FIREBRAND

Microsoft

MCSA Windows Server 2012 Certification

Courseware

Version 1.6

www.firebrandtraining.com

2015

MCSAWS Additional Material

ADDITIONAL MATERIAL FOR EXAMS 70-410, 70-411 AND 70-412

FIREBRAND TRAINING

Contents

Installing and Configuring Windows Server 2012 Additional Material

Day 0

Basic PowerShell Desired state Configuration Example

Desired State Configuration (DSC) is a new management platform in Windows PowerShell that allows us to deploy configuration settings to a host or a group of hosts. Examples of configuration settings that can be applied include:

Enabling or disabling server roles and features

Managing Registry settings

Managing Files and Directories

Deploying new software

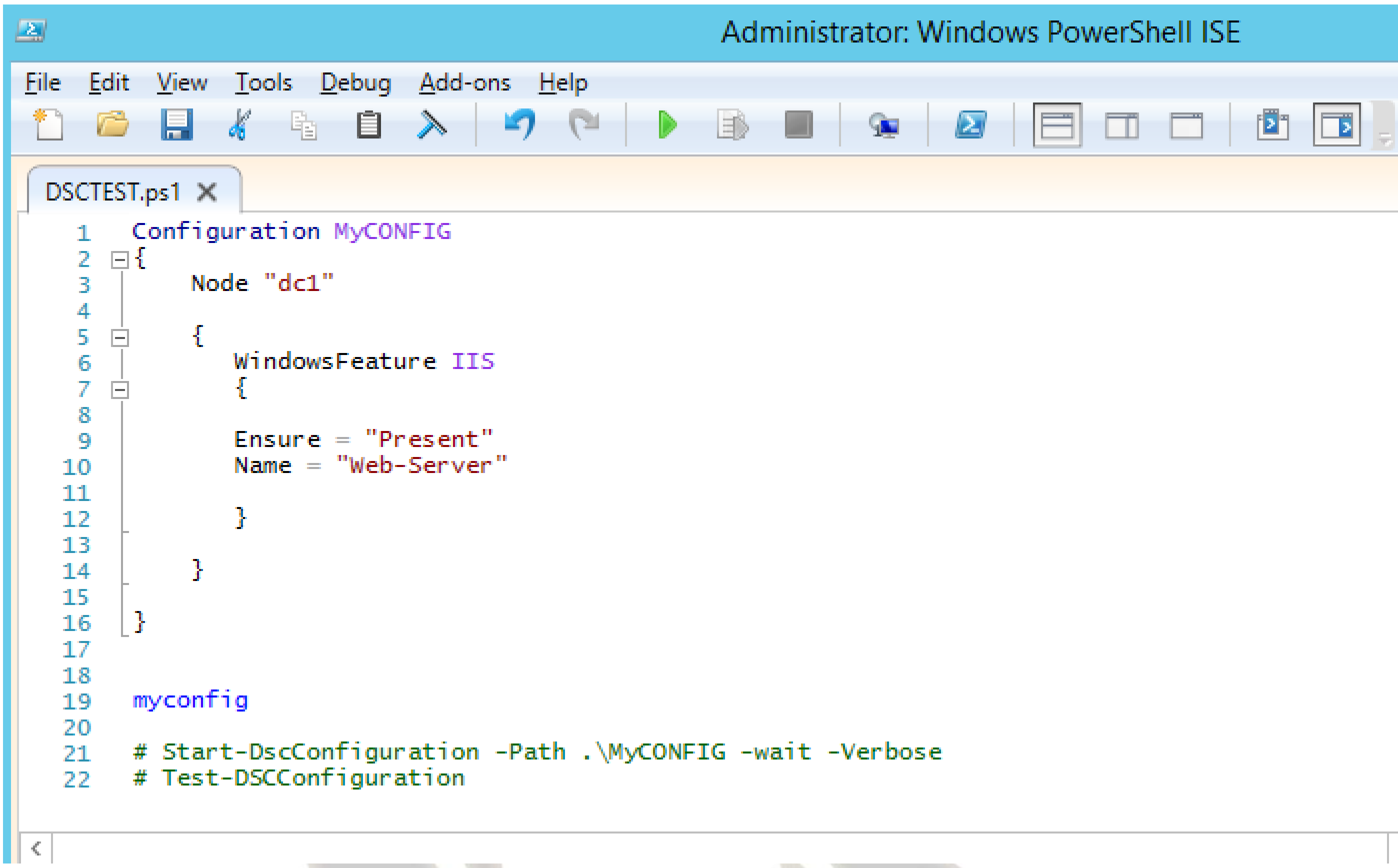
As well as configuring remote machine using PowerShell, DSC can also discover the configuration state of a machine and help fix a configuration that has drifted away from our desired state.

To Use DSC to configure a machine or group of machines we use the **CONFIGURATION** key word when we create a PowerShell script. The **CONFIGURTION** key words is used to inform PowerShell that what follows is to be used with DSC, the **CONFIGURATION** key word also allows us to provide a name for our DSC. To mark our Configuration in a PowerShell script we use braces **{}** to mark the beginning and end of the DSC block in the script.

Inside the DSC block we add node (computer) blocks, each node block contains the desired state configuration for that node, a node block starts with the **NODE** key word and again we use braches **{}** to mark the beginning and end of the **NODE** block.

Inside each node block we define Resource blocks to configure settings such as enabling a role or feature, a resource block starts with the name of the resource followed by braces {} to identify the start and end of the Resource block. Example Resource block name include **WindowsFeature** for installing and removing Windows features and **FILE** for managing file on node.

Below is a basic DSC Script created in Windows PowerShell ISE, This DSC Script is designed to check if IIS is installed on a computer and if it isn't installed it will install it.


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
DSCTEST.ps1

```
Configuration MyCONFIG
{
    Node "dc1"

    {
       WindowsFeature IIS
       {

       Ensure = "Present"
       Name = "Web-Server"

       }

    }

}


myconfig

# Start-DscConfiguration -Path .\MyCONFIG -wait -Verbose
# Test-DSCConfiguration
```

The Script start with the line **CONFIGURATION MyConfig** Configuration is used to inform PowerShell that we about to enter DSC commands and MyConfig is the name of my DSC config file.

We next have the { that marks the start of the DSC config.

Next we have the **NODE** key word that marks the start of the NODE block, we also have the name of the node"DC1″that this DSC script is designed to configure. The name of the NODE will accept variables, so that we can use DSC as part of a larger script to configure a group of nodes. After the line NODE "DC1" we have another { that marks the beginning of this NODE section.

Next we have the Resource Block, first we have the name of the resource this DSC script will work with, in my example **WindowsFeature** and a name for this block, in my case "IIS" but this can be anything you like. The start of the resource block is again marked with a {.

This resource block is performing a simple check to see if IIS is installed on node "DC1", this is where the **Ensure = "Present**" comes in. Ensure = "Present" means make sure the features is installed, if we want to make sure the feature isn't installed then we would have typed Ensure = "Absent". Next we identify the feature we want to check with the line Name =

“web-Server” (Web-Server being the name of the IIS role in Windows Server 2012). Because we have written Ensure = “Present” if the IIS role isn’t installed then it will be installed as part of this process.

The end of the resource block is identified with }

The end of the Node block is identified with }

The end of the DSC Configuration is identified with }

I saved my script and called it DSCTEST1.ps1, notice though there is one more line in the Script, it simply says **myconfig** (the same name as I used in the CONFIGURATION line). This is an important command, this command take the DSC configuration you have identified and creates MOF files that are then used to configure the target node, the MOF files are created in a folder with the same name as your configuration so I would be looking for a folder called MyConfig that contains the newly created MOF files that will be used to configure DC1 with IIS. If you have called you DSC something else other than MyConfig then that’s what you type in the final line of your script, if you save the script please give it a different name to you configuration to avoid confusion.

When the script is run you should see results that indicate that the MOF files have been created.

This first phase of DSC (crating the script) is known as the **Authoring Phase**. When you run the script this is known as the **Staging Pha**se. The final Phase is the **Implantation Phase.**

To Implement the DSC we use a PowerShell CMDLET **Start-DscConfiguration**, in the screen shot above I have included the # line as a note to remind me (and you) to run the **Start-DscConfiguration** CMDLET. You use the –Path parameter to identify the directory that contains you newly created MOF files and I used the –Verbose parameter so I could see the results as the DSC config was applied. Of course you could just run this command as part of your PowerShell script that include the DSC config.

The **TEST-DscConfiguration** CMDLET can be used to check the DSC against the node to see if the configuration matches (TRUE) or doesn’t match (false).

This simple DSC example uses DSC push mode where the configuration is pushed from the machine you are on to the target NODE. You can configure DSC Pull mode, in pull mode the Staging Phase is done on an IIS server, then we can configure our nodes to periodically check the staging area and reapply the DSC if necessary, this helps prevent configuration drift.

I performed my example using two Windows Server 2012R2 Servers, I also made sure PowerShell remoting was enabled as well as remote management.

Managing Remote Servers from Server Manager

From Server Manager you can manage older Windows Servers. You can manage Windows Server 2008 SP1 (full and Core) or Windows Server 2008 SP2 (full) and above but you must also install Windows Management Framework 3.0 (WMF 3.0) and .Net Framework 4.0 on the servers to be managed as well as enabling WINRM.

You can Manage workgroup servers but you need to:

1. Make sure you can resolve the name of the server you wish to manage.
2. Run the following command on the Server Manager Server:

Set-Item WSMAN:\localhost\client\TrustedHosts –Value “servername” –Force

The Remote Server Admin tools (RSAT) can be installed on a Windows 8.1 machine to remotely manage your servers from your desktop.

Managing Remote Servers using PowerShell

You can use PSRemoting to execute remote PowerShell commands, if PSRemoting is not enabled then you will need to run **Enable-PSremoting** on the server to be managed. You can then use the command **Enter-PSSession –Computername “Computername”** command to enter a remote session and the command **Exit-PSSession** to exit a remote session.

You can also use the **Invoke-Command** command to run remote commands.

What would these 4 example PowerShell commands do?

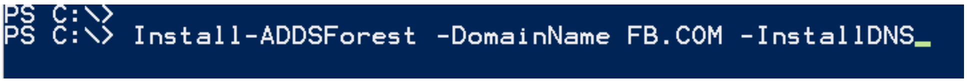
```
1.  Invoke-Command –computername LON-DC1, LON-SVR1 –Scriptblock {Get-Process}

2.  Enable-PSRemoting

3.  Enter-PSSession –Computername LON-SVR1
    Get-Service
    Exit-PSSession

4.  Set-Item WSMan:\localhost\Client\TrustedHosts –Value "SVR1.Contoso.com" –
    Force
```

Day 1

Using PowerShell to Deploy ADDS

We can use PowerShell to deploy a new domain or forest or domain controller

Install-ADDSForest –DomainName *root domain name*

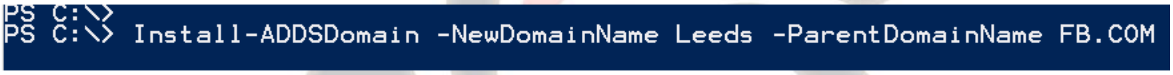


```
PS C:\>
PS C:\> Install-ADDSForest -DomainName FB.COM -InstallDNS_
```

We can use Install-ADDSForest to install a new forest root domain, other parameters include:

-DatabasePath – Path to NTDS.DIT
-DomainMode – Sets domain functional level by either using a number or name, examples are 4/ 4/Win2008R2 or 5/Win2012
-ForestMode – Sets Forest functional level by either using a number or name, examples are 4/2008R2 or 5/Win8
-LogPath – Path to Logfile location
-SysvolPath – Path to Sysvol location

Install-ADDSDomain –DomainName *child domain name* –ParentDomainName *parent domain name*

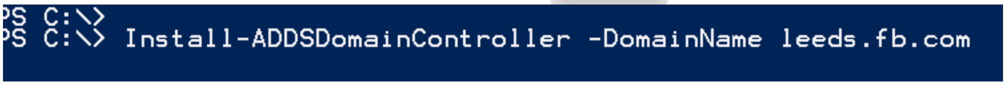


```
PS C:\>
PS C:\> Install-ADDSDomain -NewDomainName Leeds -ParentDomainName FB.COM
```

We can use Install-ADDSDomain to install a new child domain, other parameters include:

-DomainMode -- Sets domain functional level by either using a number or name, examples are 4/ 4/Win2008R2 or 5/Win2012
-ReplicationSourceDC – Sets the domain controller that we will copy partition information from.
-DatabasePath – Path to NTDS.DIT
-LogPath – Path to Logfile location
-SysvolPath – Path to Sysvol location

Install-ADDSDomainController –DomainName *domain name*



```
PS C:\>
PS C:\> Install-ADDSDomainController -DomainName leeds.fb.com
```

We can use Install-ADDSDomainController to add an additional domain controller to an existing domain, other parameters include:

-ReadOnlyReplica – Specifies whether to install the domain controller as an RODC for an existing domain.

Other ADDS CMDLets

Add-ADDSReadOnlyDomainContorllerAccount – Creates a read-only domain Controller account that can be used to install an RODC
Uninstall-ADDSDomainController– Uninstalls a domain controller in Active Directory

Other ADDS Deployment CmdLets
Add-ADDSReadOnlyDomainContorllerAccount – Creates a read-only domain Controller account that can be used to install an RODC
Uninstall-ADDSDomainController – Uninstalls a domain controller in Active Directory

Before we use the above PowerShell commands what additional command must we run first?

Domain Controller Cloning

Domain controller cloning allows us to rapidly deploy new domain controllers, the link below will take you to an article that covers the details of domain controller cloning:

http://blogs.technet.com/b/keithmayer/archive/2012/08/06/safely-cloning-an-active-directory-domain-controller-with-windows-server-2012-step-by-step-ws2012-hyperv-itpro-vmware.aspx

AD DS Simplified Administration

Server 2012 R2 has introduced several new technologies to make administering AD much simpler, the link below will take you to a TechNet article on the

https://technet.microsoft.com/library/jj574178.aspx

What would these PowerShell commands do?

Script 1

```
$admin = Get-ADGroupmember "organization Management"

foreach ($user in $admin)

{
    Set-aduser $user -Description "OUR TEST"

    }
```

Script 2

```
$users = Get-ADUser -Filter * -Properties "department"

foreach ($user in $users)
{
if ($User.Department -eq "Sales")
{
Set-Aduser $user -Department "UK Sales"
}
elseif ($User.Department -eq $null)
{
Set-ADUser $user -Department "IT"
}
}
```

Script 3

```
$users = Get-ADUser -Filter * -Properties "department"

foreach ($user in $users)

{
Switch ($user.Department)
{
"UK SALES" {Set-ADUser $user -Department "Sales"}
"IT" {Set-Aduser $user -Department $NULL}
}
}
```

IPv4 Additional Worksheets

This material is intended for those delegates that feel they need more practice with IPv4, check with your instructor for the answers to the examples in this section.

IPv4 Worksheet 1 – Working out a Computers Network ID

BINARY TABLE

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

Example 1

You have a computer with an IP Address of 192.168.2.33/27, you have been asked to work out the Network ID of this computer. To do this we need to work through the following steps:

1. Find the increment value that is being used
2. Use the increment value to work out valid Network IDs
3. From the list of Network IDs locate the correct Network ID for our host

Step 1 – Find the increment value that is being used (the long way)

The increment value is a very important number that will help you answer several IP questions in certification exams. The Increment value helps you define valid network ID's. To find the increment value in example 1 we use the CIDR notation (or subnet mask).

In example 1 the CIDR notation is /27 or 11111111.11111111.11111111.11100000

We are interested in the very last binary digit that is turned on, I have highlighted the last digit turned on below:

11111111.11111111.11111111.11**1**00000

The highlighted binary digit has a decimal value, this is our increment value. Using the binary chart at the top of this page we can see that the decimal value of the 3rd binary digit from the left is 32. So our Increment value is 32 (we will see how we use this value later)

Let's look at another example, say you have a host with an IP address of 192.168.2.9/29, this would be 11111111.11111111.11111111.11111000 in binary. The last binary digit turned on is: 11111111.11111111.11111111.11111000

This is the 5th binary number in the 4th octet and it has a decimal value of 8 so 8 is our increment value.

Try working out the increment values for each of the following IP Addresses:

1. 131.107.4.1/22
2. 192.168.2.9/30
3. 192.168.2.129/25

Step 1 – Find the increment value that is being used (the short way)

In our first example our IP address was 192.168.2.33/27. /27 equals a subnet mask of 255.255.255.224 if we follow the step below we can find our increment value:

256 – 224 = 32 and 32 is our increment value

If we have an IP Address of 192.168.2.9/29 the CIDR notation equals a subnet mask of 255.255.255.248 so….

256 – 248 = 8 and 8 is our increment value

Step 2 – Use the increment value to work out valid Network IDs

In our original example we started off with the IP Address 192.168.2.33/27 and we have already worked out that its Increment value is 32.

We can now use this value to work out valid Network IDs based on our IP Address 192.168.2.33/27 and the increment value 32.

In this example we are working in the 4th octet (this is because the 4th Octet was where we located the increment value) because we are working in the 4th octet the first three octets are being used fully by our network ids, so whatever our network ids are they will all start with 192.168.2.x with the 4th octet changing for each Network address.

The first available Network ID is always 0, in our example that makes the first available Network ID:

First available network ID = 192.168.2.0/27

We then use the increment value to find the 2nd network ID:

Second available Network ID = 192.168.2.32/27

We then keep incrementing the 4th octet by 32 (our increment value) to find additional Network IDs.

Third available Network ID = 192.168.2.64/27

Fourth available Network ID = 192.168.2.96/27

Fifth available Network ID = 192.168.2.128/27

If we had been working in the 3rd octet then the first two octets would stay the same, the third octet would change starting at 0 and incrementing based on the increment value and the last octet (used by the hosts) would remain 0

Try working out the first, second and third valid Network IDs for the examples below:

1. 192.168.2.9/30
2. 192.168.2.129/25
3. 131.107.4.1/22

Step 3 – From the list of Network IDs locate the correct Network ID for our host

In our original example we started off with the IP Address 192.168.2.33/27 and we have already worked out that its Increment value is 32 and that some of the available Network IDs are:

192.168.2.0/27

192.168.2.32/27

192.168.2.64/27

192.168.2.96/27

192.168.2.128/27

We need to look at our IP Address in the 4th Octet, in our example it is 33. The number 33 falls between two of our valid Network IDS

192.168.2.32/27

AND

192.168.2.64/27

When working out a computers Network ID the lower of the two numbers is the correct Network ID, so for computer 192.168.2.33/27 its Network ID is

192 168.2.32/27

Using the example above work out the network IDs for the following IP Addresses:

192.168.2.9/30 131.107.4.1/22

192.168.2.129/25

<u>IPv4 Worksheet 2 – How many host?</u>

Not Binary Table

256	128	64	32	16	8	4	2	Hosts or Networks
8	7	6	5	4	3	2	1	No. of Bits

This table should not be confused with the binary table on IPv4 Worksheet 1. This table will be used to answer some very specific types of questions on Microsoft and CISCO exams. The top row represents either the number of Hosts or the Number of Networks depending on the question, the bottom row always represents the number of Bits.

Example 1

You have a HOST IP Address of 192.168.2.2/24 based on this address how many hosts addresses can you have on the network that this host is on?

When working out how many hosts we can have on a network we have to find out how many host bits we have to play with, in this example we are working with a /24 address, this means that we have 8 host bits left. To work this out we must remember that IPv4 uses a 32bit addressing scheme so if we are using 24 bits for our networks that means we have 8 bits left for the host (32-24=8)

Other examples would be……

192.168.2.1/26 is our Host IP Address so we have 6 Host Bits left (32-26=6)

192.168.2.50/30 is our Host IP Address so we have 2 Host Bits left (32-30=2)

131.197.2.2/23 is our Host IP Address so we have _____ Host Bits left (32-___ = ____)

In Example 1 then we have 8 Host bits, if we use our NOT BINARY table it can help us work out how many host addresses we can create with 8 Host bits.

Using the NOT BINARY table use the bottom line that represents the number of Bits, find the number 8 and write down the number above there, in our example that number would be 256. This number represents the total number of IP Addresses made available with 8 bits, but not all of these addresses can be used for Hosts. When working out the number of valid host addresses we must Minus 2 (-2) from our number to account for the Network ID and the Host id that we cannot use. So with 8 host bits we can have 256 total addresses but only 254 usable host addresses (256-2=254). Another way to say this is that with 8 host bits we can have 254 hosts on that network.

Other examples would be……

192.168.2.1/26 is our Host IP Address so we have 6 Host Bits left (32-26=6). With 6 host bits we can have 64 total addresses which means we can have 62 hosts on that network (64-2=62)

192.168.2.50/30 is our Host IP Address so we have 2 Host Bits left (32-30=2). With 2 host bits we can have 4 total addresses which means we can have 2 hosts on that network (4-2=2)

131.197.2.2/23 is our Host IP Address so we have _____ Host Bits left (32-___ = ____) with ____ host bits we can have ___ total addresses which means we can have ____ hosts on that network (___-2=___)

Try These…..

