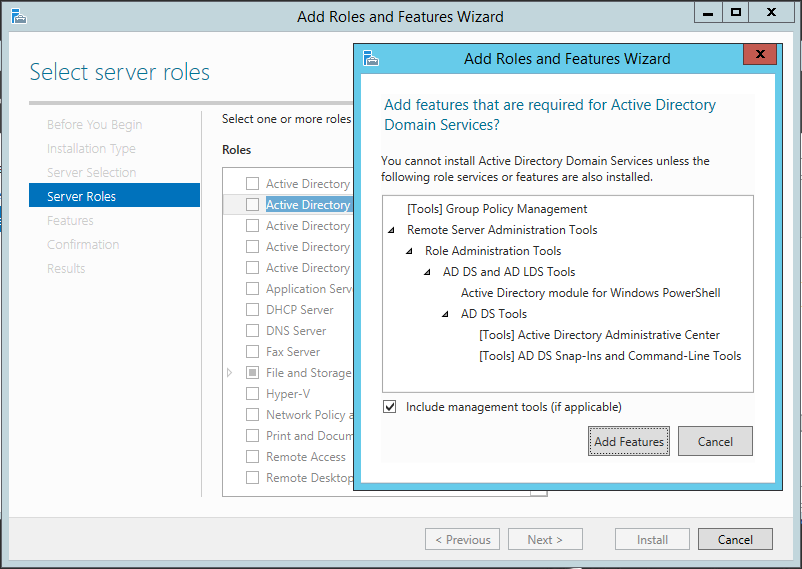
Select **Role-based or feature-based installation** (the default)



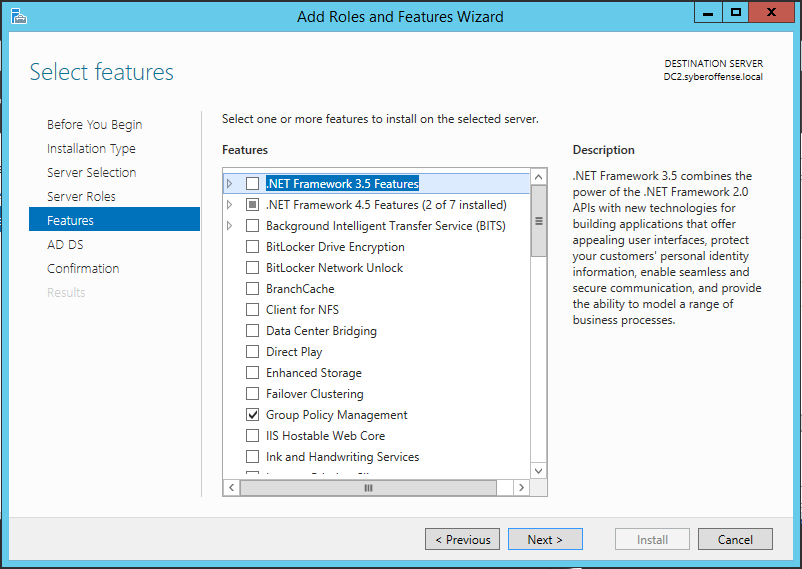
Select the new member server for your list of server present in your server pool. Click **next**.



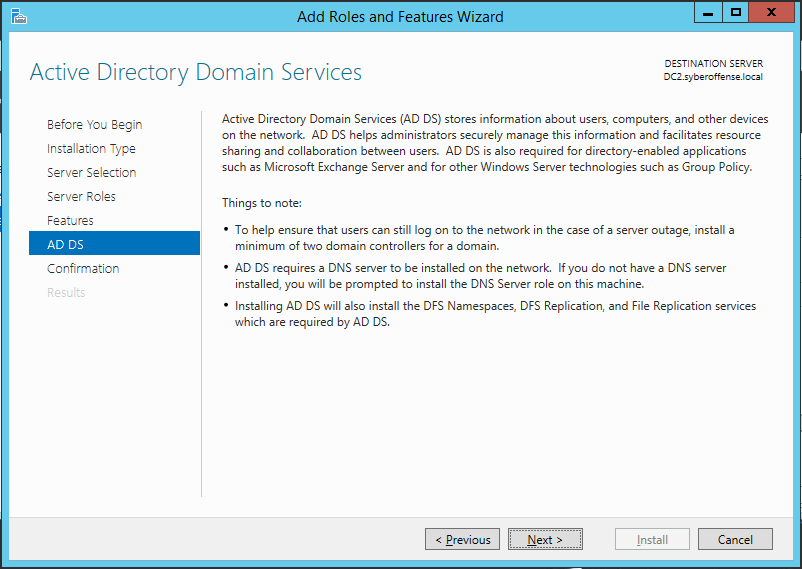
In the next window click on "**Active Directory Domain Service**". Click on "**add features**" to continue and then "**next**"



