KIT304 Server Administration and Security Assurance

Tutorial 6

Goal

In today’s tutorial you will start learning about Windows Server 2016 configuration, and introduce Active Directory and the user and group management tools that come with it.

Introduction

In the previous module we used CentOS as an example of a Unix operating system. CentOS is a Linux distribution with very close ties to RedHat. There are many different Unix and Linux distributions that a business, or administrator, may choose to use. Sometimes the choice is made for compatibility reasons, sometimes it is made for support reasons.

Today you start to look at the main alternative to this: Windows Server. You’ll be using the 2016 version, but you are probably aware that other versions exist, including 2012 and 2008. The Windows ecosystem does not have the fragmentation and multiple-choice options of Unix, which is what makes it attractive to many organisations. Windows Server 2016 was released in September 2016, and has already been superseded by Windows Server 2019, but it is sufficient for the exploration you’ll be undertaking.

In terms of popularity, you are probably aware of the dominant market share Windows has in the desktop market. Depending on the source, it is claimed that Windows has between 75% and 90% of the desktop market share, with the next biggest rival being macOS at between 6% and 13%.

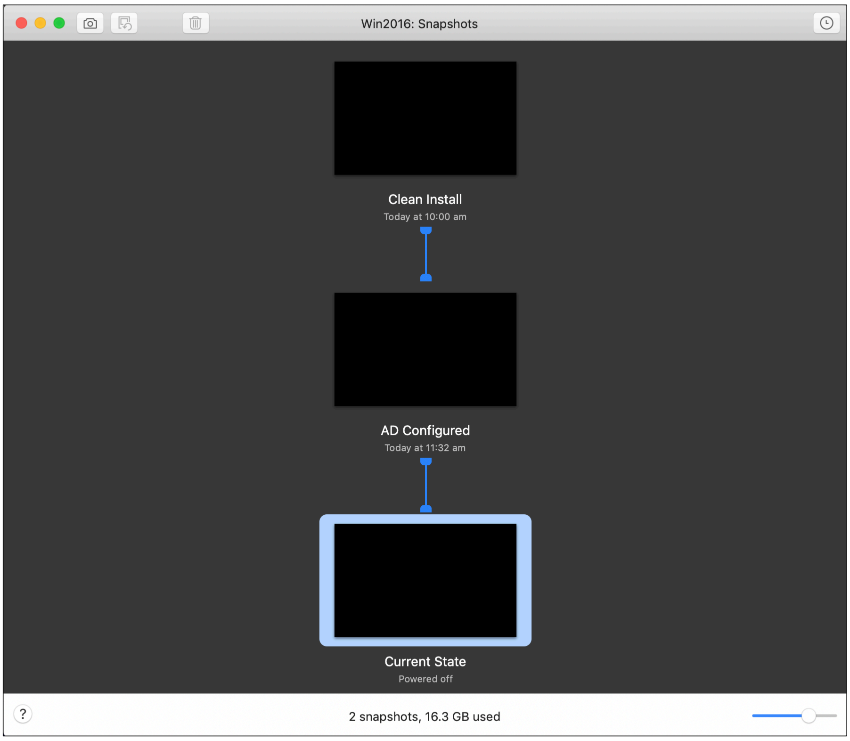
It is a different story in the server market. Of the top ten million servers that were accessible via the Internet in 2015, W3Techs reported that around 31% were Windows servers, with the remainder being Unix variants. This is not to say that Microsoft’s share is insignificant. The kind of user management and sharing of files that you did with Unix is very common on internal servers that are not visible to the Internet. These services are major components of Active Directory, and Windows Server is a very popular platform for undertaking these tasks.

In the Unix module we relied heavily on the documentation available in the **`man`** and **`info`** commands. In this module we will be taking a different approach – we will try to use some of material from Microsoft’s online resources that are provided to fill the same role. Some of this is tutorial-like content, and some is user-submitted, but there is a wealth of technical documentation as well.

Activity

1. Before you launch your virtual machines today, you need to select which snapshot of the **Windows 2016 Server** you want to load. For the remainder of the tutorials in this module, you'll be launching the default Windows 2016 instance which has already had various services enabled and configured. Today though, you will be learning how those services are set up by doing it yourself on an unconfigured version of the server.