For the following host addresses please work out how many hosts you can have on each of the networks these hosts are one:

1. 192.168.2.2/26 2) 192.168.2.33/25 3) 155.33.33.6/29

IPv4 Worksheet 3 – How many Networks?

Not Binary Table

256	128	64	32	16	8	4	2	Hosts or Networks
8	7	6	5	4	3	2	1	No. of Bits

This table should not be confused with the binary table on IPv4 Worksheet 1. This table will be used to answer some very specific types of questions on Microsoft and CISCO exams. The top row represents either the number of Hosts or the Number of Networks depending on the question, the bottom row always represents the number of Bits.

Example 1

Given the address of 192.68.2.0/27 how many subnets have been created?

This example relies on using knowing our class A, class B and class C IPv4 address ranges:

A first octet 1-126

B first octet 128 – 191

C first octet 192 – 223

And that we know that class A address ranges are assigned with a /8 subnet mask and that a class B address range is assigned with a /16 subnet mask and that a /24 address is given with class C address ranges.

In our example we have a class C address so it should be using a /24 subnet mask but instead it is using a /27. Another way to say this is that 3 bits are being used for the subnets (27-24=3)

Other examples are….

192.168.2.32/28 – This is a class C address so should be using a /24 address but is using a /28 address which means we have 4 subnet bits (28-24=4)

131.107.0.1/19 – This is a class B address so should be using a /16 address but is using a /19 address which means we have 3 subnet bits (19-16=3)

210.1.1.1/26 – This is a class ___ address so should be using a /___ address but is using a /26 address which means we have __ subnet bits (26-___=__)

In our Example 1 we have work out that we have 3 bits for making subnets, using the NOT BINARY table we can work out how many subnets we can create with 3 bits. Using the NOT BINARY table use the bottom row and find the number 3, find the number above there and write it down in our case that is 8, this is the number of subnets I can create with 3 Bits.

Other examples are….

192.168.2.32/28 – This is a class C address so should be using a /24 address but is using a /28 address which means we have 4 subnet bits (28-24=4). With 4 subnet bits we can create 16 subnets.

131.107.0.1/19 – This is a class B address so should be using a /16 address but is using a /19 address which means we have 3 subnet bits (19-16=3). With 3 subnet bits we can create 8 subnets.

210.1.1.1/26 – This is a class ___ address so should be using a /___ address but is using a /26 address which means we have __ subnet bits (26-___=__). With ____ subnet bits we can create ___ Subnets.

Try Theses……

For each of the following please work out how many subnets can be created:

1. 191.107.2.2/20 2) 136.136.136.2/23 3) 192.168.2.7/30

Example 2

You branch office has been assigned a network address of 192.168.1.0/24 for you branch office but you need to create 20 subnets, what new CIDR notation would you use?

Is this example we use the NOT BINARY table but this time we use the top row, remember this row represents Hosts or Networks, in this example it represent Networks. We need 20 subnets so we use the top row and find a number equal to or greater than 20 (as close as possible) in our example that would be 32 (16 too low and 64 too high) we then take the number below there and write it down, in our example that is 5. This is the number of bits I need to make at least 20 subnets.

Other examples are….

You branch office has been assigned 131.107.0.0/16 and you need 100 subnets. For 100 subnets we need 7 bits

You branch office has been assigned 192.168.2.0/24 but you need 10 subnets. For 10 subnets we need 4 bits

You branch office has been assigned 175.168.2.0/24 but you need 50 subnets. For 50 subnets we need ____ bits

In our Example 2 we have worked out that we need 5 bits to make our 20 subnets (actually we can make a total of 32 subnets with 5 bits) we now need to work out the new CIDR notation that will be used on our network, we take the original CIDR notation, in our example 2 that was /24 and add our number of bits to it so 24+5=29 so our network will use /29 with the first network being 192.168.1.0/29.

Other examples are….

You branch office has been assigned 131.107.0.0/16 and you need 100 subnets. For 100 subnets we need 7 bits. If we need 7 subnet bits and we started off with /16 then our new CIDR notation will be /23 (16+7=23) with the first network id being 131.107.0.0/23

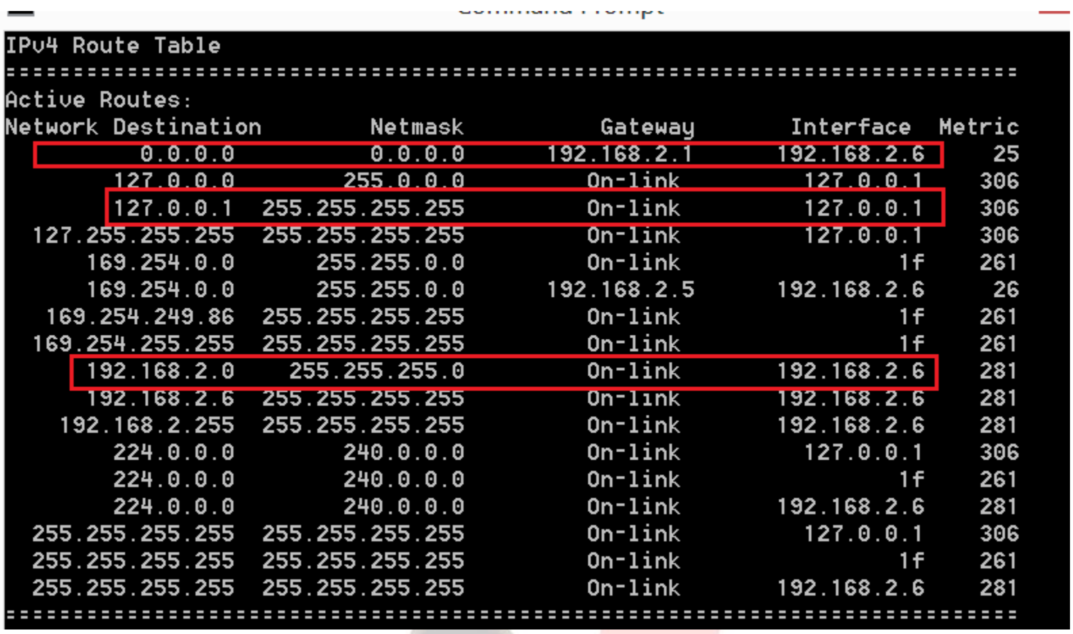
You branch office has been assigned 192.168.2.0/24 but you need 10 subnets. For 10 subnets we need 4 bits. If we need 4 subnet bits and we started off with /24 then our new CIDR notation will be /28 (24+4=28) with the first network ID being 192.168.2.0/28

You branch office has been assigned 175.168.2.0/24 but you need 50 subnets. For 50 subnets we need ____ bits. If we need ___ subnet bits and we started off with /24 then our new CIDR notation will be /___ (24+___=___) with the first network ID being

IPv4 Routing Table – Route Command and PowerShell

Each IPv4 host has a routing table that it uses to make decisions on how traffic should leave a host and in which direction it should be sent. Most hosts have a simple routing table that includes information about the networks that the host is directly connected to and a default route (Default Gateway) that they use to connect to all other networks. Networks routers have more complicated routing tables.

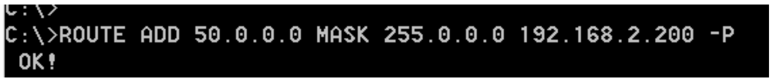
Here is a routing table from a client machine that is connected to multiple networks:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.2.1     192.168.2.6     25
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
      169.254.0.0      255.255.0.0         On-link               1f    261
      169.254.0.0      255.255.0.0      192.168.2.5     192.168.2.6     26
   169.254.249.86  255.255.255.255         On-link               1f    261
  169.254.255.255  255.255.255.255         On-link               1f    261
      192.168.2.0    255.255.255.0         On-link      192.168.2.6    281
      192.168.2.6  255.255.255.255         On-link      192.168.2.6    281
    192.168.2.255  255.255.255.255         On-link      192.168.2.6    281
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link               1f    261
        224.0.0.0        240.0.0.0         On-link      192.168.2.6    281
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link               1f    261
  255.255.255.255  255.255.255.255         On-link      192.168.2.6    281
===========================================================================
```

We can use the command **ROUTE PRINT** to see a hosts routing table
Highlighted are three common entries in a client machines routing table, 192.168.2.0 route is a network that this computer is connected to, in the interface column we can see the details of the interface (192.168.2.6) on this host that is used to connect to the 192.168.2.0 network.
We can also see an entry for 127.0.0.1, this is the loopback address used for testing the IP stack
The finale Highlighted entry 0.0.0.0 is the default gateway address, this is the route that we will send all other traffic to hat we don't have a direct connection or other path to. In the Gateway column we can see the next hop IP address 192.168.2.1 that will be used to connect to all other networks. The Default Gateway address **must** be the **host** address of the closet Router interface.

On occasion we might need to add routes to host routing table manually. To add, alter and delete routes we use the **ROUTE** command:

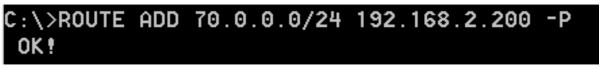


```
C:\>
C:\>ROUTE ADD 50.0.0.0 MASK 255.0.0.0 192.168.2.200 -P
 OK!
```

Here we can see the **ROUTE ADD** command has been used to reference a remote network 50.0.0.0,
50.0.0.0 = the remote network address
255.0.0.0 = the Subnet mask used on that network
192.168.2.200 = is the gateway (next hop) this host is going to use to connect to network 50.0.0.0

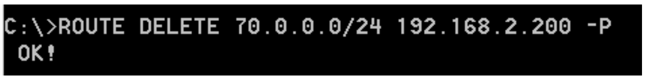
-p = Makes the route persistent in the host routing table

As well as identify the subnet mask using the MASK key word we can also use CIDR notation.



```
C:\>ROUTE ADD 70.0.0.0/24 192.168.2.200 -P
 OK!
```

To remove a route we use the **ROUTE DELETE** command



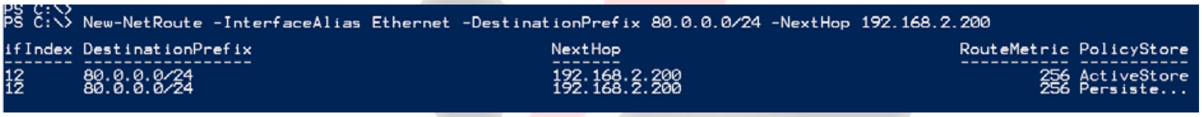
```
C:\>ROUTE DELETE 70.0.0.0/24 192.168.2.200 -P
 OK!
```

Here we have use the **ROUTE DELETE** command to remove the 70.0.0.0/24 network from the routing table.

PowerShell

As well as the ROUTE command we can also use PowerShell to edit and add entries to the routing table:

NEW-NETROUTE is used to add an entry to the routing table



```
PS C:\>
PS C:\> New-NetRoute -InterfaceAlias Ethernet -DestinationPrefix 80.0.0.0/24 -NextHop 192.168.2.200
ifIndex DestinationPrefix                                    NextHop                              RouteMetric PolicyStore
------- -----------------                                    -------                              ----------- -----------
12      80.0.0.0/24                                          192.168.2.200                                256 ActiveStore
12      80.0.0.0/24                                          192.168.2.200                                256 Persiste...
```

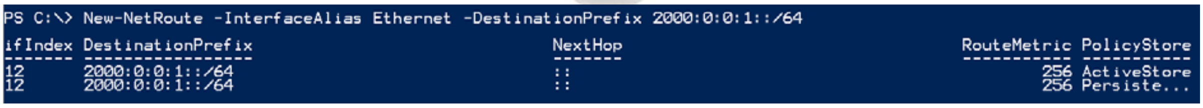
-InterfaceAlias = Interface display name (you could also use –InterfaceIndex), this is the exit interface in the host

-DestinationPrefix = The subnet you are trying to access and its Mask in CIDR format

-NextHop = Default Gateway address used to send traffic to network 80.0.0.0

Routes added using this method are automatically persistent.

IPv6 routes can also be added using New-NetRoute cmdlet (as can ROUTE). Below we can see a route to destination network 2000:0:0:1::/64, notice that we haven't included a next hop address, this means the next hop :: will be on-link meaning that the route is directly reachable



```
PS C:\> New-NetRoute -InterfaceAlias Ethernet -DestinationPrefix 2000:0:0:1::/64
ifIndex DestinationPrefix                                    NextHop                              RouteMetric PolicyStore
------- -----------------                                    -------                              ----------- -----------
12      2000:0:0:1::/64                                      ::                                           256 ActiveStore
12      2000:0:0:1::/64                                      ::                                           256 Persiste...
```

Instead of –InterfaceAlias Ethernet we could have used –interfaceindex 12 (12 is the index number of the Ethernet interface)

Set-Netroute = Make changes to an existing route in the routing table

Remove-Netroute = Remove a route from the routing table

DAY 1 Fill in the Blanks

Please fill in the Blanks

1. DCPROMO has been depreciated in Windows Server 2012 R2, it is still used but only for_______________. Today to promote a member server to be a Domain Controller we can use tools like _____________ or ___________.
2. PowerShell is an important tool in Windows Server 2012 R2, amongst other things it can be used to add a new domain to an existing forest by using the _____________ CMDLet and it can be used to add a new domain controller to an existing domain using the ____________ CMDLet.
3. Once you have installed an edition of Windows Server 2012 R2 you then add _____ and ______ to give your server a role to do on your network. To add new _______ and _______ we can use Server Manager or we can use the PowerShell CMDLet_____________ or the ________ command line tool which can also be used to service offline images as well.
4. Windows Server 2012 R2 as introduced several improvement in regards to Virtualized Domain Controllers, these include _______ which makes it safe to roll back our DC's if we make changes that called error. They also include the ability to ______ DC's that allow us to rapidly roll out new DC's
5. We often describe Active Directory Domain Controllers as being equal to each other, when we say that we are talking about the Domain Partition, each DC in a domain has read/write access to the domain partition. But some roles are so important that they can only run on a single Domain Controller at a time, we call these our Operation Master roles. There are two forest wide roles, these are ________ and _______. There are 3 domain wide roles, these are __________, ___________ and __________.
6. When upgrading an existing Windows 2008 or Windows 2008 R2 domain controller to Windows Server 2012 don't forget that you have to run the ADPREP command with the _______ Switch and the _______ Switch.
7. NTDSUTIL.exe is a general purpose tool for managing the NTDS.DIT database, we can use it to access several prompts:
    1. To move the NTDS.dit directory we would go to the______ Prompt
    2. To Create a an install from media set we would go to the ________ Prompt
    3. To Perform a restore of a single object we would go to the _______ Prompt
8. When creating a group structure to assign access to a printer we first choose the appropriate group type, so we should create _________ groups and not _________ groups. We would then create groups so that we can follow the Microsoft

recommended strategy for groups this is ____.

9. Global Catalogues are used during Logons and Look ups of AD, we can add additional attributes to be stored on Global Catalogues by editing the _________ Partition using the ____________ tool.
10. We create OUs to better organize objects but also to___________ and so that we can___________.

Day 1 Additional Labs

The Additional Labs should be done as much as possible without referring to the Official curriculum material (Skillpipe material)

1) Start Virtual Machines DC1 and DC2
2) Login in to both DC1 and DC2 using the username Administrator and the Password Pa$$w0rd
3) Using just PowerShell promote DC2 to be an additional domain controller in the FB.Com domain. It should be a global catalogue server but not a DNS server.
4) Using just PowerShell create 3 user accounts named FBUser1, FBUser2 and FBUser3
5) Using just PowerShell change the organisation name for all three uses to FB
6) Using just PowerShell get a list of all users in the Leeds OU and then using PowerShell change their set their office location to Leeds
7) Using just PowerShell create Global Security group called LeedsAdmins
8) Using just PowerShell add Users FBUser1, FBUser2 and FBUser3 to the newly created LeedsAdmins group.

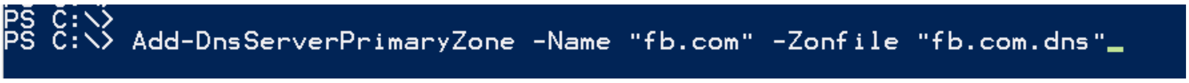
Day 2

Managing DNS from PowerShell and DNSCMD

PowerShell

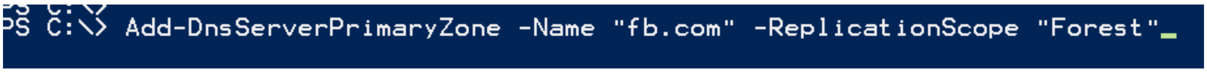
We can use PowerShell to create DNS zones, DNS Records and to manage the DNS server itself.

Add-DnsServerPrimaryZone can be used to create both standard primary and ADI zones, in the example below we have used Add-DnsServerPrimaryZone to create a standard primary zone called FB.COM that uses a zone file called fb.com.dns



```
PS C:\>
PS C:\> Add-DnsServerPrimaryZone -Name "fb.com" -Zonfile "fb.com.dns"
```

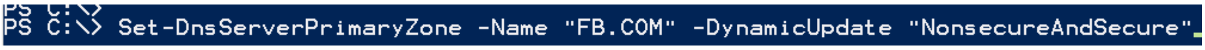
If we use the same cmdlet but don't specify a zone file we can specify a replication scope and create an ADI zone, the example below create and ADI zone called FB.Com replicated to the whole forest.



```
PS C:\>
PS C:\> Add-DnsServerPrimaryZone -Name "fb.com" -ReplicationScope "Forest"
```

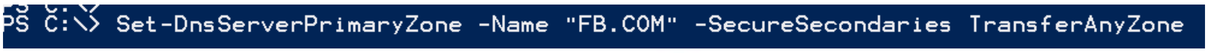
-ReplicationScope can be Forest, Domain, Legacy or Custom if you want to replicate the ADI zone to a custom application partition.

Set-DnsServerPrimaryZone can be used to adjust the properties of both Standard Primary and ADI zones. We can change the zone type, change dynamic update options, allow zone transfer etc. the example below sets the dynamic update type to non-secure and secure for a zone.