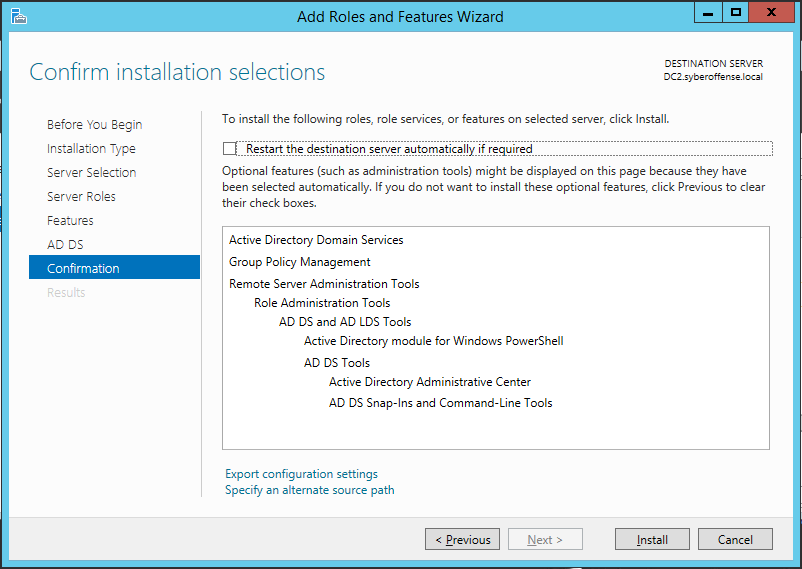
In the next window, accept the default features and click on **next** to continue



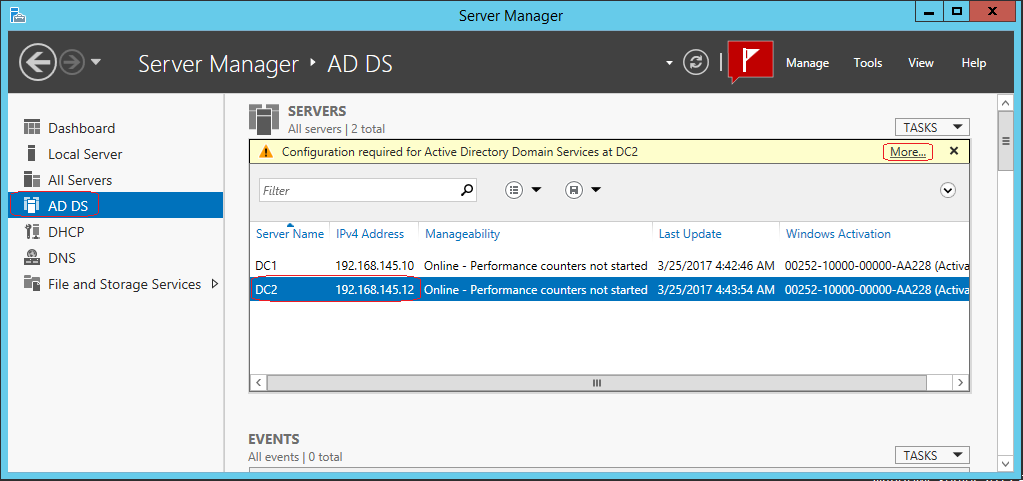
In the next window, we are given a brief description of the AD DS. Click **next**.



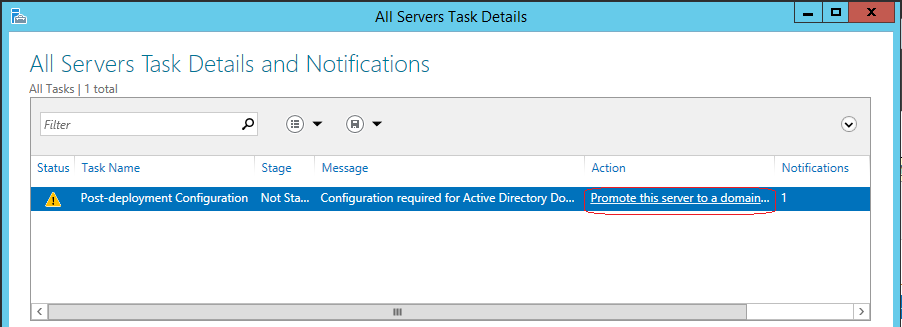
The next window asks for confirmation. Click "**install**" to begin the service installation.