   Right-click on the **Win2016** entry in the VMWare fusion window, and select the **Snapshots** option. This will open a window which should look like this:



Win2016: Snapshots

Clean Install
Today at 10:00 am

AD Configured
Today at 11:32 am

Current State
Powered off

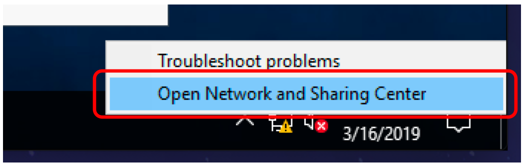
2 snapshots, 16.3 GB used

   You can see that there are three snapshots present –named **Clean Install**, **AD Configured**, and **Current State**. Double-click on the **Clean Install** icon, and in the dialog that appears, click **Don't Save**. This restores the version of the virtual machine that has not yet had Active Directory configured.

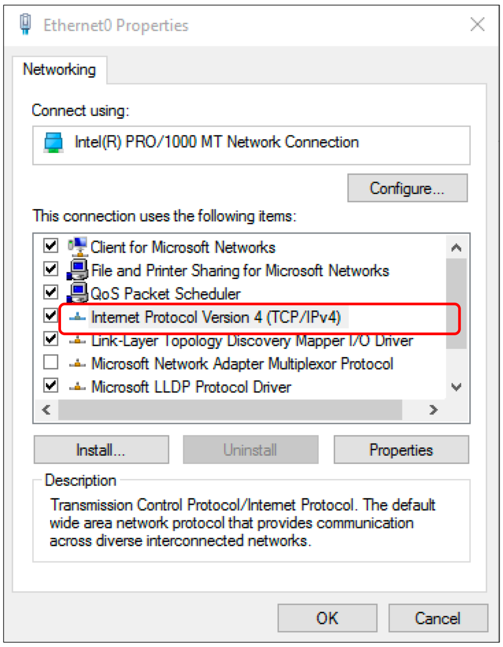
   Close the Snapshots window, and start up the virtual machine. When it has booted, type Control-Alt-Delete (or choose **Send Ctrl-Alt-Del** from the **Virtual Machine** menu) and you'll be prompted for the Administrator password, which is **ToorToor1**. Once you enter this, Windows 2016 will log you in, launch the Server Manager, and show its Dashboard.

2. Now launch the **Win7** VM. (You won't need it, but the password for the root account here is just **toor**).

3. Next, you need to give the Windows 2016 Server an IP address to enable it to interact with the network. The quickest way to do this is to **right click** on the icon of a computer with a yellow exclamation mark towards the lower right of the screen, then select **Open Network and Sharing Center.** (Alternatively, you can search for the Network and Sharing Center by clicking on the magnifying glass icon on the lower left corner of the screen).



Once the Network and Sharing Centre opens, you should see an **Ethernet0** connection in blue text towards the right. Click this to open the adapter settings, and then click the **Properties** button to reveal this window:



Ethernet0 Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

4. In the Properties window (shown above), click **Internet Protocol (TCP/IP/IPv4)** and then click the **Properties** button. In the dialog that appears, you can specify the IP address and related values for the system. Select the **Use the following IP address:** setting, and in the **IP address** box, enter the value **192.168.1.*x*** where ***x*** is any valid IP address octet). Click in the subnet mask field, and it will prefill with an acceptable value, and then press **OK**. Press **Close** on the **Properties** window to apply the IP address.

5. Repeat the process you just completed to give Windows 7 an IP address in the same subnet. Make sure your Windows 7 IP address does not conflict with your Windows 2016 Server IP address.

6. Open **Windows PowerShell** (a much-enhanced version of the command prompt) on both virtual machines and check that they can **`ping`** each other (if you can't find PowerShell, use the *Search programs and files* option in the Windows 7 Start menu, and the search icon at the lower left in Windows 2016 Server). If the machines can't ping each other, try the **`ipconfig`** command to confirm their IP addresses are correct. If not, fix them both before proceeding.

> ➢ Windows PowerShell accepts most of the commands that you would be used to typing in the more well-known command prompt, but it has many more features, some of which are similar to what you've experienced on Unix. You'll be seeing more of PowerShell in the next few tutorials.