```
PS C:\> Set-DnsServerPrimaryZone -Name "FB.COM" -DynamicUpdate "NonsecureAndSecure"
```

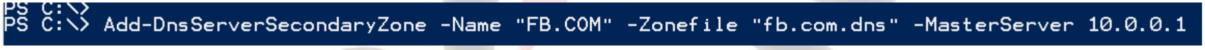
The Example below changes Zone transfer setting for a zone called FB.COM



```
PS C:\> Set-DnsServerPrimaryZone -Name "FB.COM" -SecureSecondaries TransferAnyZone
```

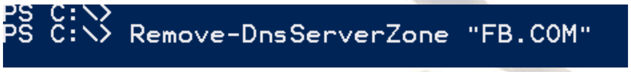
The –SecureSecondaries switch can be set to NOTransfer, TransferAnyServer, TransferToZoneNameServer and TransferToSecureServers

Add-DnsServerSecondaryZone is used to add a Secondary zone for an existing zone. In the example below we have created a secondary zone for the FB.COM domain



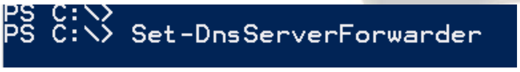
```
PS C:\> Add-DnsServerSecondaryZone -Name "FB.COM" -Zonefile "fb.com.dns" -MasterServer 10.0.0.1
```

Remove-DnsServerZone can be used to remove a zone, in the example below we have used it to remove a zone called FB.COM



```
PS C:\> Remove-DnsServerZone "FB.COM"
```

Set-DnsServerForwarder is used to add a forwarder record to a zone



```
PS C:\> Set-DnsServerForwarder
```

<u>DNSCMD</u>

DNSCMD is a command line interface for DNS, it can be used to manage all aspects of you DNS Server.

All commands use the syntax
DNSCMD /*Switch Parameter*

DNSCMD Switch	**Description**
/Zonedd	Adds a zone to the DNS Server
/Zonedelete	Removes a zone from a DNS Server
/RecordAdd	Adds a record to a specified zone
/Config	Changes values in for the DNS server and individual zones
/ZoneExport	Creates a Text file that lists all the resource records of a specified zone

DHCP Console Icon References

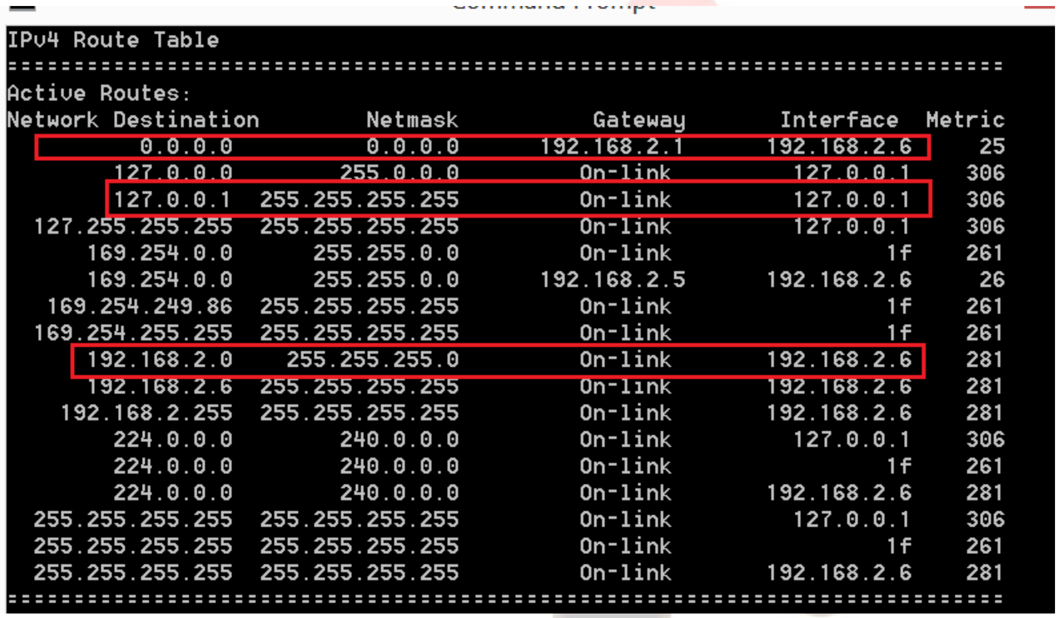
Use the link bellows to view details of DHCP icons and there meanings

https://technet.microsoft.com/en-us/library/gg722802(v=ws.10).aspx

IPv4 Routing tables – Route Command and PowerShell

Each IPv4 host has a routing table that it uses to make decisions on how traffic should leave a host and in which direction it should be sent. Most hosts have a simple routing table that includes information about the networks that the host is directly connected to and a default route (Default Gateway) that they use to connect to all other networks. Networks routers have more complicated routing tables.

Here is a routing table from a client machine that is connected to multiple networks:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.2.1      192.168.2.6     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      169.254.0.0      255.255.0.0         On-link                1f    261
      169.254.0.0      255.255.0.0      192.168.2.5      192.168.2.6     26
   169.254.249.86  255.255.255.255         On-link                1f    261
  169.254.255.255  255.255.255.255         On-link                1f    261
      192.168.2.0    255.255.255.0         On-link       192.168.2.6    281
      192.168.2.6  255.255.255.255         On-link       192.168.2.6    281
    192.168.2.255  255.255.255.255         On-link       192.168.2.6    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link                1f    261
        224.0.0.0        240.0.0.0         On-link       192.168.2.6    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link                1f    261
  255.255.255.255  255.255.255.255         On-link       192.168.2.6    281
===========================================================================
```

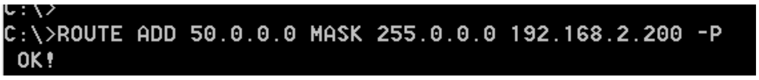
We can use the command **ROUTE PRINT** to see a hosts routing table

Highlighted are three common entries in a client machines routing table, 192.168.2.0 route is a network that this computer is connected to, in the interface column we can see the details of the interface (192.168.2.6) on this host that is used to connect to the 192.168.2.0 network.

We can also see an entry for 127.0.0.1, this is the loopback address used for testing the IP stack

The finale Highlighted entry 0.0.0.0 is the default gateway address, this is the route that we will send all other traffic to hat we don't have a direct connection or other path to. In the Gateway column we can see the next hop IP address 192.168.2.1 that will be used to connect to all other networks. The Default Gateway address **must** be the **host** address of the closet Router interface.

On occasion we might need to add routes to host routing table manually. To add, alter and delete routes we use the **ROUTE** command:



```
C:\>
C:\>ROUTE ADD 50.0.0.0 MASK 255.0.0.0 192.168.2.200 -P
 OK!
```

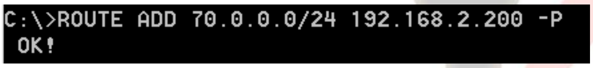
Here we can see the **ROUTE ADD** command has been used to reference a remote network 50.0.0.0,

50.0.0.0 = the remote network address

255.0.0.0 = the Subnet mask used on that network

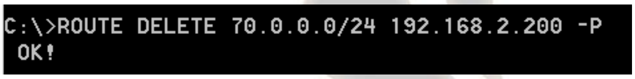
192.168.2.200 = is the gateway (next hop) this host is going to use to connect to network 50.0.0.0
-p = Makes the route persistent in the host routing table

As well as identify the subnet mask using the MASK key word we can also use CIDR notation.



```
C:\>ROUTE ADD 70.0.0.0/24 192.168.2.200 -P
 OK!
```

To remove a route we use the **ROUTE DELETE** command



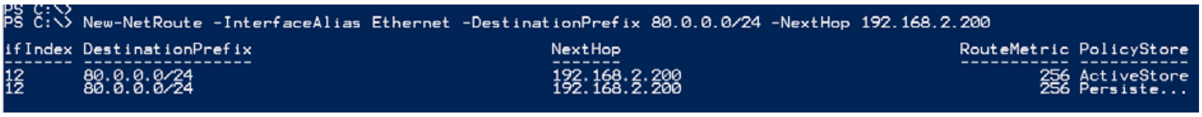
```
C:\>ROUTE DELETE 70.0.0.0/24 192.168.2.200 -P
 OK!
```

Here we have use the **ROUTE DELETE** command to remove the 70.0.0.0/24 network from the routing table.

<u>**PowerShell**</u>

As well as the ROUTE command we can also use PowerShell to edit and add entries to the routing table:

NEW-NETROUTE is used to add an entry to the routing table

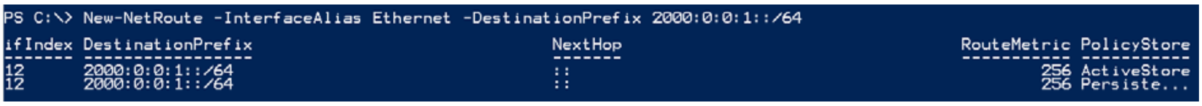


```
PS C:\>
PS C:\> New-NetRoute -InterfaceAlias Ethernet -DestinationPrefix 80.0.0.0/24 -NextHop 192.168.2.200

ifIndex DestinationPrefix                          NextHop                                RouteMetric PolicyStore
------- -----------------                          -------                                ----------- -----------
12      80.0.0.0/24                                192.168.2.200                                  256 ActiveStore
12      80.0.0.0/24                                192.168.2.200                                  256 Persiste...
```

-InterfaceAlias = Interface display name (you could also use –InterfaceIndex), this is the exit interface in the host
-DestinationPrefix = The subnet you are trying to access and its Mask in CIDR format
-NextHop = Default Gateway address used to send traffic to network 80.0.0.0

Routes added using this method are automatically persistent.

Below we can see a route to destination network 2000:0:0:1::/64, notice that we haven't included a next hop address, this means the next hop :: will be on-link meaning that the route is directly reachable



```
PS C:\> New-NetRoute -InterfaceAlias Ethernet -DestinationPrefix 2000:0:0:1::/64
ifIndex DestinationPrefix                               NextHop                                  RouteMetric PolicyStore
------- -----------------                               -------                                  ----------- -----------
12      2000:0:0:1::/64                                 ::                                               256 ActiveStore
12      2000:0:0:1::/64                                 ::                                               256 Persiste...
```

Instead of –InterfaceAlias Ethernet we could have used –interfaceindex 12 (12 is the index number of the Ethernet interface)

Set-Netroute = Make changes to an existing route in the routing table
Remove-Netroute = Remove a route from the routing table

DHCP Option 60 Video

DHCP option 60 is used when both DHCP and WDS are on the same server, this short video will explain how to configure DHCP option 60 and when to use it:

DHCP Option 60

Or

https://www.youtube.com/watch?v=-y7Hr3WrVjA&list=PL2QNrvCUc_M9ZpX3LRDdPojvlfL99aY10&index=2

IPv6

Types of IPv6 Address:

Global Unicast Addresses

- These addresses start with either 2000:: or 3000::
- These addresses are assigned by ISP's and are globally unique
- These addresses equivalent to Public IPv4 addresses

Unique Local Unicast Addresses

- These addresses start with FD00:: or FC00::
- These addresses are assigned internally and are routable throughout you organisation
- These addresses are equivalent to Private IPv4 addresses

Link Local Unicast Addresses

- These addresses start with FE80::
- These addresses are assigned automatically by the IPv6 host itself and are not routable. The closest equivalent IPv4 address is an APIPA address, however unlike APIPA addresses that usually represent a problem on you network Unique Local addresses are a requirement for IPv6 and are the preferred address type for local network communication

Remember…….

Global Unicast addresses will be assigned to your organization with a /48 bit prefix. This will include the global routing prefix which identifies your region, your ISP and a set of BITS that represent your organization. The next 16 bits of an IPv6 Address can be used for subnets in your organization taking you up to a /64 bit prefix. So with 64 bits representing you and your subnets that means there will be 64 bits that are used for Hosts.

64bits for networks and 64bits used for hosts is the standard split so we can use features like Stateless auto-configuration

Q1) if you run a branch office and are assigned an address of 2001:0001:0001:0100:/56 from head office that means you have 8 Subnet bits left for your branch (64-56=8). With 8 subnets bits how many subnets can you have in your branch office?

Q2) if you need an internally routable address for a host in your organization which address would you choose?

1. 2000:0001:0001:0001:a2af:0001:0030:0001/64
2. Fe80:0011:a34f:a3ff:fffe:0001:a34f:a3fe/64
3. Fd00:ffe3:5463:213f:0001:000a:aaaf:123a/64
4. Dc33::0123::a2af:a4fe::/64

IPv6 Subnetting Example 1

IPv6 addresses are 128 bits in length and written in HEX. Each HEX digit is 4 bits in length.

In IPv6 each section of the address is 16 bits in length, in HEX that means each section can start at 0000 and end at FFFF

2001:0000:0000:0800:: /54 is assigned to your branch from head office. You have lots of subnets in your branch and you need to work out what the first and last subnet addresses will be?

Whatever our subnet address are the first 54 bits will stay the same. These bits are assigned by head office and cannot change, so all of our subnets will start with the following 54 bits.

IN BINARY

0010 0000 0000 0001:0000 0000 0000 0000:0000 0000 0000 0000**:0000 10**00

In Hex this is how our IPv6 address will look

2001:0000:0000:**0800**::/64

This is our first subnet address (when working with IPv6 subnets we will almost always use /64 as the prefix value).

Now we need to work out the last network address

HEX 0800 = 0000 1000 0000 0000 in binary

The first 6 bits are protected (assigned from head office) and will not change, the last ten bits can change starting at:

00 0000 0000 all the way up to 11 1111 1111

In full this is

0000 1000 0000 0000 to 0000 1011 1111 1111

If we convert theses number to HEX we get

0800 to 0BFF

So our subnets will be from:

2001:0000:0000:0800::/64 (first subnet) to 2001:0000:0000:0BFF::/64 (last Subnet

DHCP for IPv6 Video

This video looks at configuring DHCP to support an IPv6 network

DHCP for IPv6

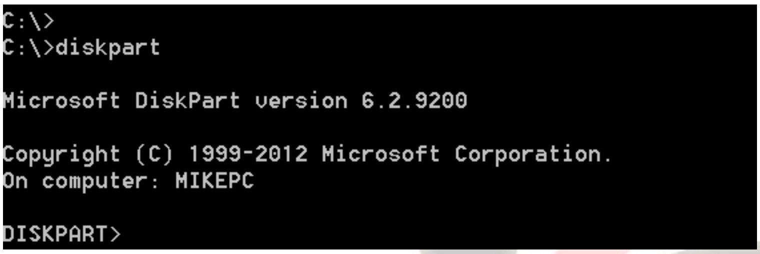
Or

https://www.youtube.com/watch?v=ZBQNdqvLZps&index=3&list=PL2QNrvCUc_M9ZpX3LRDdPojvlfL99aY10

Storage - DiskPart

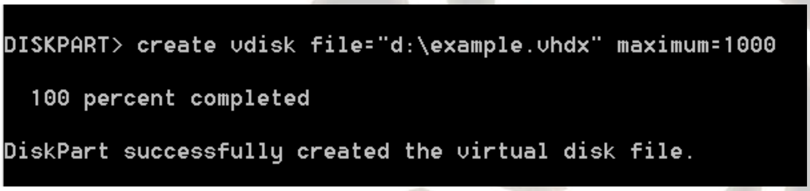
DiskPart is a text-mode command interpreter that enables you to manage disks, partitions, volumes or Virtual hard disks. In the following examples we will be using DiskPart to create and manage Virtual Disks.

By typing the command **DiskPart** at the command prompt you get access to the DiskPart prompt, form here you can run the rest of commands you need.



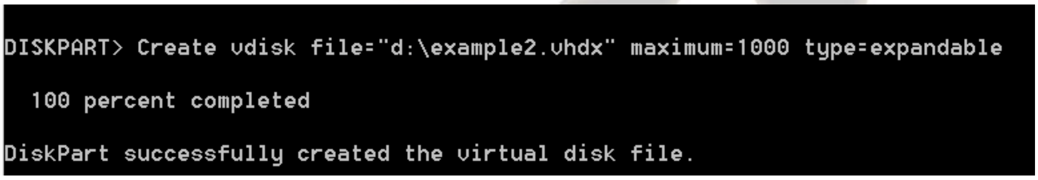
```
C:\>
C:\>diskpart

Microsoft DiskPart version 6.2.9200

Copyright (C) 1999-2012 Microsoft Corporation.
On computer: MIKEPC

DISKPART>
```

By using the **Create** command we can create a vdisk, in this example we create a disk called example.vhdx that is 1GB in size.



```
DISKPART> create vdisk file="d:\example.vhdx" maximum=1000

  100 percent completed

DiskPart successfully created the virtual disk file.
```

In the Example below we have used the **type** command to make this vdisk that is a dynamically expanding disk

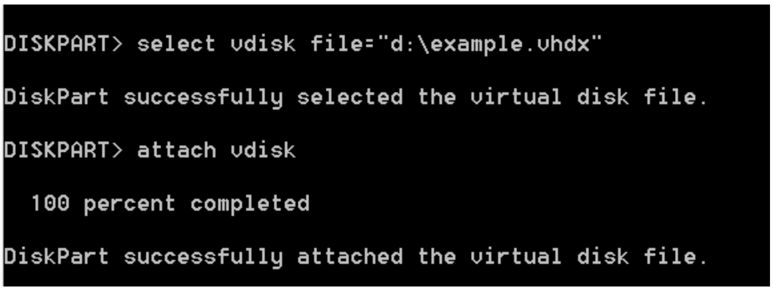


```
DISKPART> Create vdisk file="d:\example2.vhdx" maximum=1000 type=expandable

  100 percent completed

DiskPart successfully created the virtual disk file.
```

We can also use the Create vdisk to create Differencing disks and to copy existing VHD/VHDX files.

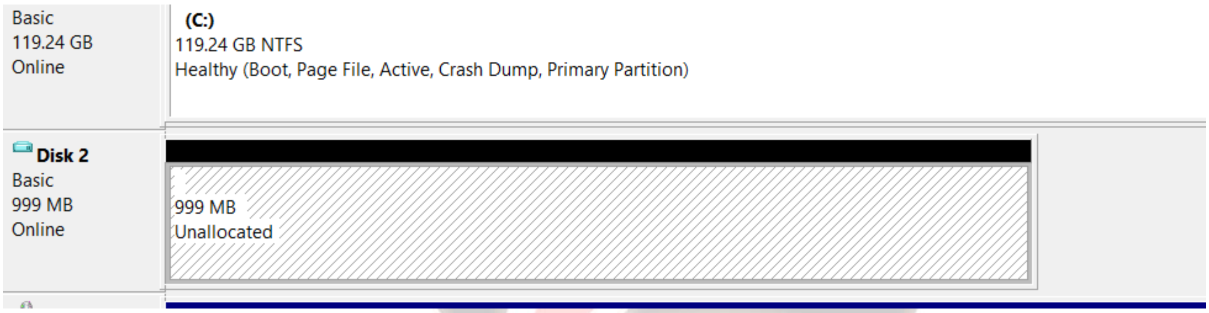
One other useful feature of DiskPart is its ability to attach a VHD/VHDX file to a computer, making available as a local disk in the machine. Once attached we could create partitions, format them and assign drive letters and then copy data to it. Also we can use DISM to add an image file to the attached disk.

First we need to set the focus of DiskPart on the VHD/VHDX that we want to attach, ones we have set focus we can then attach the VHD/VHDX file.



```
DISKPART> select vdisk file="d:\example.vhdx"

DiskPart successfully selected the virtual disk file.

DISKPART> attach vdisk

  100 percent completed

DiskPart successfully attached the virtual disk file.
```

In the example above we have set focus on a virtual disk called Example.vhdx by using the **select vdisk** command, then we use the **attach vdisk** command to attach it.



Basic
119.24 GB
Online

(C:)
119.24 GB NTFS
Healthy (Boot, Page File, Active, Crash Dump, Primary Partition)

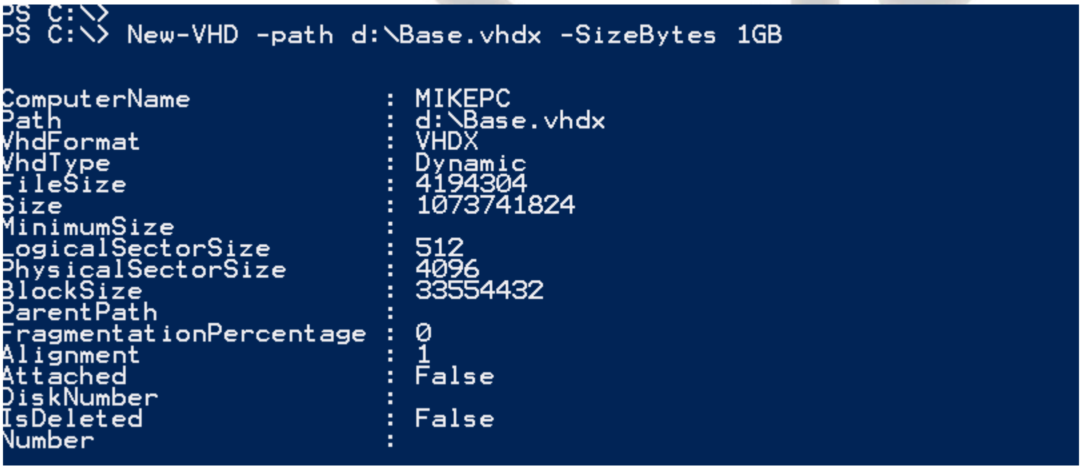
Disk 2
Basic
999 MB
Online

999 MB
Unallocated

The disk then appears as a disk in disk manager ready to use.

Storage – PowerShell

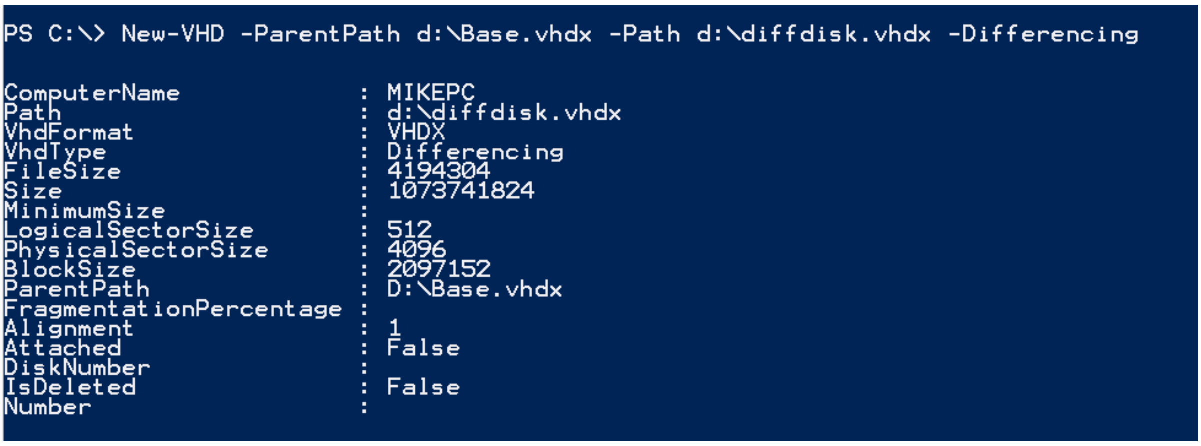
New-VHD can be used to create vhd/vhdx files from PowerShell, below we have created a .VHDX file called Base.vhdx that is 1GB in size



```
PS C:\>
PS C:\> New-VHD -path d:\Base.vhdx -SizeBytes 1GB

ComputerName            : MIKEPC
Path                    : d:\Base.vhdx
VhdFormat               : VHDX
VhdType                 : Dynamic
FileSize                : 4194304
Size                    : 1073741824
MinimumSize             :
LogicalSectorSize       : 512
PhysicalSectorSize      : 4096
BlockSize               : 33554432
ParentPath              :
FragmentationPercentage : 0
Alignment               : 1
Attached                : False
DiskNumber              :
IsDeleted               : False
Number                  :
```

One useful way to conserve disk space is to use Differencing disks, each differencing disk is based on a parent. The parent disk would usually include a syspreped operating system and each differencing disk is then used to create a Virtual machine, the differencing disk is then used to save the changes that each VM wants to make.