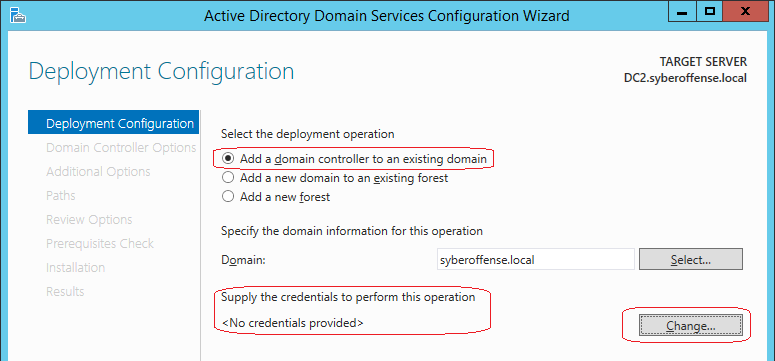
Once installation completes, open **Server Manager** and click on "**AD DS**." In the upper right corner of the panel, click on “**More**" as shown in the image

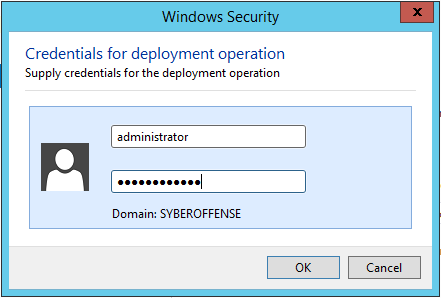


Click on option "**Promote this server to a domain….**"

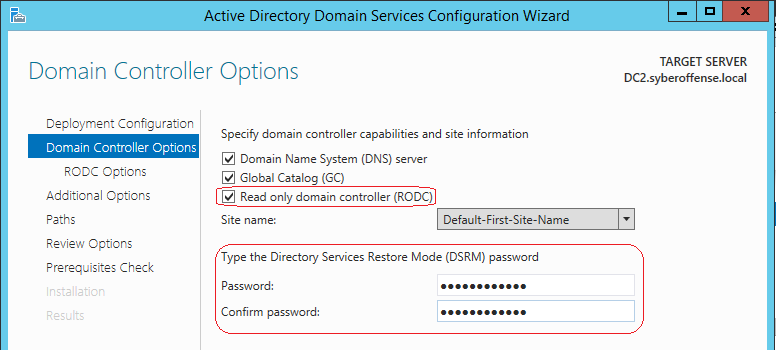


The AD DS Configuration Wizard opens. Accept the default selection and click **next**. You may need to provide your domain admin username and password.

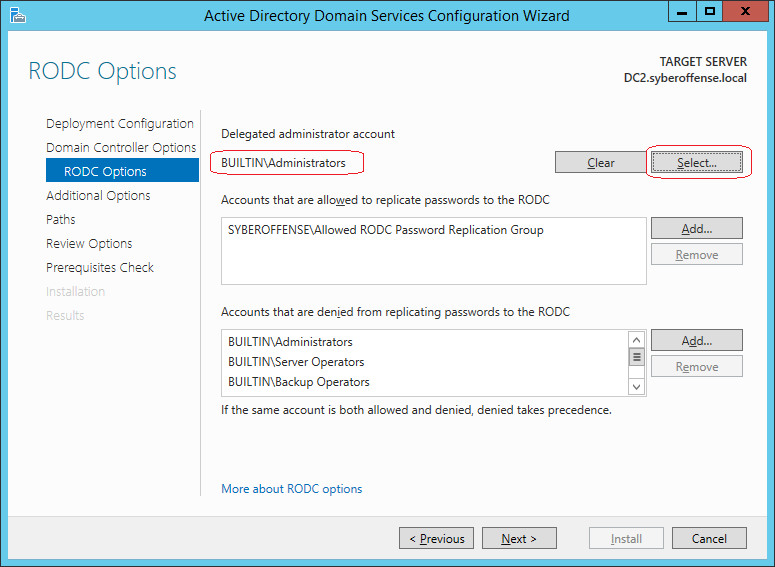
****

****

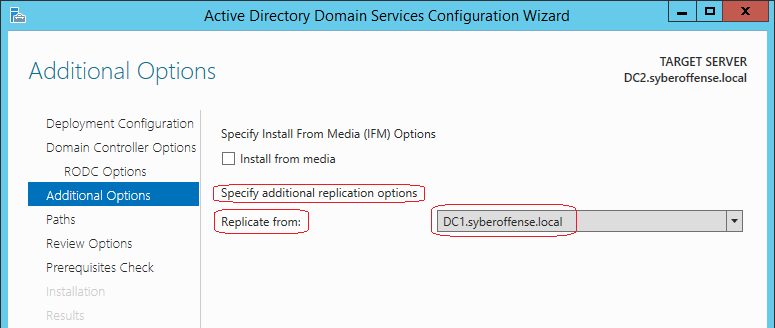
In the next window, select the "Read-only domain controller(RODC)" option and type a password for restore. Click on next to continue.