7. Next, you're going to setup an **Active Directory Domain Controller**, which is a system for managing (among other things) user accounts and computers on the network. For example, AD can control password policy and access rights for the whole *domain* (network).

   To do this you're going to follow through a Tutorial from Microsoft Technet. The online version is available at the link below, but a simplified version with some of the unnecessary details removed is attached as an appendix to this document. Use the attached version to save time. When you're done working through the appendix, return to step 8 below.

   https://social.technet.microsoft.com/wiki/contents/articles/22622.building-your-first-domain-controller-on-2012-r2.aspx

8. On the **Windows 7** computer, change the name of the computer away from root-PC as follows:

   a) Click on the Windows "Start" icon (lower left corner), right-click on **Computer** in the menu that pops up, and choose **Properties**.
   b) In the computer information window, just below the middle of the page, you'll see the Computer name is **root-PC** – click the **Change settings** link which opens the System Properties dialog, then click **Change** and name the computer something else (eg., your name, or a department name such as "marketing". Restart when prompted.
   c) After the reboot, go back into the TCP/IPv4 settings (steps 3-4 above) and in the **Use the following DNS server address**, set the **Preferred DNS server** value to the IP address of the Windows 2016 server. You don't have a DNS Server yet, but you will once the domain controller is completely setup.

9. After the Domain Controller is set up, you're going to create some user accounts. You're going to create a total of five users to get some practice and experience with different scenarios. The first user you will create will just be a regular user. The second will be an admin user, which you will give Domain Administration privileges. The third will have their own storage space located on the server, and the last two users will be members of different groups with a shared group directory on the Server. First though, write down the usernames you want to use for your five users so you know which to use at each step later:

a. basic user ____

b. domain admin user ____

c. storage user ____

d. group member 1 ____

e. group member 2 ____

The following link takes you to some Microsoft documentation about how to manage users, groups, and other entities on active directory:

https://technet.microsoft.com/en-us/library/cc754217.aspx

Open the link, and drill down into **Managing Users**, then **Create a New User Account**. You can use this as a guide to creating your new users, but note the following replacements for steps 1 and 2:

i) In the Server Manager window, select **Active Directory Users and Computers** from the **Tools** button near the top-right corner

ii) In the window that opens, in the console tree in the left pane, you'll see the domain name **networks.local**. Click the small arrow to its left to expand it down so that you can see a tree of the different types of entities it can manage. Right-click on **Users**, and continue to step 3 on the Microsoft document.

Be sure to create all five user accounts.

10. To enable the second user account to be a domain administrator, you should look at this Microsoft document:

    https://technet.microsoft.com/en-us/library/cc700835.aspx

    This document talks in general about securing Active Directory administrative groups and accounts, which you may find generally useful, but you particularly want the section about 20% of the way into the document named **Creating a New User Account with Domain Admins Credentials**. Because you've already created your user accounts, skip forward to step 6 in this section, and make your second user a domain administrator.

11. Your third user will need a home directory on the server. To set that up, follow these steps

i. First you need a folder to share. In the root of the C: drive on the server, create a folder called **Home** using the **File Explorer**.

ii. Now that you have a folder to share, you can share it like this: right-click the **Home** folder and select **Properties**, click the **Sharing** tab, and then click the **Share…** button. In the window that opens, accept the defaults and click the **Share** button, click the **Done** button and finally close the **Properties** window.

iii. With the **Home** folder now shared, you need to set up the user's account to automatically attach to it when they log in. Back in the **Active Directory Users and Computers** window, locate the user account that you want to give a home folder (your third user) – they should be listed in the Users folder of the **networks.local** domain.

Right-click the user account name, select **Properties**, click the **Profile** tab, click the **Connect** button, and select a drive letter (which is where the user will see the shared Home directory you just set up) – you may want to use **H:** to represent "Home".

Next, you need to specify a path in the **To** box. The path can be expressed like this:

\\*serverName*\shareName\*folderName*

Generally, you want different users to have different folders in the share (so they have private storage spaces), and you want each folder to be the user's own account name. You can substitute **%username%** as the folder name in the **To** box to have the username substituted automatically. If you've been using all of the suggested values from the preceding steps to get to this point, you should be able to specify the path like this:

```
\\corpdc1\Home\%username%
```

Once you click **OK**, a new folder is created *inside* the **Home** folder specifically for this user and the permissions on the folder are set to give the user read and write access to it.