New-VHD can be used to make the differencing disk and associate with a parent disk.



```
PS C:\> New-VHD -ParentPath d:\Base.vhdx -Path d:\diffdisk.vhdx -Differencing

ComputerName              : MIKEPC
Path                      : d:\diffdisk.vhdx
VhdFormat                 : VHDX
VhdType                   : Differencing
FileSize                  : 4194304
Size                      : 1073741824
MinimumSize               :
LogicalSectorSize         : 512
PhysicalSectorSize        : 4096
BlockSize                 : 2097152
ParentPath                : D:\Base.vhdx
FragmentationPercentage   :
Alignment                 : 1
Attached                  : False
DiskNumber                :
IsDeleted                 : False
Number                    :
```

Convert-VHD can be used to convert an existing vDisk to a different type.

NOTE: Storage pools have their own set of Cmdlets for creating storage pools, virtual disks and partitions. The cmdlet **NEW-VirtualDisk** is used to create virtual disks but only for use in a specified storage pool, it is not used to create a vDisk for general use.

Other CMDLets used for creating and managing storage pools are:

New-Storagepool – create a new storage pool from Physical disks
New-Partition – Creates a new partition on a specified disk object
Add-PhysicalDisk – Adds a physical disk to a specified storage pool

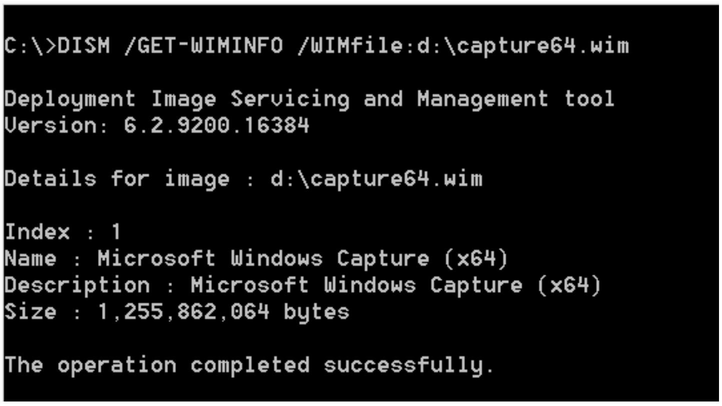
DISM – Online and Offline Servicing

Deployment Image Servicing and Management (DISM) is a command line tool used to service Windows images offline. It will allow you to install, uninstall, configure and update Windows features, packages and drivers. As well as servicing image offline DISM can also be used to service online images by for example adding and removing features from a running version of Server 2012. This is particularly useful for managing Server core deployments. DISM is installed with Windows 8 and also comes as part of the Windows automated Deployment Tool Kit.

Using DISM to view and mount an Image

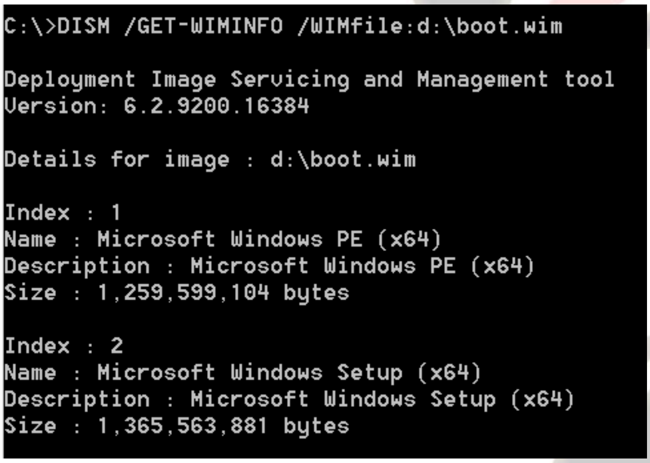
Before adding features, packages or drivers to an existing image you must first choose the image you want to work with and mount that image so we can work with it. Windows images are base around the .WIM imaging format. This is a non-destructive imaging format that uses single instances to save space and has the ability to store multiple individual images inside each .WIM file. So our first task is to look inside a .WIM file and identify the image we want to work with. For this and the following examples I have .WIM files called capture64.wim and boot.wim.

DISM.exe /GET-WIMINFO /WIMFILE:D:\capture.wim



```
C:\>DISM /GET-WIMINFO /WIMfile:d:\capture64.wim

Deployment Image Servicing and Management tool
Version: 6.2.9200.16384

Details for image : d:\capture64.wim

Index : 1
Name : Microsoft Windows Capture (x64)
Description : Microsoft Windows Capture (x64)
Size : 1,255,862,064 bytes

The operation completed successfully.
```

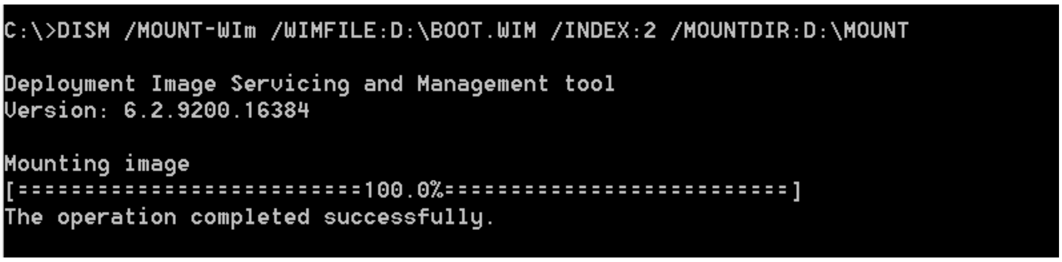
Here we can see the results of using DISM with the **/GET-WIMINFO** switch. We can see inside the .WIM file to view a list of all the images contained within it. Each separate image is give an Index number, in this .WIM file there is only 1 image that has an Index number of 1.
If we run the same command against Boot.wim we can see that there are two images in this file identified as Index 1 and Index 2.



```
C:\>DISM /GET-WIMINFO /WIMfile:d:\boot.wim

Deployment Image Servicing and Management tool
Version: 6.2.9200.16384

Details for image : d:\boot.wim

Index : 1
Name : Microsoft Windows PE (x64)
Description : Microsoft Windows PE (x64)
Size : 1,259,599,104 bytes

Index : 2
Name : Microsoft Windows Setup (x64)
Description : Microsoft Windows Setup (x64)
Size : 1,365,563,881 bytes
```

Once we have identified the image we want to work with by its Index number we can now mount the image so we can begin working with it.

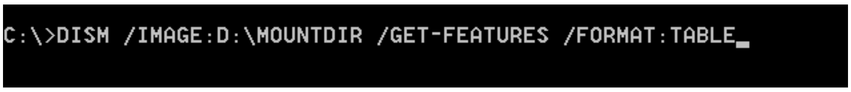
DISM.exe /MOUNT-WIM /WIMFILE:D:\BOOT.WIM /INDEX:2 /MOUNTDIR:D:\MOUNT



```
C:\>DISM /MOUNT-WIm /WIMFILE:D:\BOOT.WIM /INDEX:2 /MOUNTDIR:D:\MOUNT

Deployment Image Servicing and Management tool
Version: 6.2.9200.16384

Mounting image
[==========================100.0%==========================]
The operation completed successfully.
```

Using the **/Mount-WIM** and **/index** switches we identify the image we want to mount and then us the **/mountdir** switch to identify an empty folder where we want to mount it.
Now we have the image mounted we can work with it.

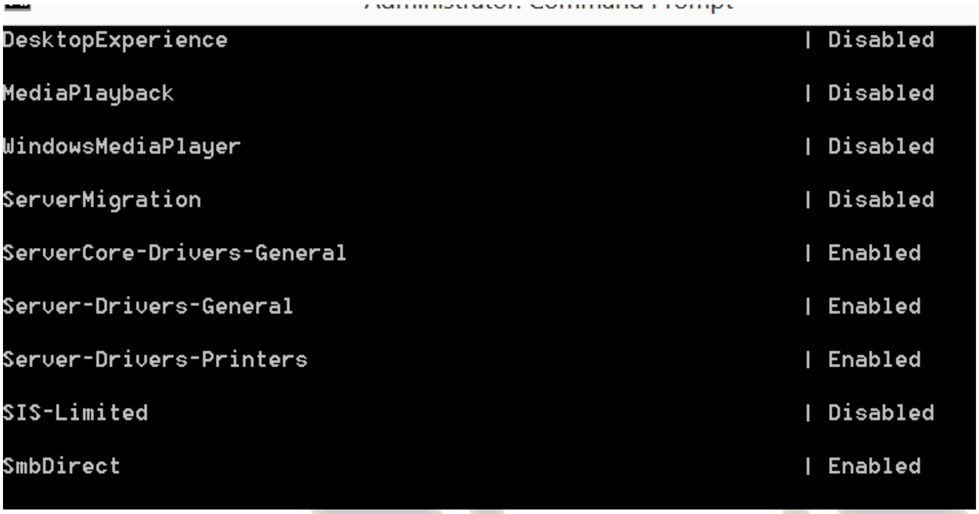
Using DISM to add a feature to a mounted image



```
C:\>DISM /IMAGE:D:\MOUNTDIR /GET-FEATURES /FORMAT:TABLE_
```

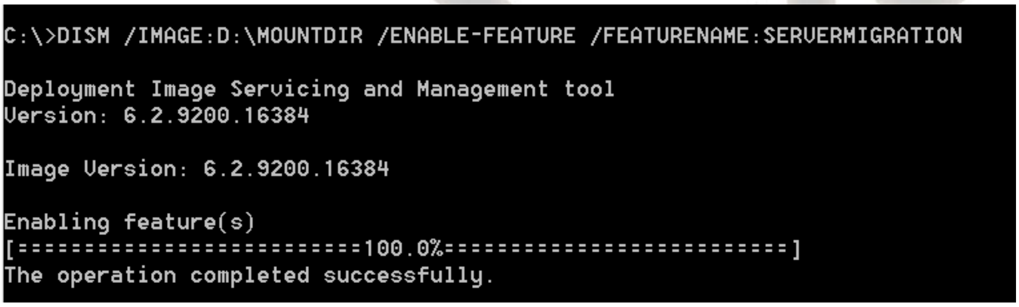
D ISM /IMAGE:D:\MOUNTDIR /GET-FEATURES /FORMTAT:TABLE

With the **/get-features** switch we can see a list of roles and features Enabled and Disabled in the mounted image. The **/format** switch allows me to view the list in one of several ways. Here we can see that the SmbDiret feature is enabled but the ServerMigration tools and disabled.



```
DesktopExperience                                           | Disabled

MediaPlayback                                               | Disabled

WindowsMediaPlayer                                          | Disabled

ServerMigration                                             | Disabled

ServerCore-Drivers-General                                  | Enabled

Server-Drivers-General                                      | Enabled

Server-Drivers-Printers                                     | Enabled

SIS-Limited                                                 | Disabled

SmbDirect                                                   | Enabled
```

DISM /IMAGE:D:\MOUNTDIR /ENABLE-FEATURE /FEATURNAME:SERVERMIGRATION



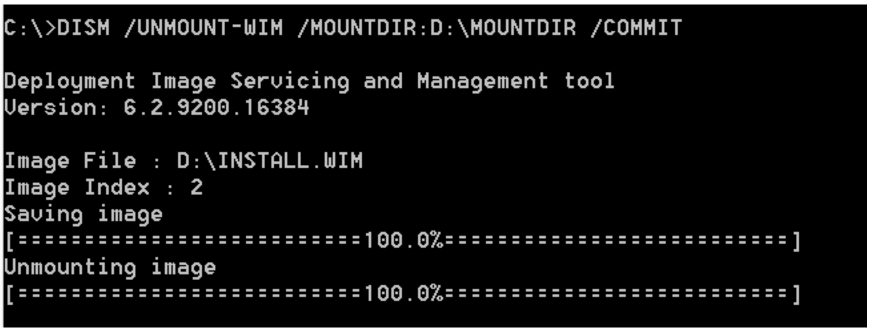
```
C:\>DISM /IMAGE:D:\MOUNTDIR /ENABLE-FEATURE /FEATURENAME:SERVERMIGRATION

Deployment Image Servicing and Management tool
Version: 6.2.9200.16384

Image Version: 6.2.9200.16384

Enabling feature(s)
[==========================100.0%==========================]
The operation completed successfully.
```

With the **/enable-feature** switch and the /**featurename** switch we can enable a role or feature. Here we are enabling the Server Migration feature. This image has all the required binary files available to it to install additional role and features. But if you have an image and the binary files are not install with it then you may also have to use the **/Packagepath** switch to identify the install location.
As well as installing roles/features you can also add other packages like update packages. Using the /ADD-Package switch with the /PackagePath switch you can identify the location of the .cab or .msu file that contains the information about the package you would like to install

DISM /IMAGE:*mounted image path* **/ADD-PACKAGE /PACKAGEPATH:***package path*

Using DISM to unmount and commit an Image

Once we have add the features/packages to our mounted image it needs to be unmounted and the changes we have made committed to the image file.
DISM /UNMOUNT-WIM /MOUNTDIR:D:\MOUNTDIR /COMMIT



```
C:\>DISM /UNMOUNT-WIM /MOUNTDIR:D:\MOUNTDIR /COMMIT

Deployment Image Servicing and Management tool
Version: 6.2.9200.16384

Image File : D:\INSTALL.WIM
Image Index : 2
Saving image
[==========================100.0%==========================]
Unmounting image
[==========================100.0%==========================]
```

Instead of the **/commit** switch you can also use the **/discard** switch the discard changes

Using DISM to perform online servicing and other tasks

To add Drivers
DISM /IMAGE:*image path* /ADD-DRIVER /DRIVER:*path to driver .inf file*

To set OS Edition and Product key
DISM /IMAGE:*image path* /SET-EDITION:*edition name* /PRODUCTKEY:*product key*
The /set-edition switch can be used to change the edition of offline as well as online images

To Service online image (currently installed OS)
DISM /ONLINE – in order to service online images just replace the /Image switch with the /Online switch. Also /enable-windowsfeature can be used to enable a disabled windows feature on an online deployment.

To apply an unattended answer file to an Image file
DISM /IMAGE:*image path* /Apply-Unattedn:*unattend.xml path*

Storage Spaces

Storage Spaces enable us to virtualize storage by grouping together standard disks into storage pools, and then creating Virtual disks (also known as Storage Spaces) from the available capacity in the storage pool. Once we have created a virtual disk we can then create a volume that we can format and begin to write data to.

To create a Storage space you must first create a Storage Pool from the available physical disks. In order to be considered to for a Storage pool the following perquisites must be met:
Disk bus type – Serial Attached SCSI (SAS) or Serial Advanced Technology Attachment (SATA)
Disk Configuration – Physical disks must be at least 4GB in size and disks must be blank and not formatted without any volumes configured
Initially all eligible storage is placed on the Primordial Pool, each disk is given a number and from the Primordial pool we can create out storage pools.

To create a Storage pool using all available physical disk:

```
New-StoragePool –FriendlyName StoragePool1 –StorageSubsystemFriendlyName
“Storage Spaces*” –PhysicalDisks (Get-PhysicalDisk –CanPool $True)
```

To create a Storage pool using just 4 of the 5 available disks:

```
New-StoragePool –FriendlyName StoragePool1 –StorageSubsystemFriendlyName
“Storage Spaces*” –PhysicalDisks (Get-PhysicalDisk PhysicalDisk1, PhysicalDisk2,
PhysicalDisk3, PhysicalDisk4)
```

Disks can be added straight away to a pool (default allocation) or has a HOT SPARE only to be used in the event that a disk in the pool fails.

Once we have created out Storage Pool we can now create a virtual disk from available space. When creating a virtual disk we can choose a layout (resiliency type) and a provisioning type.

Available layouts are:
Simple
Mirror (2way or 3way)
Parity

Available Provision types are:
Thin
Fixed

To create 50GB Vdisk on Storagepool1:

```
New-VirtualDisk –StoragePoolFriendlyName StoragePool1 –FriendlyName VirtualDisk1 –
Size (50GB)
```

To create a Vdisk on Storagepool1 using all available space and setting the layout to Mirror:

```
New-VirtualDisk –StoragePoolFriendlyName StoragePool1 –FriendlyName VirtualDisk1 –
ResiliencySettingName Mirror –UseMaximumSize
```

To create a thin provisioned Vdisk on Storagepool1:

```
New-VirtualDisk –StoragePoolFriendlyName StoragePool1 –FriendlyName VirtualDisk1 –
Size (50GB) –ProvisioningType Thin
```

Now we have a Virtual disk we can create a volume.

When you create a volume, you can configure the size, the drive letter or folder, the file system (NTFS file system or Resilient File System (ReFS)), the allocation unit size, and an optional volume label.

The example below uses Powershell to create a new volume on VirtualDIsk1

```
Get-VirtualDisk –FriendlyName VirtualDisk1 | Get-Disk | Initialize-Disk –Passthru | New-
Partition –AssignDriveLetter –UseMaximumSize | Format-Volume
```

Layouts

Name	Number of Disks	Description
Simple	At least 1	Simple Layouts write data in stripes across the Vdisk, they do not provide fault tolerance but do offer improved read/write performance
Mirror	2 (for 2 way mirror) or 5 (for 3 way mirror)	Mirror layouts offer fault tolerance, with a 2way mirror we can lose 1 disk and still continue to read and write data with a 3way mirror we can lose 2 disks and still read and write data With a Mirror layout we lose 50% of disk space to Mirror data.
Parity	At least 3	Parity offer fault tolerance by writing data in strips across the vdisk, for each stripe a parity block is written that can be used to reconstruct data in the event that we lose 1 disk. We cannot afford to lose more than 1 disk if we do then we lose access to the entire volume. With Parity layouts we lose the equivalent of 1 disk to parity information.

Order for Creating Storage Spaces

1) Create a Storage pool from Physical Disks
2) Create Virtual Disk (storage space) setting Layout and Provisioning options
3) Create volume including formatting, drive letter etc.

Day 2 Fill in the Blanks

1. When installing the DHCP role you are asked to perform additional configuration tasks, two DHCP admin groups will be created the first is the ____________ group and the second is the ____________ group. The second tasks is to _____________ the DHCP server, if it is not __________ then the DHCP Server will not respond to client requests for IP Addresses.
2. If the DHCP Server is not authorized you would expect to see an _______ icon when using the DHCP Management console, if the DHCP Service was stopped you would expect to see a _______ icon when using the DHCP Management Console.
3. If you want to reserve and IP Address for an IPv4 client you would use the client's __________. If you want to reserve an IP Address for an IPv6 client you would use the client's ________ and ______.
4. If you want to prevent a client from obtaining an IP Address from your DHCP Server you could create a DHCP _________ on your DHCP server.
5. Once you have installed a DNS server you can then add Zones to make your DNS Server Authoritative for a particular name space, so if you wanted your DNS Server to be Authoritative for the FB.COM you could add a __________ Zone or a __________ Zone or and _________ Zone.

6. If you want to create a new zone by using PowerShell you could use the _______________ CMDlet
7. If you create an _________ Zone you can set its replication scope so it is replicated to only the DC’s that contain that application partition, there are two default application partitions they are the _____________ and the _________
8. If you want your DNS Server to resolve names that it is not Authoritative for you can add a_________ or ________ or use __________ to connect your DNS server to the outside world.
9. In order to create storage spaces you need to create _______ and _______ and _______.
10. When choosing layout options for your storage spaces you can choose ________ layouts that require 1 or more disks, or __________ layouts that require 2 or 5 disks or you can create ________ layouts that require 3 or 7 disks.