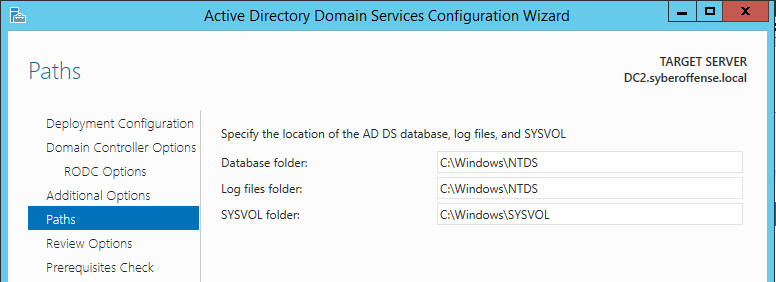
In the next window, select what groups/users allowed for the password caching, what group/users denied for caching and delegated admin accounts. For this lab accept the default selection. For the delegated admin account, I selected the built-in administrator's group.



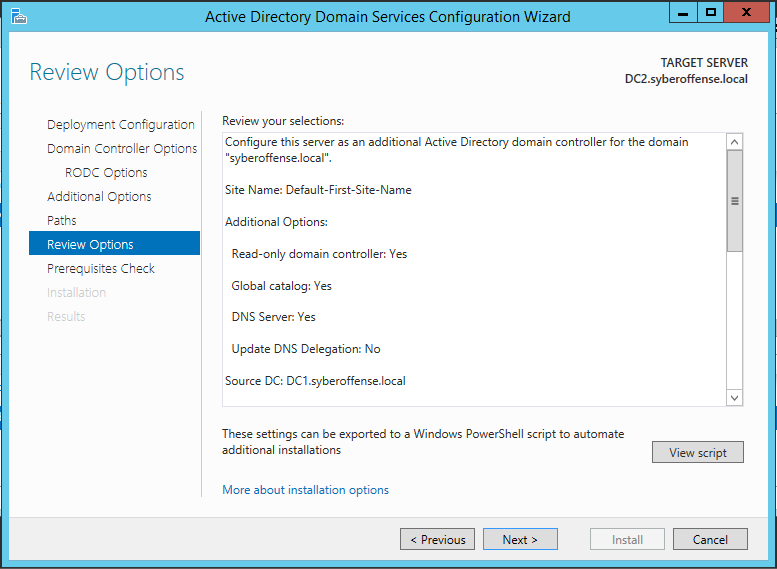
In the next window, we can select which DC this RODC will replicate with.



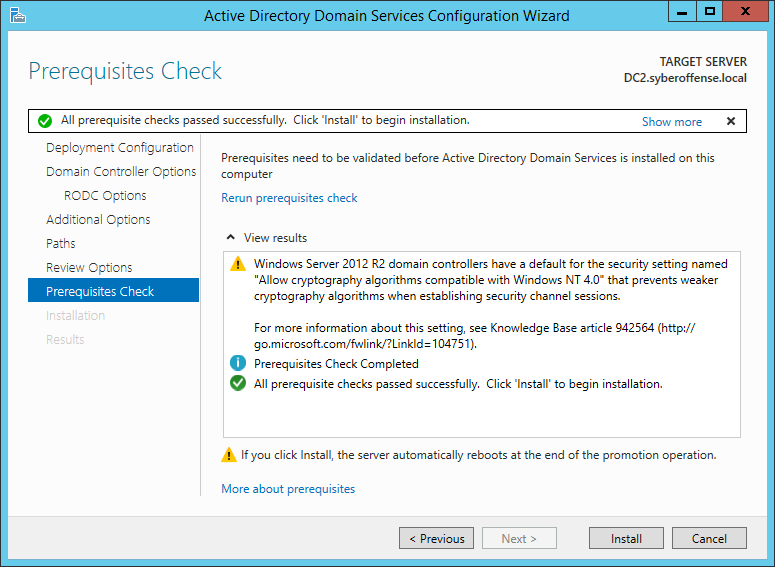
In the next window, accept the default folder paths and click **next**.



Confirm your selections and click **next**.



In the next window, the wizard checks if all the prerequisites for the installation have been met. Click **Install** to begin the installation



Once the installation has completed, the system will automatically reboot.

**Summary**

RODCs are additional domain controllers for a domain that host complete, read-only copies of the partitions of the Active Directory database and a read-only copy of the SYSVOL folder contents.

By selectively caching credentials, RODCs address some of the challenges that enterprises encounter in branch offices and perimeter networks (also known as DMZs) that may lack the physical security that is commonly found in data centers and hub sites.

As an additional domain controller for a domain, a read-only domain controller (RODC) performs the same operations as a writable domain controller. For example, because an RODC contains a copy of the directory database and a copy of the SYSVOL folder that contains the Group Policy objects (GPOs) and logon scripts for client computers, it can respond to authentication requests just as a writable domain controller does.

End of the lab!