12. You're almost done customising your user accounts. For this step, you're going to set up two new groups, and make your last two users members of them. To do that, you're going to revisit this link:

https://technet.microsoft.com/en-us/library/cc754217.aspx

After opening the link, drill down into **Managing Groups**, then **Create a New Group**. As before, note the following replacements for steps 1 and 2:

i. Your **Active Directory Users and Computers** tool should already be open.

ii. The **networks.local** domain should already be expanded. Right-click on **Users**, and continue to step 3 on the Microsoft document.

Create two groups – one called **development** and one called **marketing**. You can accept the default values for the group scope and group type.

When the groups have been created, you'll see them listed in the main window when the domain's Users folder is selected. Now, it should be a straightforward process to open each group's **Properties** window (much like you did in step 10 when making the second user a domain administrator) and in the **Members** tab, add a user to that group. Add your fourth user to the development group, and your fifth user to the marketing group.

13. With your groups created, and with some of your users now members of them, all that remains is to create a shared folder for each group's work on the server. To do that, follow these steps:

    i. Open a **File Explorer** window, navigate back to the root of the C: drive, and create a folder named **Groups**.
    ii. Inside the new **Groups** folder, create two more folders named **Development** and **Marketing**.
    iii. For *each* of these group folders, right-click on them, and select Properties, then select the **Sharing** tab, and click the **Share…** button. In the window that opens, enter the group's name in the entry field, and click **Add**. In the list below that (that the group was just added to), change the **Read** permission to **Read/Write**, and then click the **Share** button and then the **Done** and **Close** buttons.

Let's take stock of what you've done to date:

- you've turned on the active directory domain controller service
- you've created 5 users with different capabilities
- you've created two groups, and added a member to each
- you've created a home directory for one user, and shared folders for each of the groups

By itself, those steps have been useful as a learning exercise, but you haven't really closed the loop – you need to provide a way for all of those users and groups to be able to access the things you've set up. And do to that, you need to join their computer(s) to the domain server as well.

14. To join the **Windows 7** system to the domain, follow these steps:

    i. Clicking the Windows "Start" button (at the bottom left corner of the screen), in the menu that is displayed, right-click on **Computer**, and then select **Properties**.
    ii. Under **Computer name, domain, and workgroup settings**, click **Change settings**.

iii. In the **Computer Name** tab, click the **Change** button. Under **Member of**, click **Domain** and then type the name of the domain you set up in step 7 (if you followed the steps exactly as shown, it's most likely **networks.local**).

iv. You will then be asked for a username and password for the domain. For the user name, enter the account name of the second user that you created earlier – the one with domain administrator privileges. After a short pause, you'll be welcomed to the domain, and you'll see a message telling you to restart. Close the Properties box, and restart.

v. When the computer has rebooted, you'll see a login window (previously, the system was set to log in automatically as the **root** user). Click the **Switch User** button, then click **Other User** and then enter the username of the first user you created.

Your Active Directory server is now controlling access to the Windows 7 system through the accounts you created back in step 9. The first user is a standard, non-privileged account on the Windows 7 machine.

15. Experiment with the five accounts that you created earlier, testing that each can log into the Windows 7 system, and that everything works as it should. Some of the things to test:

i. As the third user, you should be able to see the network share set up in the server's **Home** folder is automatically mounted and that you are able to create files and folders in it. You should also be able to see these files on the 2016 server, since that is where they are hosted.

ii. As any user, you should be able to browse for network shares on the server. For example, in an explorer window, type `\\` followed by your server name (perhaps **`corpdc1`**) in the address field at the top, and you should see which shares are being exported by the server. Only the fourth and fifth users you created should be able to access and modify files in the shares for their respective groups.

16. As a final step, if you have time, try joining the Windows 10 system to the domain. The steps would be:

i. Start the **Win10** virtual machine, and login as the root user with the password **toor**.

ii. Give it an appropriate IP address and set the DNS server field to the IP address of the Windows 2016 Server (see steps 3 and 4 earlier).

iii. Type **This PC** into the Windows Search field (lower left of the screen), and on the best match that is found, right click and select **Properties**, then follow the steps from 14.ii onward.