Day 2 Additional Labs

The Additional Labs should be done as much as possible without referring to the Official curriculum material (Skillpipe material)

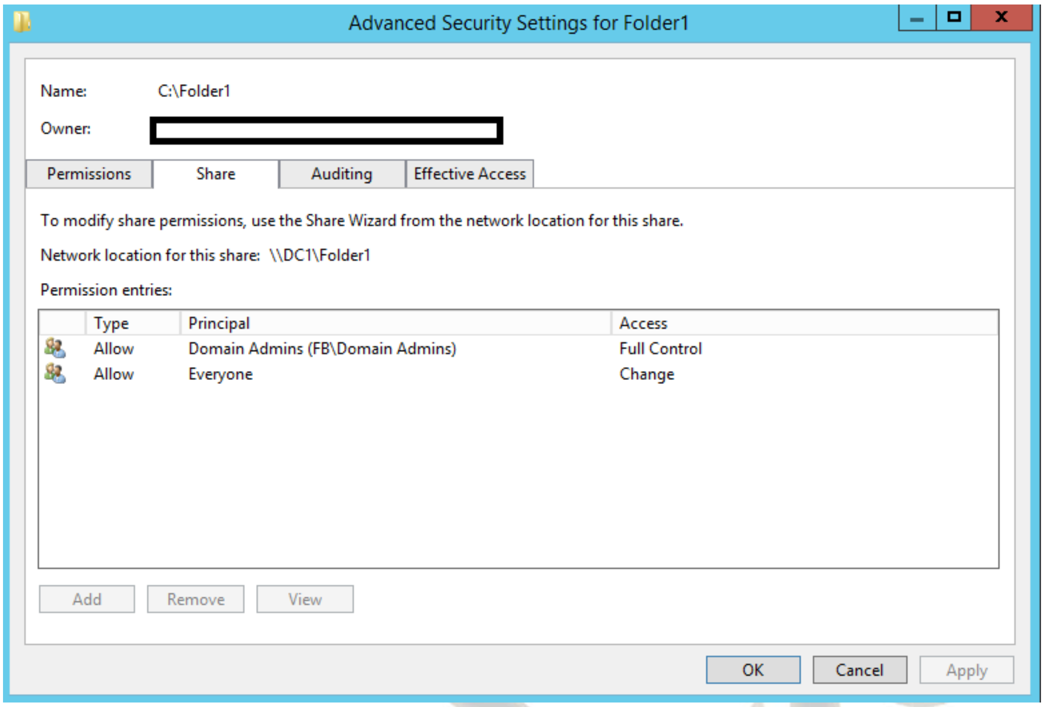
1) Start Virtual Machines DC1 and DC2
2) Login in to both DC1 and DC2 using the username Administrator and the Password Pa$$w0rd
3) Using PowerShell install the DHCP feature on to DC2, make sure the DHCP server is authorised
4) Add a new DHCP Scope to DC2 for the 10.0.0.0/24 network excluding the addresses from 10.0.0.1 to 10.0.0.100 and 10.0.0.150 – 10.0.0.200
5) Disable the DHCP service on DC1 if it is running and then test your DHCP server by starting FBWSK1 and configuring it to obtain an IP Address automatically.
6) DC1 is a DNS server and holds an ADI Zone for FB.com domain, using only PowerShell install the DNS feature on DC2 and add an ADI zone appears there.
7) On DC1 and only using PowerShell configure a Primary Zone for Widgets.com
8) On DC2 and only using PowerShell and a Secondary Zone for Widgets.com

DAY 3

Go through these examples on your own and we will check your results during our review session.

Share and NTFS Example 1

Share Permission for folder1



Advanced Security Settings for Folder1

Name: C:\Folder1

Owner: [redacted]

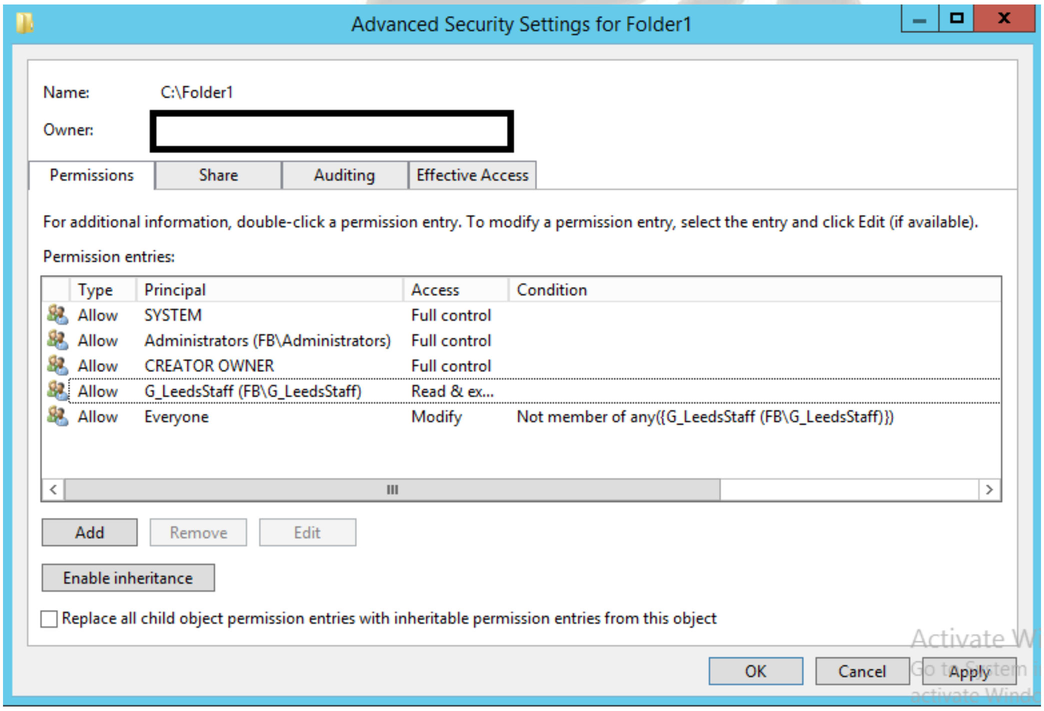
To modify share permissions, use the Share Wizard from the network location for this share.

Network location for this share: \\DC1\Folder1

Permission entries:

Type	Principal	Access
Allow	Domain Admins (FB\Domain Admins)	Full Control
Allow	Everyone	Change

NTFS Permissions for Folder1



Advanced Security Settings for Folder1

Name: C:\Folder1

Owner: [redacted]

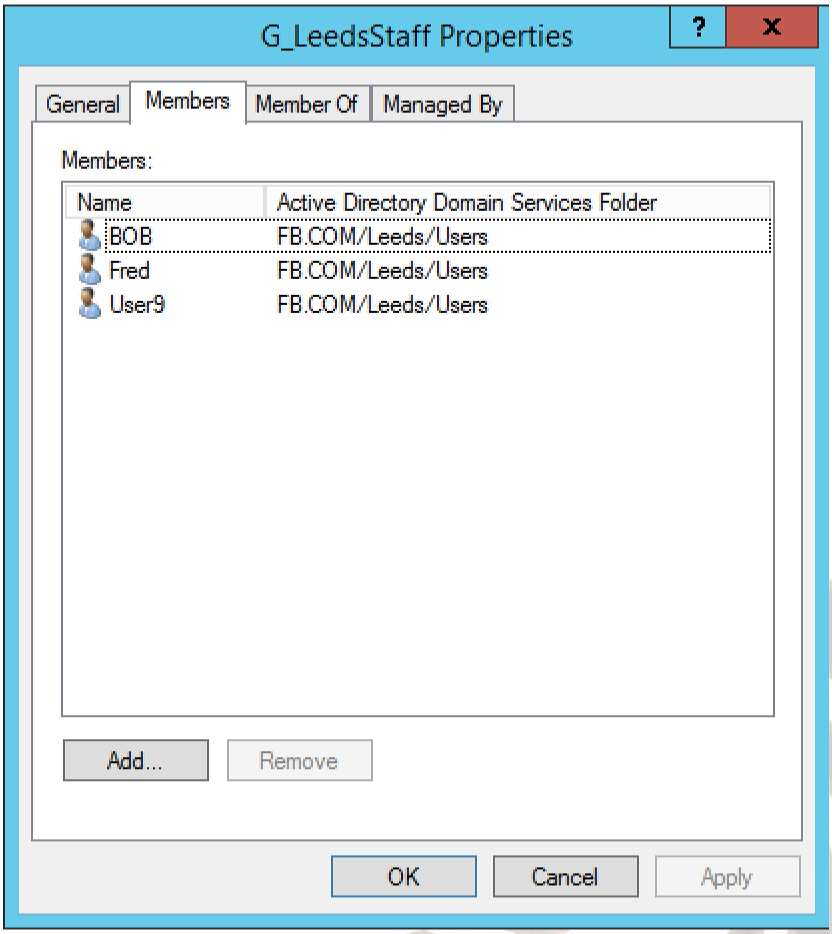
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Condition
Allow	SYSTEM	Full control	
Allow	Administrators (FB\Administrators)	Full control	
Allow	CREATOR OWNER	Full control	
Allow	G_LeedsStaff (FB\G_LeedsStaff)	Read & ex...	
Allow	Everyone	Modify	Not member of any({G_LeedsStaff (FB\G_LeedsStaff)})

□ Replace all child object permission entries with inheritable permission entries from this object

G_LeedStaff Group Membership



G_LeedsStaff Properties

Members:

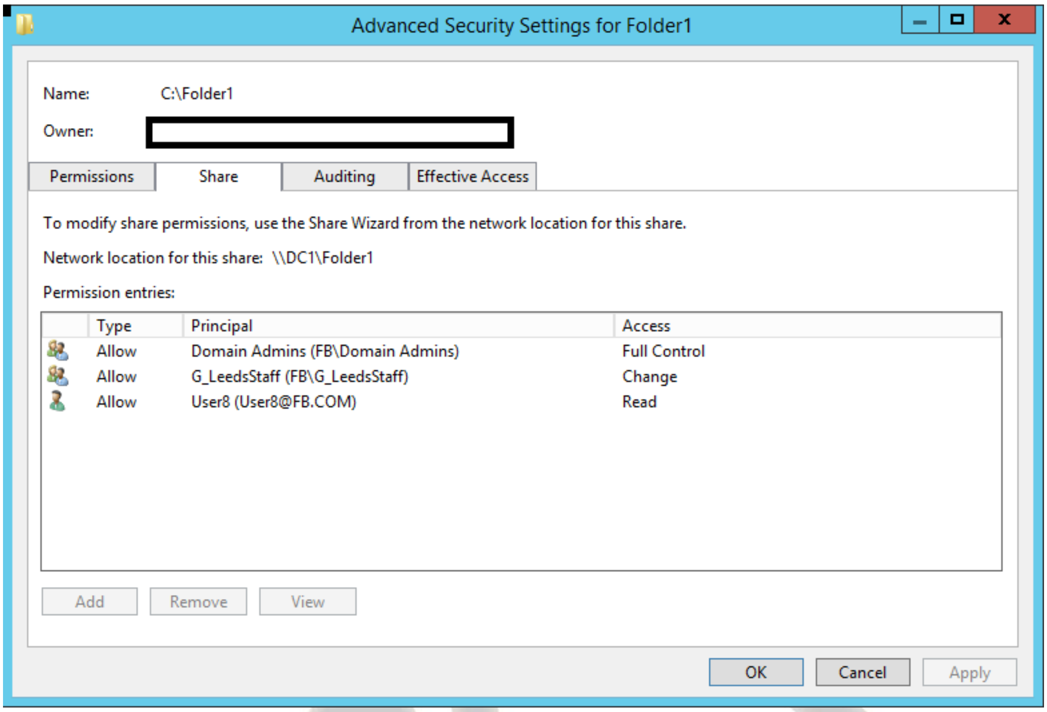
Name	Active Directory Domain Services Folder
BOB	FB.COM/Leeds/Users
Fred	FB.COM/Leeds/Users
User9	FB.COM/Leeds/Users

Based on the information above which of the Following statement are true?

1. FB\Bob will be able to delete file in Folder1
2. FB\User8 will be able to delete file in Folder1
3. FB\Administrator will be able to delete file in Folder1

Share and NTFS Example 2

Share Permission for folder 1



Advanced Security Settings for Folder1

Name: C:\Folder1

Owner: [redacted]

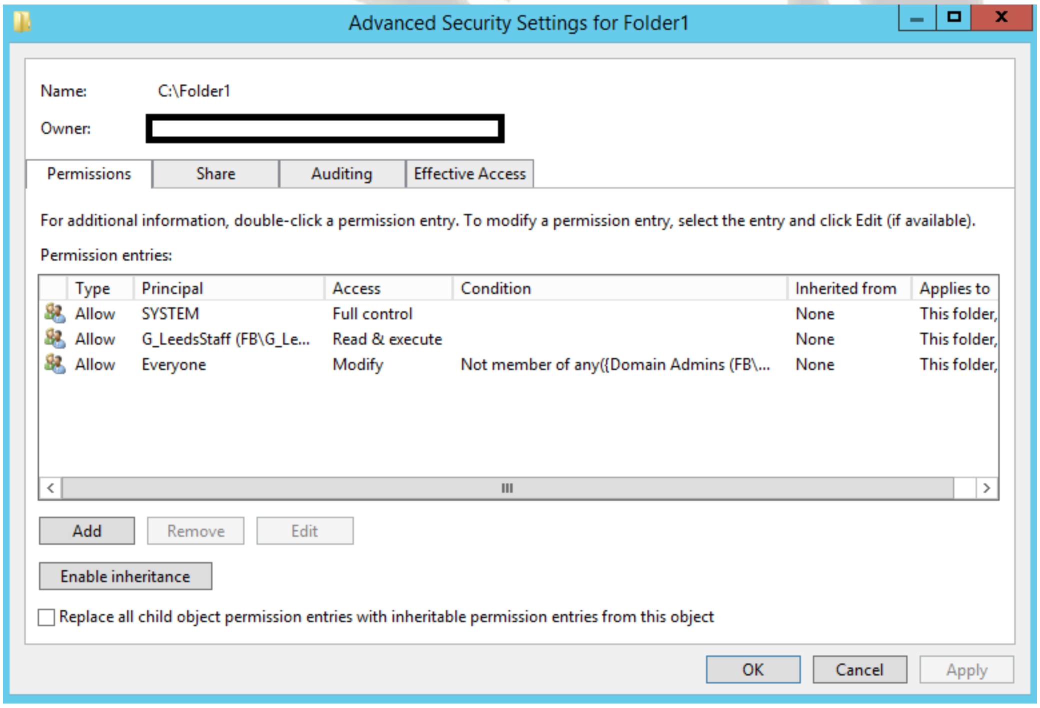
To modify share permissions, use the Share Wizard from the network location for this share.

Network location for this share: \\DC1\Folder1

Permission entries:

Type	Principal	Access
Allow	Domain Admins (FB\Domain Admins)	Full Control
Allow	G_LeedsStaff (FB\G_LeedsStaff)	Change
Allow	User8 (User8@FB.COM)	Read

NTFS Permissions for Folder 1



Advanced Security Settings for Folder1

Name: C:\Folder1

Owner: [redacted]

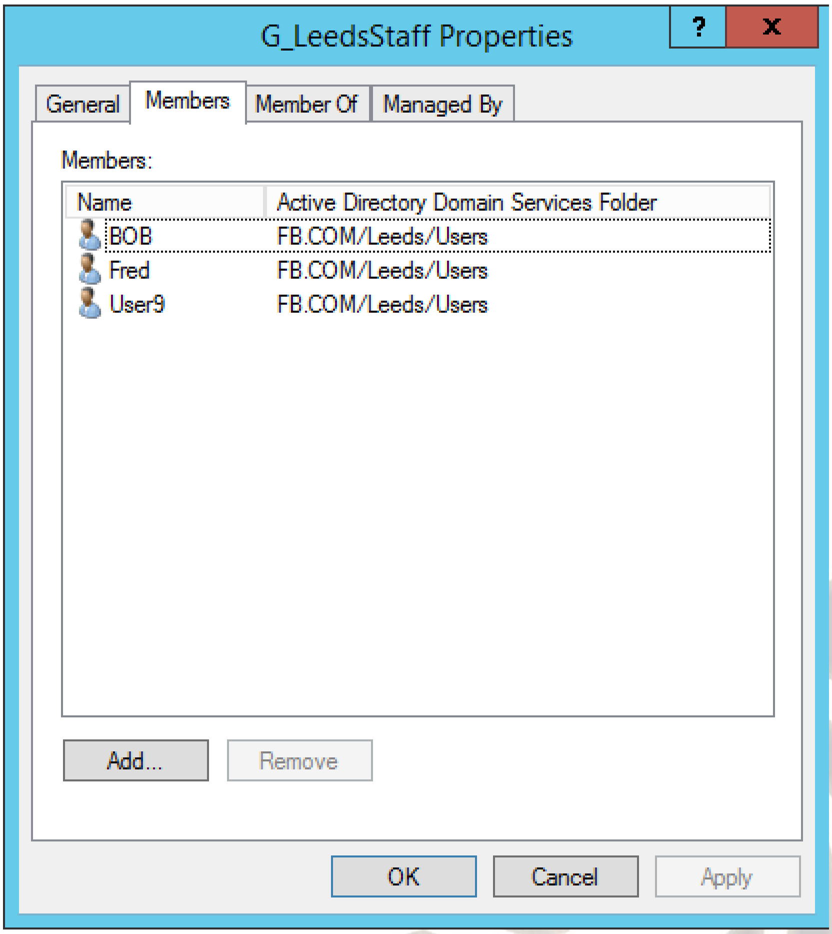
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Condition	Inherited from	Applies to
Allow	SYSTEM	Full control		None	This folder,
Allow	G_LeedsStaff (FB\G_Le...	Read & execute		None	This folder,
Allow	Everyone	Modify	Not member of any({Domain Admins (FB\...	None	This folder,

□ Replace all child object permission entries with inheritable permission entries from this object

G_LeedStaff Group Membership



Members:

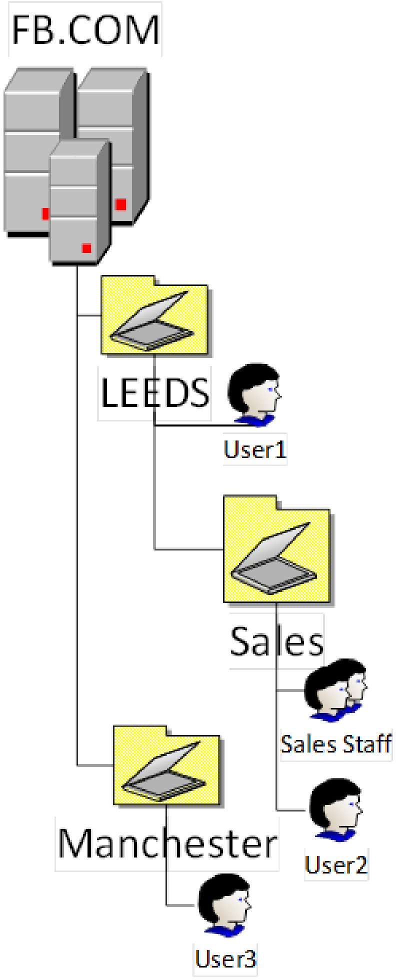
Name	Active Directory Domain Services Folder
BOB	FB.COM/Leeds/Users
Fred	FB.COM/Leeds/Users
User9	FB.COM/Leeds/Users

Based on the information above which of the Following statement are true?

1. FB\Bob will be able to delete file in Folder1
2. FB\User8 will be able to delete file in Folder1
3. FB\Administrator will be able to delete file in Folder1

GPO Example 1

Domain and OU structure



You are the Administrator for the FB.COM domain and it is your job to manage Group Policy Objects. You have been asked to provide information on some of your existing Group Policies that are already linked to your domain and OU's.

User Information

User	**OU**	**Group Membership**
User1	Leeds	Standard groups plus Sales Staff Group
User2	Sales	Standard groups
User3	Manchester	Standard groups

GPO Information

GPO	Where is GPO Linked	Filtering Options
GPO1	Linked to Domain Level and Sales OU	User 2 Denied Read
GPO2	Linked to Leeds OU	–
GPO3	Linked to Sales OU	–

Other Information

1. An Administrator has Blocked Inheritance at the Sales OU Level
2. GPO1 is Enforced

Questions

1. Which GPOs apply to User1 and in what Order are they processed?

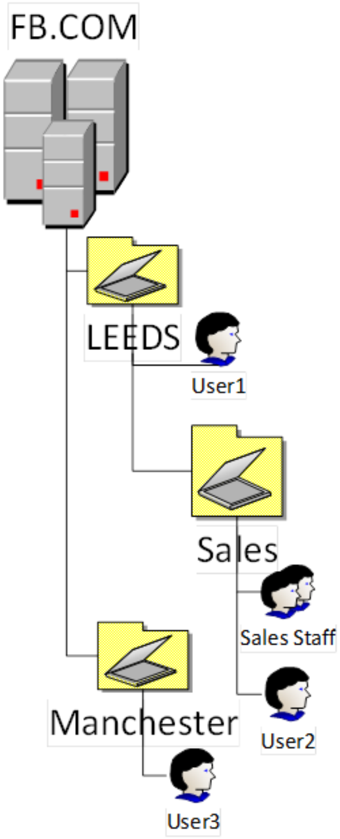
2. Which GPOs apply to User2 and in what Order are they processed?

3. Which GPOs apply to User3 and in what Order are they processed?

4. If we move User3's account to the Sales OU which GPO's would apply and in what order would they be processed?

GPO Example 2

Domain and OU structure



You are the Administrator for the FB.COM domain and it is your job to manage Group Policy Objects. You have been asked to provide information on some of your existing Group Policies that are already linked to your domain and OU's.