Conclusion

This ends your first foray into Windows 2016 Server. For some users, having the administration tools accessible via a GUI is preferable to having to use a command line like Unix. For others (generally, "power users") the command line is the preferred way. As you'll see in the next few tutorials, Windows Server allows you to perform all of the actions you've done today in the GUI, on the command line instead.

Skills to Master

To successfully complete this tutorial, you must have mastered the following skills:

- set up an Active Directory Domain Controller using guided steps
- create new users on the domain controller
- create new groups on the domain controller, and make users members of those groups
- create folders and manipulate their group permissions
- join (or **bind**) a client system (Windows 7, Windows 10) to the domain controller
- verify that you can log in on a windows client bound to the domain controller using credentials for the users you created on that domain controller
- verify that the group permissions you applied to the folders you created are applied to individual users according their group membership

Of these skills, the only one that you would not be required to demonstrate in a practical exam is setting up the Active Directory Domain Controller.

Appendix 1 – Building Your First Domain Controller on 2012 R2

Adapted from https://social.technet.microsoft.com/wiki/contents/articles/22622.building-your-first-domain-controller-on-2012-r2.aspx. for KIT304.

So you want to build an Active Directory domain? Congratulations! This guide is not really meant for the seasoned admins who eat, sleep, & breathe Active Directory. It is meant for the folks who have a real job, but since they own a computer at home, they are now the company's network administrator. You know who you are!

I will go through the process in as non-techie terms as possible, but will link to online documentation just in case you want to dive deeper. In this post I walk through setting up a brand new 2012R2 Standard edition Server. While technically I am building out a virtual machine, a physical machine would be the same process. So why build a domain in the first place? There are many reasons to need or want a domain;

- Software like Exchange Server and many 3rd party vendors require having Active Directory in your environment.
- Centralized security - All user accounts are stored in the domain so users will be able to log into any PC in the domain and all Active Directory integrated apps with the same account - that means no more password post-it notes attached to monitors
- Centrally manage user and computer policies to control things like how long a password should be and what drive letters should be mapped for users
- Many, many other reasons.

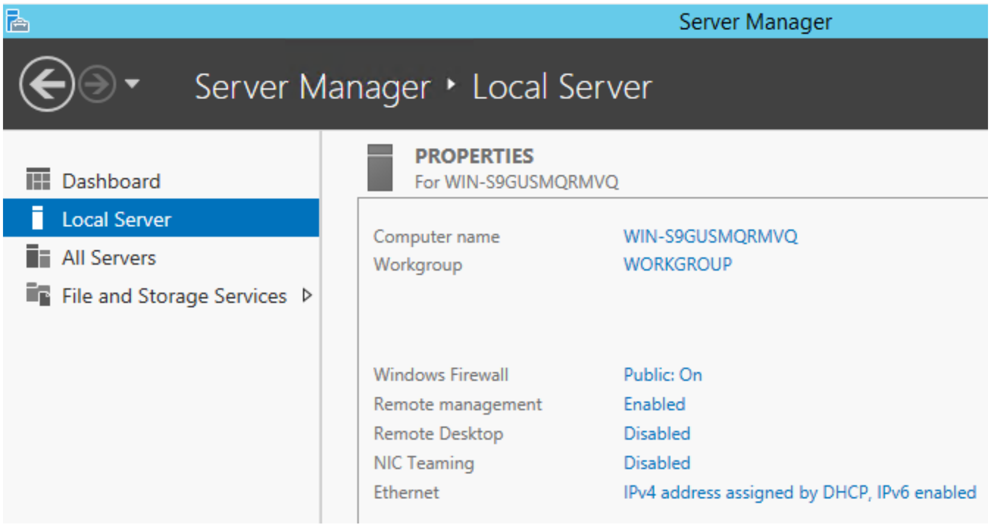
But this isn't a walkthrough on why, but how. Let's start:

Step 1 - Evaluate

- Domain - What are you going to call this creature you are about to build? In my test lab I build out a fictional company called Matrix.loc (Yes I really liked the movie). There are a few things to note about the name, Matrix is the fictional company name and loc is a fake root domain. The fake root domain could easily be .com, edu, .net and I would have made it that if I actually owned those names on the internet - I don't own them so I use a fake root name. It won't matter the server will still be able to get to the internet as will the clients.