User Information

User	OU	Group Membership
User1	Leeds	Standard groups plus Sales Staff Group
User2	Sales	Standard groups
User3	Manchester	Standard groups

GPO Information

GPO	Where is GPO Linked	Filtering Options
GPO1	Linked to Domain Level and Sales OU	Sales Staff Group Denied Read and Denied Apply
GPO2	Linked to Leeds OU	–
GPO3	Linked to Sales OU	–

Other Information

1. An Administrator has Blocked Inheritance at the Manchester OU Level
2. GPO2 is Enforced

Questions

1) Which GPOs apply to User1 and in what Order are they processed?

2) Which GPOs apply to User2 and in what Order are they processed?

3) Which GPOs apply to User3 and in what Order are they processed?

4) If we move User3's account to the Sales OU which GPO's would apply and in what Order would they be processed

GPO CMDLets

Backup-GPO	Backs up one GPO or all the GPOs in a domain.
Copy-GPO	Copies a GPO
Import-GPO	Imports the Group Policy settings from a backed-up GPO into a specified GPO
Invoke-GPUPDATE	Updates Group Policy on a local computer or remote computer.
New-GPLink	Links a GPO to a site, domain, or OU.
New-GPO	Used to create a new GPO
Set-GPInheritance	Blocks or unblocks inheritance for a specified domain or OU
Set-GPPermission	Grants a level of permissions to a security principal for one GPO or for all the GPOs in a domain
Set-GPLink	Sets the properties of the specified GPO link

Printer Scheduling Video

This Video looks at Printer Scheduling

[Printer Scheduling]

Or

https://www.youtube.com/watch?v=zynOtA9XcFQ&list=PL2QNrvCUc_M9ZpX3LRDdPojvlfL99aY10&index=1

Work Folders

For a description of what work folders are and how they are configured please follow this link

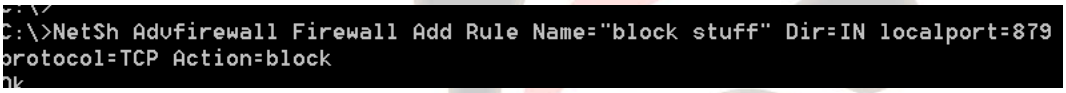
http://mgbleeds.co.uk/2014/06/14/windows-server-2012-r2-work-folders/

Configuring Windows Advanced Firewall with NETSH and PowerShell

NetSh advfirewall is a command line tool for administering Windows firewall and Advanced Security

To configure a firewall rule with NetSH

NetSh Advfirewall Firewall Add Rule name=*rulename* dir=*In/out* –localport=*Portnumber* localprotocol=*protocol* Action=*Allow/Block*

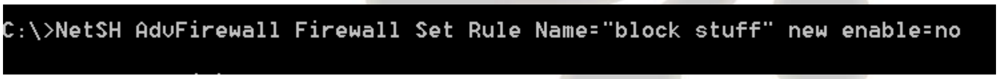


```
C:\>NetSh Advfirewall Firewall Add Rule Name="block stuff" Dir=IN localport=879
protocol=TCP Action=block
```

This example adds an inbound firewall rule to block an application called “Block Stuff” that uses TCP port 879

To Update and existing Firewall Rule with Netsh

Netsh AdvFirewall Firewall Set Rule Name=*rulename* new enable=*yes/no*

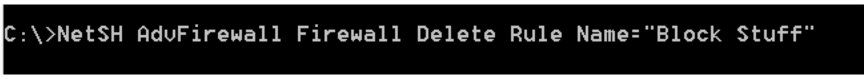


```
C:\>NetSH AdvFirewall Firewall Set Rule Name="block stuff" new enable=no
```

This command changes the state of a firewall rule state from enabled to disabled, use the SET command to make changes to an existing rule.

To Delete a Firewall Rule using Netsh

NetSH AdvFirewall Firewall Delete Rule Name=*rulename*

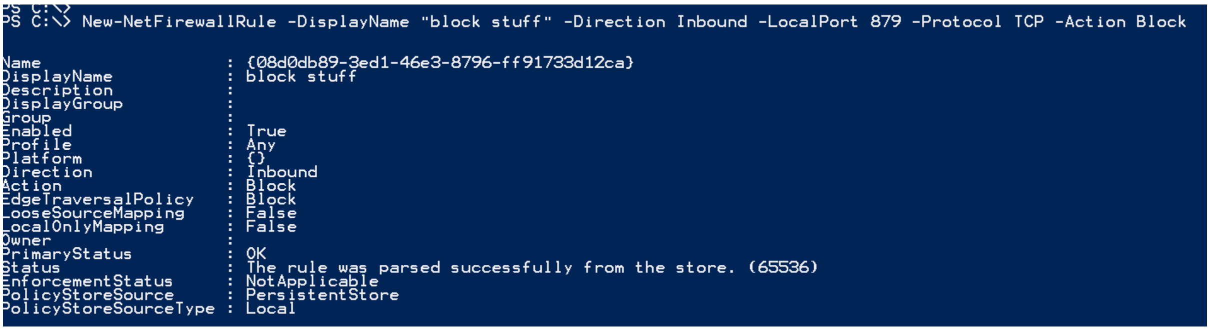


```
C:\>NetSH AdvFirewall Firewall Delete Rule Name="Block Stuff"
```

This command deletes a firewall rule by using the Delete command and specifying the name of the rule.

To configure a firewall rule with PowerShell

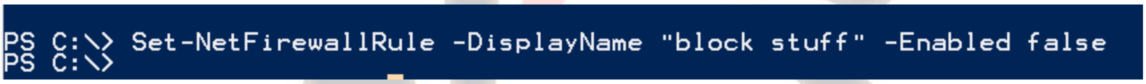
New-NetFirewallRule –displayname *displayname* –Direction *outbound/inbound* –Localport *localport* –Protocol *protocol* –Action *Block/Allow*



```
PS C:\>
PS C:\> New-NetFirewallRule -DisplayName "block stuff" -Direction Inbound -LocalPort 879 -Protocol TCP -Action Block

Name                      : {08d0db89-3ed1-46e3-8796-ff91733d12ca}
DisplayName               : block stuff
Description               :
DisplayGroup              :
Group                     :
Enabled                   : True
Profile                   : Any
Platform                  : {}
Direction                 : Inbound
Action                    : Block
EdgeTraversalPolicy       : Block
LooseSourceMapping        : False
LocalOnlyMapping          : False
Owner                     :
PrimaryStatus             : OK
Status                    : The rule was parsed successfully from the store. (65536)
EnforcementStatus         : NotApplicable
PolicyStoreSource         : PersistentStore
PolicyStoreSourceType     : Local
```

To Update and existing Firewall Rule with PowerShell

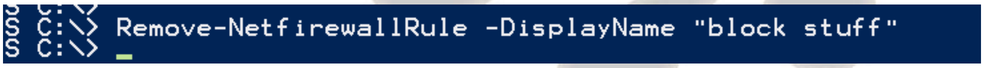
Set-NetFirewallRule –DisplayName *displayname* –Enabled *true/false*



```
PS C:\> Set-NetFirewallRule -DisplayName "block stuff" -Enabled false
PS C:\>
```

Use the Set-NetFirewallRule to make changes to an existing firewall rule, in this example we have changed a rule from enabled (true) to disabled (false)
To Delete a Firewall Rule using PowerShell

Remove-NetfirewallRule –Displayname *displayname*



```
PS C:\>
PS C:\> Remove-NetfirewallRule -DisplayName "block stuff"
PS C:\> _
```

Use the Remove-NetFirewallRule to remove an existing firewall rule by specifying its display name.

Day 3 Fill in the Blanks

1. Before creating virtual machines in Hyper-V there are several building blocks that you should consider creating first. One of the building blocks to consider is virtual machine networking, with Hyper-V on Windows Server 2012 R2 we can create three types of virtual switch, these are _________, ________ and _________ virtual switches.
2. If you want your virtual machine to connect directly to the datacentre network you would create a _____________ virtual switch which is bound to a Network Interface card. Remember that if you create a virtual switch as one type it can be converted at any time to another type of switch.
3. When choosing storage for you virtual machines you can use physical disks or virtual disks, we call the physical disks __________ disks but in order to use them they must

be _________ to the physical machine. If you choose to use virtual disks you have a choice of _______ disks, _______ disks or _______ disks.

4. When you connect a virtual machine to a virtual switch all network traffic from the VM is sent through that switch, if you want to send traffic direct from the VM to the NIC you can as long as you enable _________ on both the Virtual Switch and the VM. In order for this to work you will have to install the drivers for the NIC inside the VM and remember in order to enable ________ on the virtual switch you have to do it when you create the switch, you cannot enable it afterwards without removing and recreating the virtual switch. Also ______ breaks physical NIC teaming.
5. Integration services are offered by the Host server to the virtual machines, integration services include _________, __________, ________ and _________.
6. When we use a Generation 1 virtual machines we need to use a ____________ in order to perform PXE Boot, it is important to place the _________ at the top of the BIOS boot order. When we use Generation 2 virtual machines we can use a ____________ in order to perform PXE Boot, it is important to place the ____________ at the top of the firmware boot order.
7. You can measure the average amount of Processor, Memory, Disk and network resources a VM is using by enabling ___________. To do this you need to run the ____________ CMDLet first and to view the results you can run the ______________ CMDLet.
8. For each VM you can set Advanced Features of the Network Interface Cards, these include DHCP Guard, Router Guard as well as _________, _________ and _______.
9. MAC Address spoofing can be enabled on a VM by VM basis, this enables a VM to use multiple MAC Addresses. One feature that will require MAC Address spoofing is ___________.

Day 3 Additional Labs

The Additional Labs should be done as much as possible without referring to the Official curriculum material (Skillpipe material)

1) Start Virtual Machines DC1 and DC2 and WKS1
2) Login in to both DC1 and DC2 and WKS1 using the username Administrator and the Password Pa$$w0rd
3) Create a folder on drive C: on DC2 called Public
4) Using PowerShell create a share called Public using c:\public .
5) Grant User1 and User2 full control access to the Public share
6) Login to WKS1 as User1 and test access to the Public Share
7) Using PowerShell create a GPO called NoControlPanel link the GPO to the Leeds OU.
8) Edit the GPO to deny access to Control Panel

9) Make sure User1 is in the Leeds OU then login to WKS1 as User1 and make sure that User1 cannot access control panel.
10) Make sure User2 is in the Leeds OU, makes sure that the NoControlPanel GPO does not affect user 2. Login to WKS1 as User2 and sure that user2 can access control panel.

70-410 Additional Material

Azure Information for the MCSA Windows Server Exams

Microsoft Azure is a huge platform, it is impossible to detail it all in a single book. In this book we will be concentrating on Azure Infrastructure as a Service (IAAS) components. There are plenty of resources that explain the differences between the different cloud computing models. Microsoft Azure allows you to build both IAAS and PAAS resources, at the end of this book we will be providing an overview of Azure PAAS components and links to where you can find more information. For the rest of this book if we are talking about an Azure feature it is a future used to create an IAAS solution.

The first thing you need to do is sign up for an Azure trial subscription, don't use your work or MSDN subscription while you are learning Azure just in case you make a mistake. You can sign up for a trial Azure subscription be going to http://Azure.Micorosoft.com

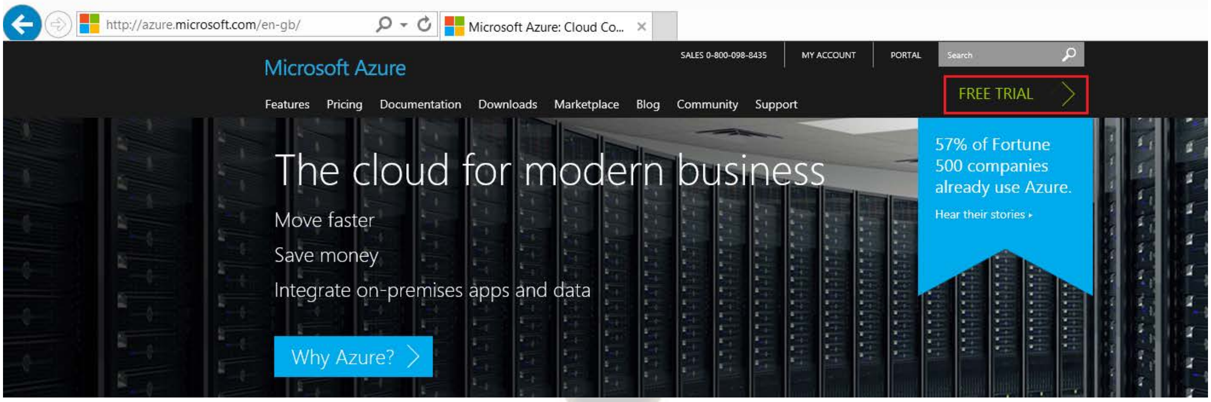


Fig 1.1

Follow the FREE TRIAL link, you will need an Email address and credit / debit card to setup the trial. It should take no more than 10 or 15 minutes to setup your trial and you will have access to it for 30 days or until you spend the free money Microsoft associates with your account. Once the trial has been created you can then begin your Azure journey.

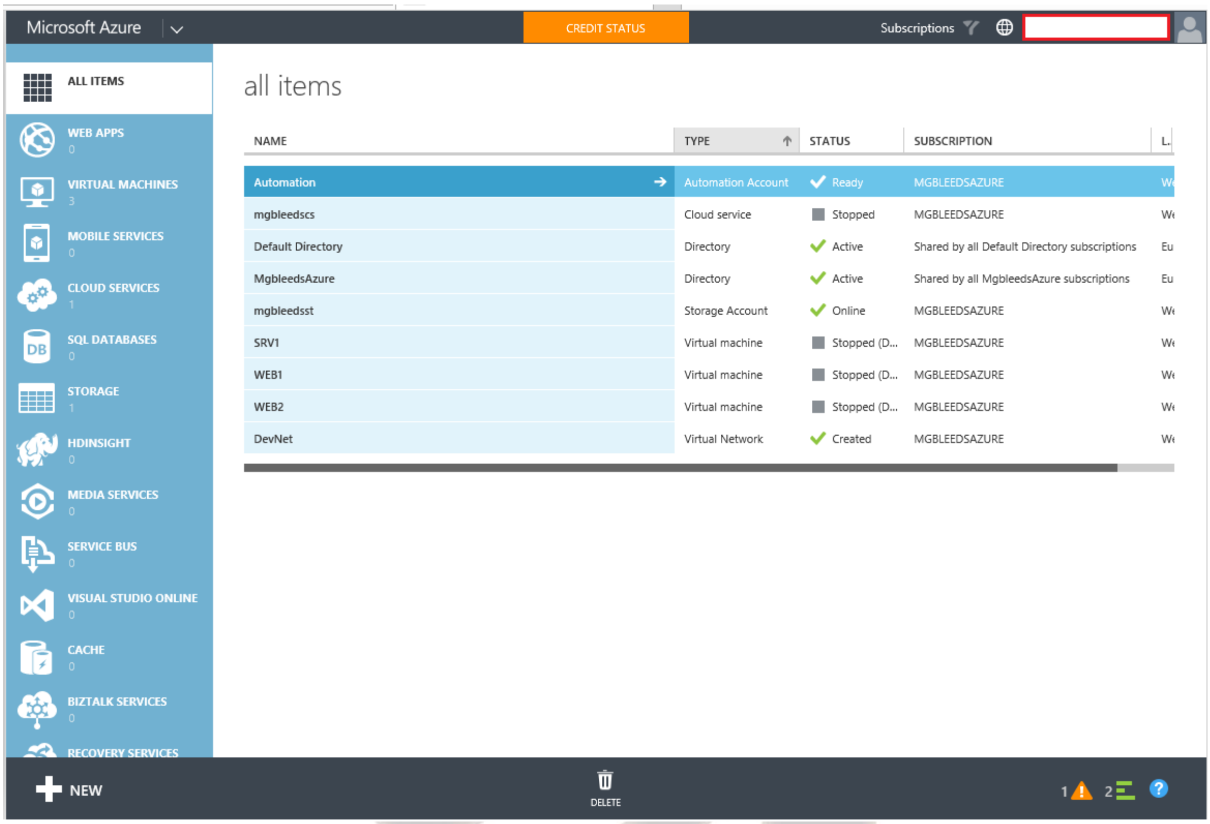
Managing Azure is primarily done using one of the two management portals or by using a command line tool such as PowerShell of the Azure Cross-Platform command line utility.

Managing Microsoft Azure using the Portal

At the time of writing there are two management portals for you to use. The first is the Azure portal and the second is Azure Preview portal. All features are available through the Azure portal but Microsoft are committed to developing the Preview Portal for all future features. The Preview Portal has been in preview for quite some time and does make some nice management features available but when you are first learning a feature it will probably be easier to learn using the azure portal first and then trying the feature in the preview portal.

To access the azure portal use the following URL http://manage.windowsazure.com

Once there, sign in with the email address you used to create your trial subscription and you will be logged in to the Azure Portal.



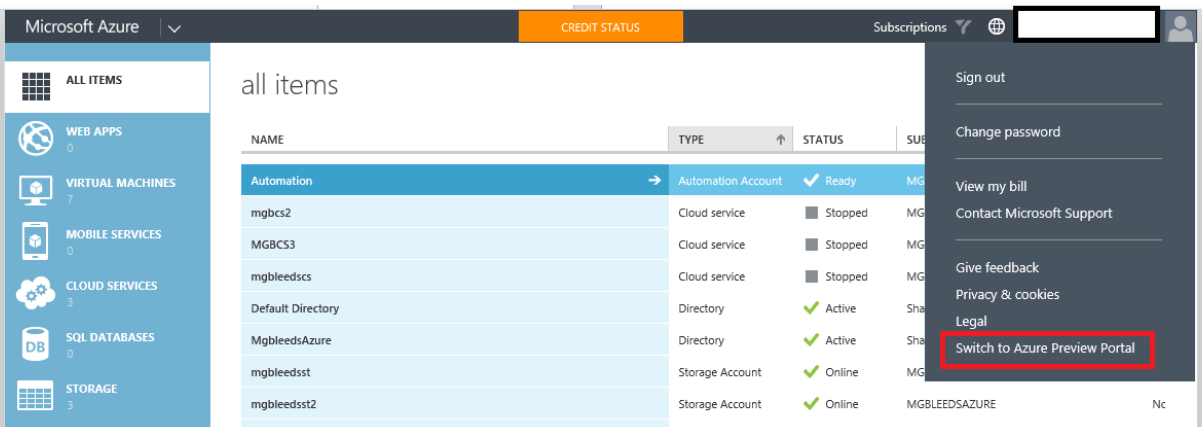
all items

NAME	TYPE	STATUS	SUBSCRIPTION	L.
Automation	Automation Account	✓ Ready	MGBLEEDSAZURE	W
mgbleedscs	Cloud service	■ Stopped	MGBLEEDSAZURE	W
Default Directory	Directory	✓ Active	Shared by all Default Directory subscriptions	Eu
MgbleedsAzure	Directory	✓ Active	Shared by all MgbleedsAzure subscriptions	Eu
mgbleedsst	Storage Account	✓ Online	MGBLEEDSAZURE	W
SRV1	Virtual machine	■ Stopped (D...	MGBLEEDSAZURE	W
WEB1	Virtual machine	■ Stopped (D...	MGBLEEDSAZURE	W
WEB2	Virtual machine	■ Stopped (D...	MGBLEEDSAZURE	W
DevNet	Virtual Network	✓ Created	MGBLEEDSAZURE	W

Fig 1.2

When you login to the Azure Portal you will be on ALL ITEMS, this node shows you all the items currently configured in your subscription. Unlike mine your subscription will probably only have a Default Directory listed.

To Access the preview portal you can use the following URL http://portal.azure.com or if you are already logged in to the Azure Portal click on your email address and from the bottom of the list that appears you can select **Switch to Azure Preview Portal**



NAME	TYPE	STATUS	SUB
Automation	Automation Account	✓ Ready	MG
mgbcs2	Cloud service	■ Stopped	MG
MGBCS3	Cloud service	■ Stopped	MG
mgbleedscs	Cloud service	■ Stopped	MG
Default Directory	Directory	✓ Active	Sha
MgbleedsAzure	Directory	✓ Active	Sha
mgbleedsst	Storage Account	✓ Online	MG
mgbleedsst2	Storage Account	✓ Online	MGBLEEDSAZURE Nc

Fig 1.3

As stated previously all new features will be available through the Preview Portal but it is worth noting that not all old features are available through there. So if you are looking for a feature in the preview port and can't find it then flip back to the Azure Portal.