Step 2 - Set Server up

- When you log into the server for the first time, Server Manager will start up
- Select **Local Server** on the left and you should see a screen similar to below:

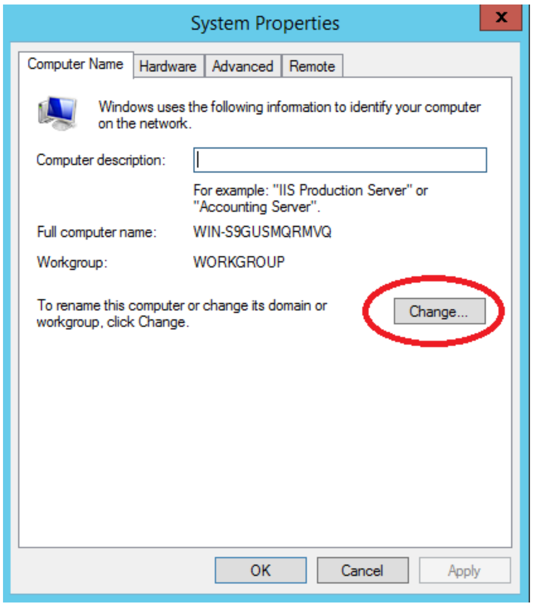


PROPERTIES
For WIN-S9GUSMQRMVQ

Computer name	WIN-S9GUSMQRMVQ
Workgroup	WORKGROUP
Windows Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled

- NOTE: there are a few things you need to change here – the first being **Computer name** (Nobody will remember that name if they needed to)

- Click on the computer's name (the Blue text) and the window on the right will show up – click the **Change** button.



Windows uses the following information to identify your computer on the network.

Computer description:

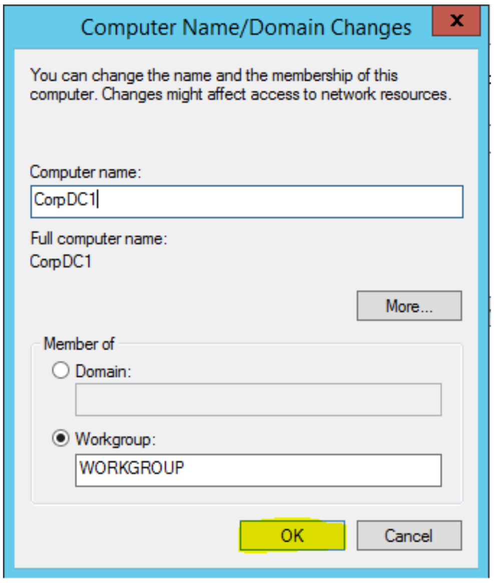
For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-S9GUSMQRMVQ

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

- Type in the Computer name that you want for this domain controller in the screen that comes up like below:



You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: CorpDC1

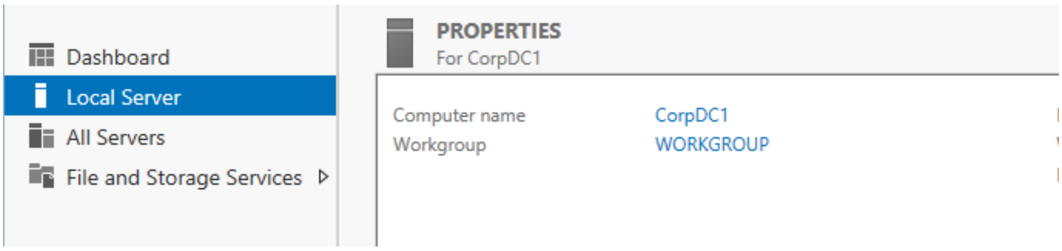
Full computer name: CorpDC1

○ Domain:

● Workgroup: WORKGROUP

- Click **OK** when done, and then close the screen behind. Reboot when it asks you to.

- Login to Windows and when the Server Manager comes back up, click on **Local Server** again and validate the name change:

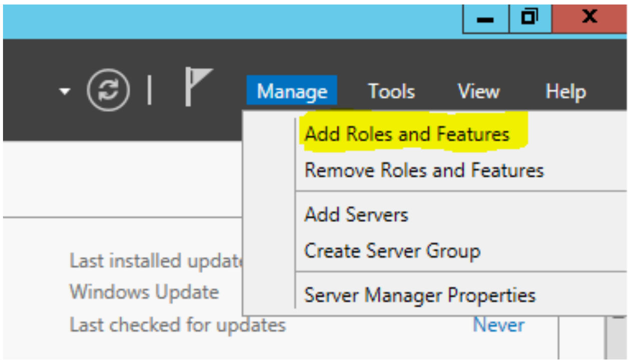


PROPERTIES
For CorpDC1

Computer name CorpDC1
Workgroup WORKGROUP

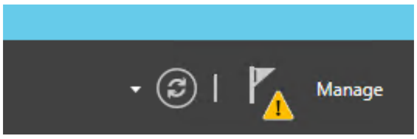
Step 3 – Promote to Domain Controller

- Once everything is up and running again – it's time to finally install the Directory Services role
  - In Server Manager, click **Manage** (upper right) and then **Add Roles and Features**
  - Click **Next** on the first screen
  - In the Installation Type section, keep the defaults (Role-based or feature-based installation) and click **Next**
  - In the Server Selection section, keep the defaults (select a server from the server pool), make sure your new server is highlighted, click **Next**
  - In the Server Roles section, put a check mark next to **Active Directory Domain Services**, and, if it's not already checked, next to **DNS Server** a few lines further down, and in the popup window, click **Add Features**, then click **Next**
  - In the Features section, click **Next**
  - In the AD DS section, click **Next**
  - In the DNS Server section click **Next**
  - And finally in the Confirmation section, click **Install**
  - At this point the Active Directory binaries will be installed (it may take a few minutes). Once it finishes click the **Close** button

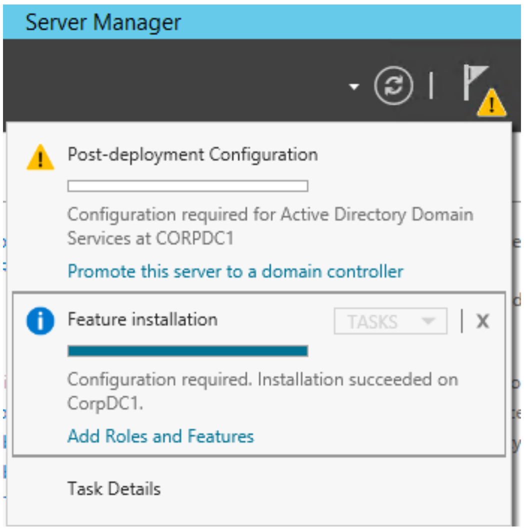


Last installed updat
Windows Update
Last checked for updates Never

- The binaries are installed but where is my Active Directory? At this point you should be looking at Server Manager, and at the top of the screen there should be a flag next to the word manage with a yellow caution symbol (as shown on the right).



- When you click the flag a window will open telling you that there is still some configuration that is needed to make this server a domain controller.
- Click the **Promote this server to a domain controller** link