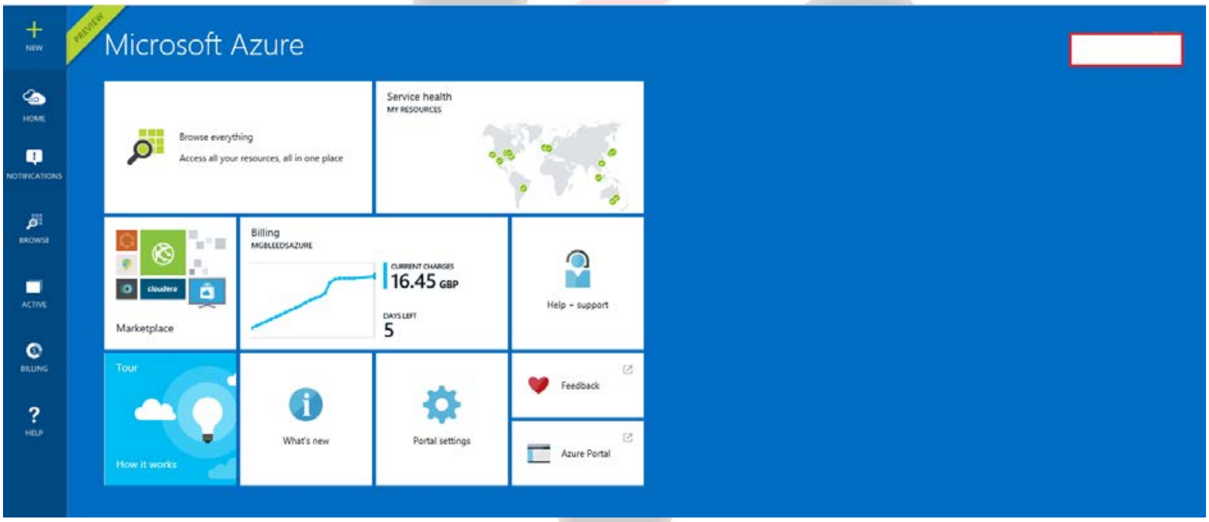


Fig 1.4

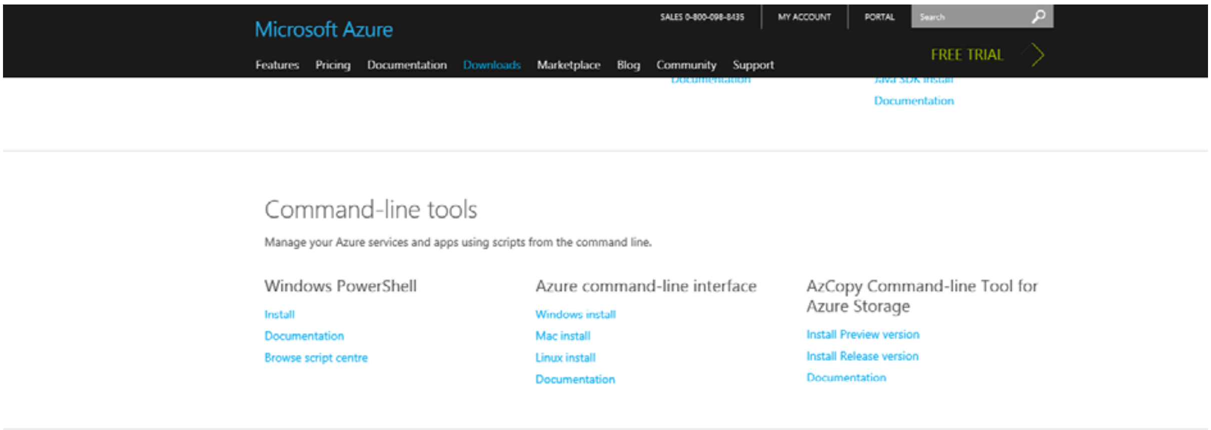
When you use the Preview Portal you first access the dashboard, the dashboard is customisable and shows useful information about your subscription and the Azure service. The Service health in particular you will find useful when fielding support calls.

We will navigate around the two different portals as we go through the rest of the chapters in this book, for now have a click around and familiarise yourself with the interfaces. Notice as you select items in the Azure Portal the detail pain changes to show you the feature you have selected and when you navigate around the Preview Portal 'blades' appear showing the details you have selected to view.

Managing Microsoft Azure using PowerShell

Although your day to day administration will be performed through the two portals bulk tasks, repetitive tasks and administration of individual virtual machines and services can be done thorough PowerShell.

The first thing you will need to do is download the latest Azure PowerShell module. If you go to http://azure.microsoft.com you can select Downloads from the menu bar then scroll towards the bottom of the download section and you will see a command-line tools section



Command-line tools

Manage your Azure services and apps using scripts from the command line.

Windows PowerShell

- Install
- Documentation
- Browse script centre

Azure command-line interface

- Windows install
- Mac install
- Linux install
- Documentation

AzCopy Command-line Tool for Azure Storage

- Install Preview version
- Install Release version
- Documentation

Fig 1.5

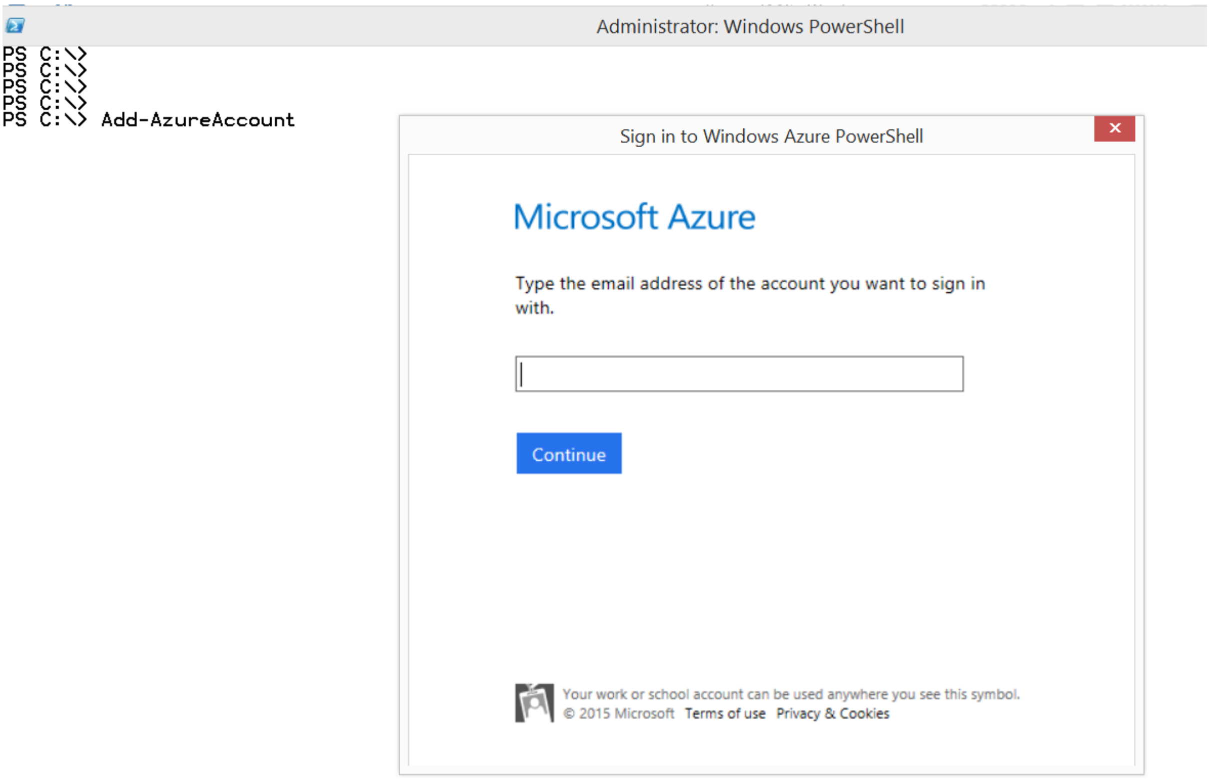
From here you can choose to Install Windows PowerShell. After the install you should have a new Microsoft Azure PowerShell tool installed. Now you have installed the Azure PowerShell module you have access to all the Azure PowerShell CMDLets but you won't be able to use them until you connect and authenticate PowerShell to your Azure subscription. There are two ways to do this. The first uses a PowerShell CMDLet call **Add-AzureAccount** and the second used the CMDLet **Get-AzurePublishSettingFile**

Add-AzureAccount

In order to use the Add-AzureAccount CMDLet you will need to download and install the **Microsoft Online Services Sign-in Assistant** application first. Make sure you download the latest version.

1) Open Microsoft Azure PowerShell
2) Type Add-AzureAccount

You should see a sign in screen appear like the one in Fig 1.6



Administrator: Windows PowerShell

```
PS C:\>
PS C:\>
PS C:\>
PS C:\>
PS C:\> Add-AzureAccount
```

Sign in to Windows Azure PowerShell
Microsoft Azure

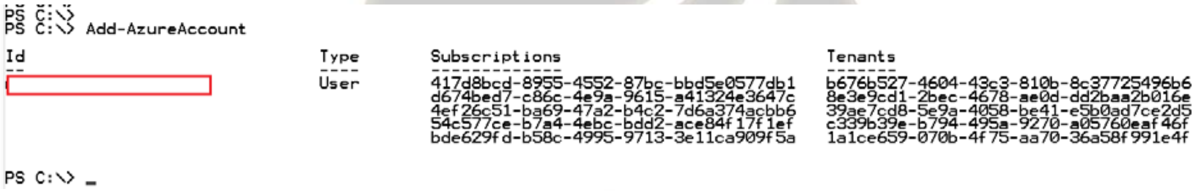
Type the email address of the account you want to sign in with.

Continue
Your work or school account can be used anywhere you see this symbol.
© 2015 Microsoft Terms of use Privacy & Cookies

Fig 1.6

3) Sign in using the Email address you used when creating you Azure subscription

After a short delay you should be connected to you Azure subscription and see a screen similar to the one in fig 1.7



```
PS C:\>
PS C:\> Add-AzureAccount

Id                              Type      Subscriptions                            Tenants
--                              ----      -------------                            -------
[redacted]                      User      417d8bcd-8955-4552-87bc-bbd5e0577db1     b676b527-4604-43c3-810b-8c37725496b6
                                          d674bed7-c86c-4e9a-9615-a41324e3647c     8e3e9cd1-2bec-4678-ae0d-dd2baa2b016e
                                          4ef26c51-ba69-47a2-b4c2-7d6a374acbb6     39ae7cd8-5e9a-4058-be41-e5b0ad7ce2d5
                                          54c577ce-b7a4-4ebc-bdd2-ace84f17f1ef     c339b39e-b794-495a-9270-a05760eaf46f
                                          bde629fd-b58c-4995-9713-3e11ca909f5a     1a1ce659-070b-4f75-aa70-36a58f991e4f

PS C:\> _
```

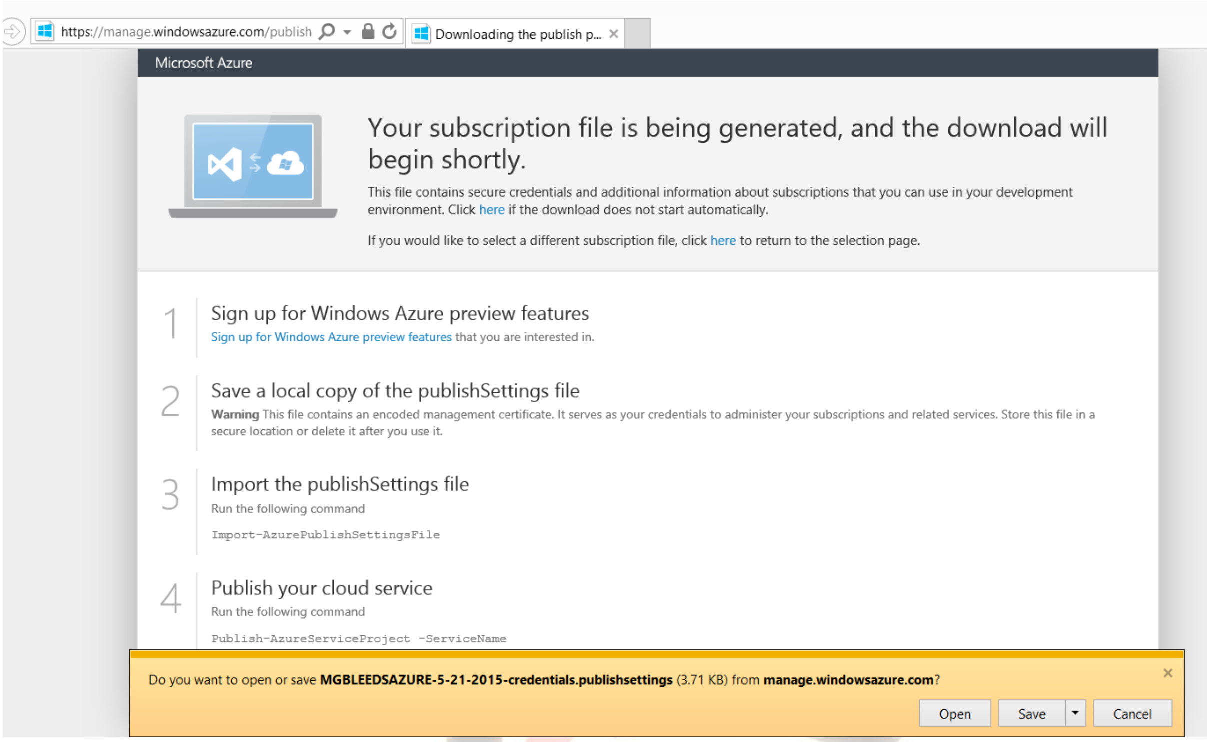
Fig 1.7

You are now connected to your Azure Subscription, (the reason I see multiple subscriptions is because my email account is associated to four different subscription)

Get-AzurePublishSettingFile

1) Open Microsoft Azure PowerShell
2) Type **Get-AzurePublishSettingFile**

This time Internet Explorer (or another browser) should open up and give you the option to login using the email address you used when you created your Azure Trial account.



https://manage.windowsazure.com/publish
Downloading the publish p...
Microsoft Azure

Your subscription file is being generated, and the download will begin shortly.

This file contains secure credentials and additional information about subscriptions that you can use in your development environment. Click here if the download does not start automatically.

If you would like to select a different subscription file, click here to return to the selection page.

1 Sign up for Windows Azure preview features

Sign up for Windows Azure preview features that you are interested in.

2 Save a local copy of the publishSettings file

Warning This file contains an encoded management certificate. It serves as your credentials to administer your subscriptions and related services. Store this file in a secure location or delete it after you use it.

3 Import the publishSettings file

Run the following command

```
Import-AzurePublishSettingsFile
```

4 Publish your cloud service

Run the following command

```
Publish-AzureServiceProject -ServiceName
```

Do you want to open or save **MGBLEEDSAZURE-5-21-2015-credentials.publishsettings** (3.71 KB) from **manage.windowsazure.com**?

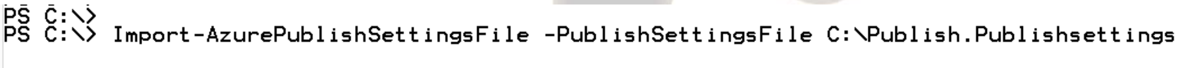
Fig 1.8

Once you have authenticated a Subscription Setting file will be generated and you will be given an option to download you .Publishsettings file. Make sure you save your file with a meaningful name,

Once saved go back to Azure PowerShell and type

3) **Import-AzurePublishSettingsFile –PublishSettingsFile *FilePath***

Fig 1.9 shows an example of this.



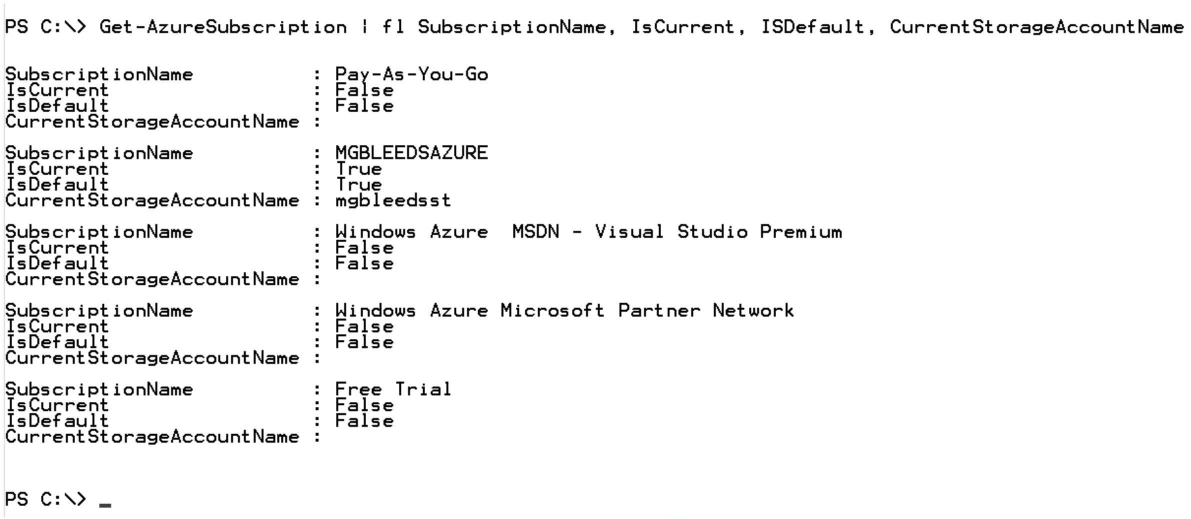
```
PS C:\>
PS C:\> Import-AzurePublishSettingsFile -PublishSettingsFile C:\Publish.Publishsettings
```

Fig 1.9

Once you have run the import you are now connected to your azure subscription but there might be a couple more tasks you need to perform before you start issuing command.

Firstly if you have multiple subscriptions associated with your Email address then you will probably want to choose which subscription is your default subscription so that when you type in Azure PowerShell commands you don’t have specify the subscription name each time.

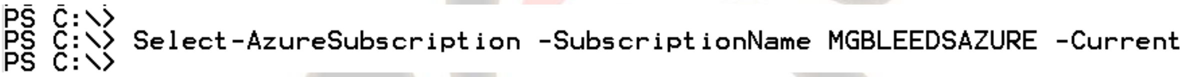
To do this first use the **Get-AzureSubscription** CMDLet to get a list of the subscriptions you are now connected to, then use the **Select-AzureSubscription** CMDLet to choose which is your default. Figs T1.10 and T1.11 shows these commands.



```
PS C:\> Get-AzureSubscription | fl SubscriptionName, IsCurrent, ISDefault, CurrentStorageAccountName

SubscriptionName          : Pay-As-You-Go
IsCurrent                 : False
IsDefault                 : False
CurrentStorageAccountName :

SubscriptionName          : MGBLEEDSAZURE
IsCurrent                 : True
IsDefault                 : True
CurrentStorageAccountName : mgbleedsst

SubscriptionName          : Windows Azure  MSDN - Visual Studio Premium
IsCurrent                 : False
IsDefault                 : False
CurrentStorageAccountName :

SubscriptionName          : Windows Azure Microsoft Partner Network
IsCurrent                 : False
IsDefault                 : False
CurrentStorageAccountName :

SubscriptionName          : Free Trial
IsCurrent                 : False
IsDefault                 : False
CurrentStorageAccountName :


PS C:\> _
```

Fig 1.10

In Fig 1.10 we have used the **Get-AzureSubscription** CMDlet to view a list of the connected subscriptions plus some of their properties including SubscriptionName and CurrentStorageAccountName.

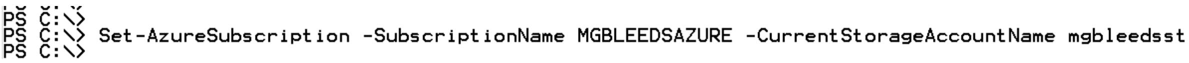


```
PS C:\>
PS C:\> Select-AzureSubscription -SubscriptionName MGBLEEDSAZURE -Current
PS C:\>
```

Fig 1.11

In Fig T1.11 we have used the **Select-AzureSubscription** CMDLet with the –SubscriptionName and –Current parameters. This command sets the named subscription as the current and default subscription so that when we run other Azure PowerShell CMDLets now they will be run against this subscription unless we specify another subscription name.

Another thing you might want to do is to set a default storage account. A storage account is used to store all your objects such as .VHD files. We will cover creating storage accounts and storage in general in chapter 2. By setting a default storage account you won’t have to specify it every time you want to create a new object. Use the **Set-AzureSubscription** CMDLet to specify the default storage account for a subscription.



```
PS C:\>
PS C:\> Set-AzureSubscription -SubscriptionName MGBLEEDSAZURE -CurrentStorageAccountName mgbleedsst
PS C:\>
```

Fig 1-12

Using one of the above methods you have now connected PowerShell to your azure subscription. In later chapters we will be using PowerShell to administer Azure.