Post-deployment Configuration

Configuration required for Active Directory Domain Services at CORPDC1

Promote this server to a domain controller

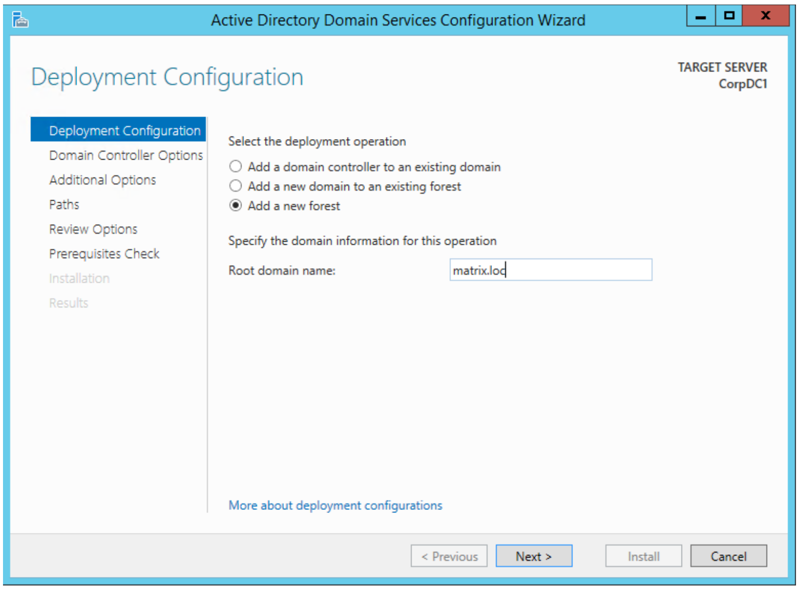
Feature installation

Configuration required. Installation succeeded on CorpDC1.

Add Roles and Features

Task Details

- In the configuration window that appears, select the option to **Add a new forest** and then type the domain name that you want (we can use **networks.local**), then click **Next**



Deployment Configuration

Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

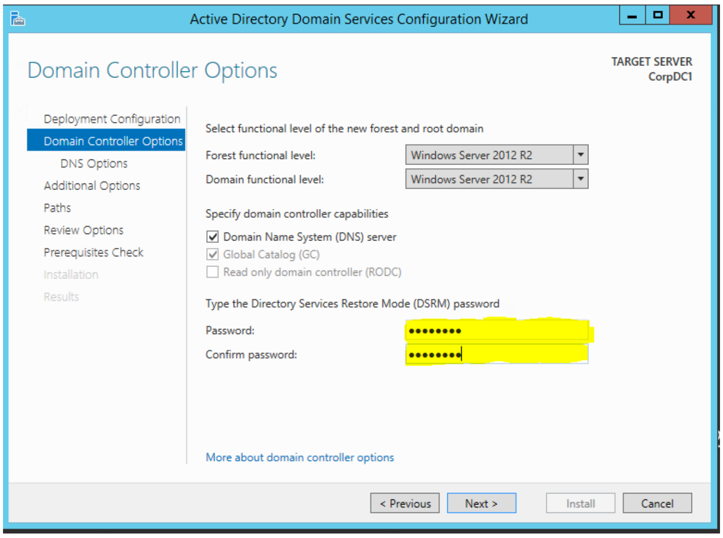
Specify the domain information for this operation

Root domain name: matrix.loc

NOTE: Here are some guidelines for domain names stay away from:

- Don’t use single label names i.e. Matrix
- Don't over complicate it, if the name of your company is Brads Totally Awesome Computer Repair and Web Design, I would never create a domain called bradstotallyawesomecomputerrepairandwebdesign.local. In Fact the domain name should be less than 15 characters for technical reasons. In the example above I would shorten it up to something like BTAC.local – trust me your users will thank you ☺
- Avoid using special characters in the domain name like |/\?"> <:*, periods are ok as long as it is not the first character, dashes (–) are OK but still wouldn't use as first character

- On the Domain Controller Options screen
  - Leave the Forest functional and Domain functional level – at their default settings – the wizard will pick the highest functional level that the OS will support, so defaults are usually the best bet.
  - In the section labelled **Specify domain controller capabilities** again the defaults are the best option
  - In the section for the DSRM password, enter and confirm a password for restore mode – this should be something that is easily remembered or stored securely somewhere, as the only time you will need this password is during a disaster (for the tutorial, you can use **ToorToor1**.
  - Click **Next**



Domain Controller Options

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: ••••••••

- On the DNS options screen, **ignore the warning** about the delegation and click **Next**
- On the Additional options page, make sure that the name of your domain is listed as the NetBios domain name. For example, if your Domain is **networks.local**, the NetBios name is **NETWORKS**. Once this is entered, click **Next**
- On the Paths screen, the defaults should be fine but if you so desired you could change them to another local hard disk or partition. Click **Next**
- On review options click **Next**
- The server will now check to make sure all the prerequisites for the domain controller is satisfied, there will be some warnings, but that should be fine, review and click **Install**
- Once the install completes the server will reboot
- Once rebooted you will sign into your new domain

Once the domain is up and running there are a few things that will need to be done to fully utilize Active Directory

1. Users will need to be created
2. Client computers will need to point their network adaptor DNS settings to the server’s IP
3. Computers will need to be joined to the domain