Azure Networking

One of the fundamentals uses for Azure is creating virtual machines, one big aspect of creating virtual machines is configuring networking. Virtual machines created in Azure receive IP Address in one of two ways

1) Assigned by Microsoft

2) Assigned dynamically from a virtual network you create

IP Addresses for virtual machine in Azure are never assigned statically through network card properties they are only ever assigned dynamically.

When an IP address is assigned to your virtual machine form Microsoft pool your virtual machine will have a private IP address that will allow the virtual machine access to the internet.

If you want to connect you virtual machines to you on premise networks then you will have to plan and create your own virtual networks. This will involve defining an IP pool including DNS Server IP address.

When you create a virtual machine you will have the option of connecting it to your newly created virtual network and once the virtual machine starts it will be assigned an address from your pool. Each time the newly created VM starts it will be assigned an available address, if you want your VM to have the same IP Address from you pool every time it restarts then you need to assign a static IP address, to do this we use PowerShell and not the VMs network card properties.

The two PowerShell commands below can be used to assign a static IP Address to an Azure Virtual machine:

```
Test-AzureStaticVNetIP –VNetName "Devnet" –IPAddress "192.168.1.4"

Get-AzureVM -ServiceName "MgbleedsCS" -Name MGBSRV1 | Set-AzureStaticVNetIP -
IPAddress 192.168.1.4 | Update-AzureVM
```

The **Test-AzureStaticVNetIP** cmdlet is used to target one of your virtual networks and see if a particular IP Address is available. The second set of cmdlets get the details of an Azure VM and then using the **Set-AzureStaticVNetIP** cmdlet assigns the IP Address to the virtual machine.

Additional Tools and Additional PowerShell CMDLets

Please be aware that the following list of tools is only a guide, you should use this list as a base that you build upon. These tools are the sort of tools that you expect to see questions about in the 70-410 exam, if you would like more detailed examples of these command line tools and other then the best resources is TechNet.

Tool	Description	Brief Example / When to use
WINRS	Windows Remote Management allows you to manage and execute programs	Winrs /r:server1 Ipconfig

	remotely.	
Sconfig	The Server Configuration Tool is used to configure and manage several common aspects of server core and GUI installations	Use to configure: domain settings, computer name, network settings, local admin settings, remote management, remote desktop and date and time settings.
NetSH	Network Shell is a command line utility used to configure and display the status of various network roles and components	NetSH commands will appear in all three MCSA Exams, for this exam concentrate on examples for managing interfaces. Look at NetSH Interface commands in particular.
DISM	Deployment Image Servicing and Management tool is used to manage both offline and online images	Although DISM is primarily used to manage offline .wim images it can also be used to manage installed operating systems aswell, for example you can use DISM /Online to install windows roles and features to the current operating system.
ROUTE	ROUTE is used to manage the local routing table.	Route ADD is used to add routes to the routing table. Route Delete is used to remove routes from the routing table. Route Print is used to display the IP routing table.
CSVDE	CSVDE is a command line tool is used to import and export data from Active Directory. It uses file that store data in the CSV format. It can be used to create new objects but cannot be used to edit or delete existing objects.	CSVDE –i –f c:\filename – this is used to import the content of the CSV file into AD. Make sure you can recognise the format of a CSV file.
LDIFDE	LDIFDE is use to create,	LDIFDE –i –f c:\filename

	modify and delete objects in AD.	
REDIRCMP	Changes the default container for new computer accounts	Redircmp ou=NewOU,dc=domainname,dc=com
REDIRUSR	Changes the default container for new user accounts	Redirusr ou=NewOU,dc=Domainname,dc=com
WinRM	WinRM is part of the WS-Management protocol it is used to process management requests received over the network.	If remote management is not enabled then you will have trouble remotely managing servers across the network. **WinRm Quickconfig** is used to enable remote management.

PowerShell is by far the most powerful command line tool Microsoft has ever given us, in the 70-410 exam you will see example lots of questions that test your knowledge of PowerShell. My advice would be to:

1. Learn the PowerShell syntax and make sure you can differentiate when to use GET- SET- and NEW- CMDLets.
2. Memorize a list of 10 to 15 CMDLets that you have come across during labs and write them down before you start your exam.
3. As you go through the exam write downs any CMDLets you see during the test, they might be useful later on

Use the following list as a starting off point.

CMDLet	Description
New-Aduser	New-ADuser is used to create a new Active Directory User Account, once you have created a new user account then the Set-Aduser CMDLet can be used to make changes to user accounts.
Set-AdAccountControl	This CMDLet is used to modify user account control values for an AD Account, example of things that you can change with this CMDLet include setting the user CanNotChangePassword option, PasswordNeverExpires option, AllowReversiblePasswordEncryption option.
New-VHD	The CMDLet is used to create .VHD and .VHDX files that can be used for various purposes including creating virtual machines. This cmdlet should not be confused with the NEW-VirtualDisk CMDLet which is used during the creation

	Storage Spaces
Add-DnsServerPrimaryZone	This CMDLet is used to create both standard and ADI zones. Once a zone is created the Set-DNSServerPrimaryZone CMDLet can be used to make changes to the zone.
Add-DnsServerSeondaryZone	This CMDLet is used to create a Secondary Zone on a DNS Server
Install-ADDSForest	This CMDLet is used to create a new AD Forest
Install-ADDSDomain	This CMDLet is used to create a new AD Domain in an Existing Forest
Enable-VMResourceMetering	This CMDLet is used to enable the monitoring of disk, memory processes or and network usage of a virtual machine
Measure-VM	This CMDLet is used to view the statistics that Enable-VMResourceMetering has gathered.

Windows Server Migration Tools

The Window Server migration tools can be used to migrate roles and features as well as files and folders from one server to another. The Windows Server Migration Tools can be installed as a feature on a Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2 server. If you wish to migrate roles, features, files or folders from a Windows 2008 or Windows 2003 server then you must first deploy the Windows Server migration tools to that server first.

Deploying the Windows Server Migration Tools to a Windows 2003 or Windows 2008 server

1. Install the Windows Server Migration tools on a Windows 2008R2 or Windows 2012 Server
2. Navigate to the C:\windows\System32\ServerMigrationtools directory
3. Run the following for to create a deployment package to migrate a role from a windows 2003 amd64 computer storing the package in a local folder called Deployment**Smigdeploy.exe /Package /architecture amd64 /os WS03 /path C:\deployment**

You could use x86 instead of AMD64 and WS08 instead of WS03

4. Copy the deployment folder you have just created to the source server

5. From the command prompt on the source computer navigate to the deployment folder you have just copied and run **SMIGDEPLOY.EXE**

Windows Server Migration Tools CmdLets

Receive-SmigServerData – run on the destination Server for a migration of Folders and Files with associated permissions and share properties

Send-SmigServerData – Run on the source server for a migration of Folders and Files with associated permissions and share properties

Get-SmigServerFeature – lists all the roles that can be migrated with the Windows Server Migration tools.

Export-SmigServerSettings – run on the source Server for a migration of a role or feature

Import-SmigServerSettings – run on the destination Server for a migration of a role or feature

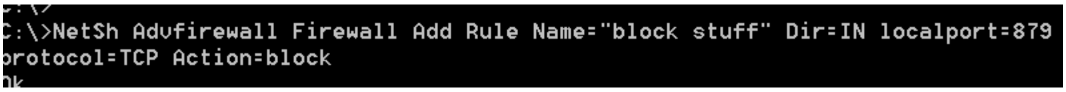
For detailed information on using these CMDLets to migrate content please follow the link below:

https://technet.microsoft.com/en-us/library/jj134202.aspx

Configuring Windows Advanced Firewall with NETSH and PowerShell

NetSh advfirewall is a command line tool for administering Windows firewall and Advanced Security
To configure a firewall rule with NetSH

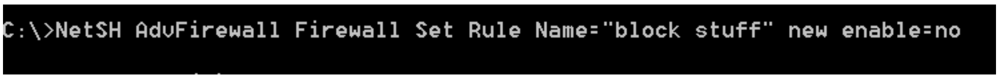
NetSh Advfirewall Firewall Add Rule name=*rulename* dir=*In/out* –localport=*Portnumber* localprotocol=*protocol* Action=*Allow/Block*



```
C:\>NetSh Advfirewall Firewall Add Rule Name="block stuff" Dir=IN localport=879
protocol=TCP Action=block
Ok
```

This example add an inbound firewall rule to block an application called “Block Stuff” that uses TCP port 879
To Update and existing Firewall Rule with Netsh

Netsh AdvFirewall Firewall Set Rule Name=*rulename* new enable=*yes/no*

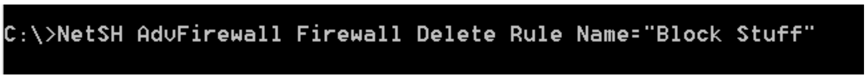


```
C:\>NetSH AdvFirewall Firewall Set Rule Name="block stuff" new enable=no
```

This command changes the state of a firewall rule state from enabled to disabled, use the SET command to make changes to an existing rule.

To Delete a Firewall Rule using Netsh

NetSH AdvFirewall Firewall Delete Rule Name=*rulename*

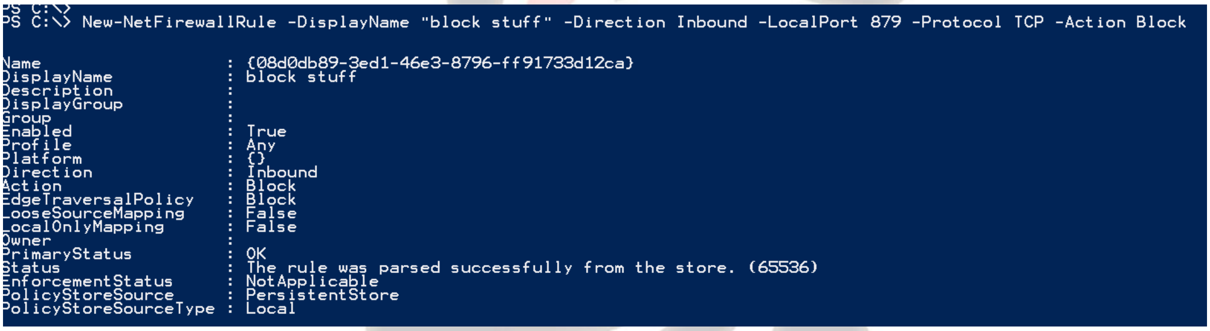


```
C:\>NetSH AdvFirewall Firewall Delete Rule Name="Block Stuff"
```

This command deletes a firewall rule by using the Delete command and specifying the name of the rule.

To configure a firewall rule with PowerShell

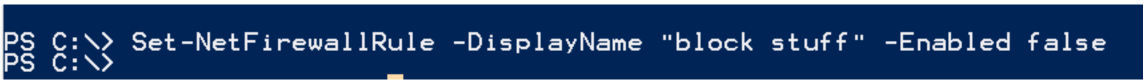
New-NetFirewallRule –displayname *displayname* –Direction *outbound/inbound* –Localport *localport* –Protocol *protocol* –Action *Block/Allow*



```
PS C:\> New-NetFirewallRule -DisplayName "block stuff" -Direction Inbound -LocalPort 879 -Protocol TCP -Action Block

Name                  : {08d0db89-3ed1-46e3-8796-ff91733d12ca}
DisplayName           : block stuff
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Block
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

To Update and existing Firewall Rule with PowerShell

Set-NetFirewallRule –DisplayName *displayname* –Enabled *true/false*

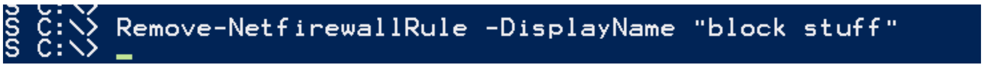


```
PS C:\> Set-NetFirewallRule -DisplayName "block stuff" -Enabled false
PS C:\>
```

Use the Set-NetFirewallRule to make changes to an existing firewall rule, in this example we have changed a rule from enabled (true) to disabled (false)

To Delete a Firewall Rule using PowerShell

Remove-NetfirewallRule –Displayname *displayname*



```
S C:\> Remove-NetfirewallRule -DisplayName "block stuff"
S C:\>
```

Use the Remove-NetFirewallRule to remove an existing firewall rule by specifying its display name.

Day 4

Day 4 is all about revision, with your instructor you will review DNS and GPOs as well as Hyper-V and virtualization.

This is the first exam day with exam 70-410 at 4pm

Hyper-V Cmdlets

CMDLET	Description
Checkpoint-VM	Creates a snapshot of a virtual machine
Enable-VMResourceMetering	Collects resource utilization data collection for a virtual machine or resource pool
Measure-VM	Reports resource utilization data for one or more virtual machines
Measure-VMReplication	Gets replication statistics and information associated with a virtual machine
Add-VMFibreChannelHba	Adds a virtual Fibre Channel host bus adapter to a virtual machine

Administering Windows Server 2012

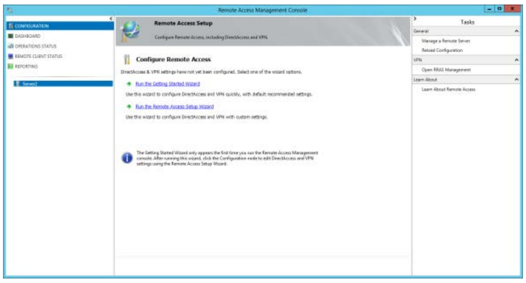
Day 5

Direct Access Basic Setup

Direct Access in Windows Server 2012 has been massively simplified. All configurations for the Direct Access Server can now be done from one area, the Remote Access Management Console. IPv6 is still a requirement for a Direct Access connection but Certificate Services is not (although I would suggest that an enterprise Direct Access deployment would employ digital certificates for authentication).

Before you configure Direct Access you may want to add a security group to AD that will be used to give you Computers access to direct access.

1) Access the Remote Access Management Console, from here you can run the getting started wizard.



Configure Remote Access, including DirectAccess and VPN.

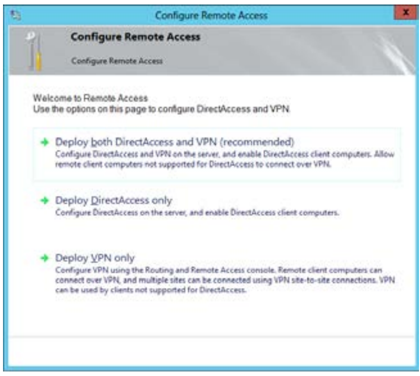
DirectAccess & VPN settings have not yet been configured. Select one of the wizard options.

Use this wizard to configure DirectAccess and VPN quickly, with default recommended settings.

Use this wizard to configure DirectAccess and VPN with custom settings.

The Getting Started Wizard only appears the first time you run the Remote Access Management console. After running this wizard, click the Configuration node to edit DirectAccess and VPN settings using the Remote Access Setup Wizard.

2) Once you have selected the Getting started wizard you get to choose to deploy both Direct Access and VPN or Direct Access Only or VPN Only. Choose Direct Access only.

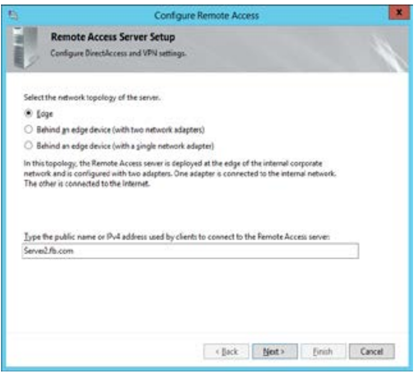


Configure Remote Access

Configure Remote Access

Welcome to Remote Access
Use the options on this page to configure DirectAccess and VPN

- Deploy both DirectAccess and VPN (recommended)
  Configure DirectAccess and VPN on the server, and enable DirectAccess client computers. Allow remote client computers not supported for DirectAccess to connect over VPN.
- Deploy DirectAccess only
  Configure DirectAccess on the server, and enable DirectAccess client computers.
- Deploy VPN only
  Configure VPN using the Routing and Remote Access console. Remote client computers can connect over VPN, and multiple sites can be connected using VPN site-to-site connections. VPN can be used by clients not supported for DirectAccess.



Remote Access Server Setup

Configure DirectAccess and VPN settings.

Select the network topology of the server.

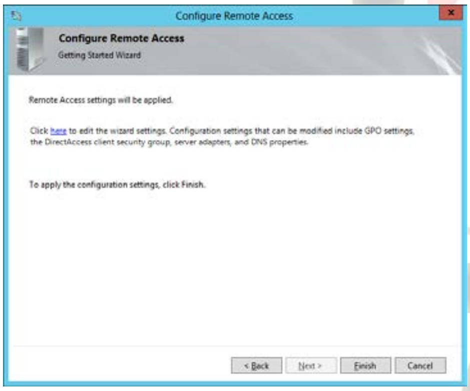
● Edge
○ Behind an edge device (with two network adapters)
○ Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.

Type the public name or IPv4 address used by clients to connect to the Remote Access server:
Server2.fb.com

3) The next screen gives you the option of choosing a configuration for you Direct Access connection. With Direct Access in windows Server 2012 you can now deploy Direct Access with a single network card, you can configure your Direct Access Server behind a NAT server or you can configure your Server on the edge with two network cards, one facing internally and one facing externally. I choose an Edge Deployment.

You are also asked for the IPv4 address or FQDN that clients will use on the outside to connect to your Direct Access Server.



Configure Remote Access

Getting Started Wizard

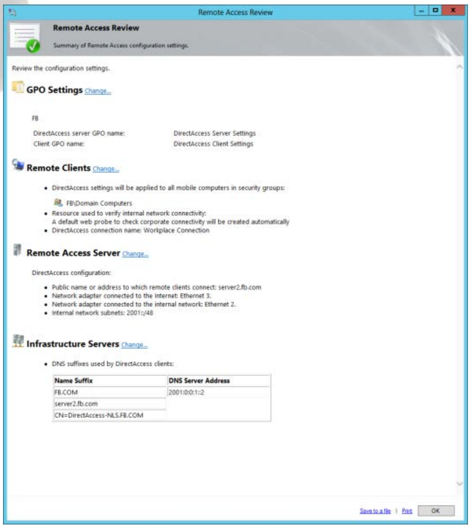
Remote Access settings will be applied.

Click here to edit the wizard settings. Configuration settings that can be modified include GPO settings, the DirectAccess client security group, server adapters, and DNS properties.

To apply the configuration settings, click Finish.

4. If you do nothing else and click finish then your Direct Access server will be configured with standard setting, or you can select to edit the default settings.

If you edit the settings you get to do several things, firstly you can edit the Client and Server Settings, you can also configure settings for the NRPT Table.



Remote Access Review

Summary of Remote Access configuration settings.

Review the configuration settings.

GPO Settings Change...

FB

DirectAccess server GPO name:	DirectAccess Server Settings
Client GPO name:	DirectAccess Client Settings

Remote Clients Change...

- DirectAccess settings will be applied to all mobile computers in security groups:
  FB\Domain Computers
- Resource used to verify internal network connectivity:
  A default web probe to check corporate connectivity will be created automatically
- DirectAccess connection name: Workplace Connection

Remote Access Server Change...

DirectAccess configuration:

- Public name or address to which remote clients connect: server2.fb.com
- Network adapter connected to the Internet: Ethernet 3.
- Network adapter connected to the internal network: Ethernet 2.
- Internal network subnets: 2001::/48

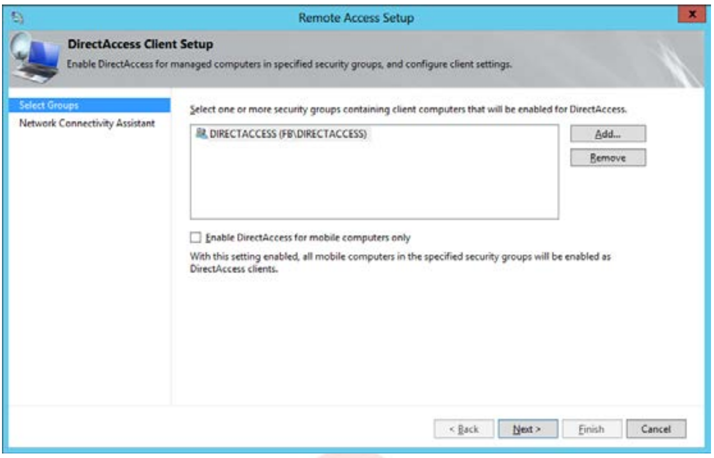
Infrastructure Servers Change...

- DNS suffixes used by DirectAccess clients:

Name Suffix	DNS Server Address
FB.COM	2001:0:0:1::2
server2.fb.com	
CN=DirectAccess-NLS.FB.COM	

5. Here we can edit the Client Settings, notice how I have removed the default group and chosen a group called Direct Access, all computers that I want to use direct access should be added to this group. The GPO that direct access wizard creates will be filtered to apply to this group. Also notice that I have removed

the tick for the Enable DirectAccess for mobile computer only box. When this box is selected a WMI filter is linked to the DirectAccess GPO to filter the GPO to only apply to Mobile Clients.



DirectAccess Client Setup

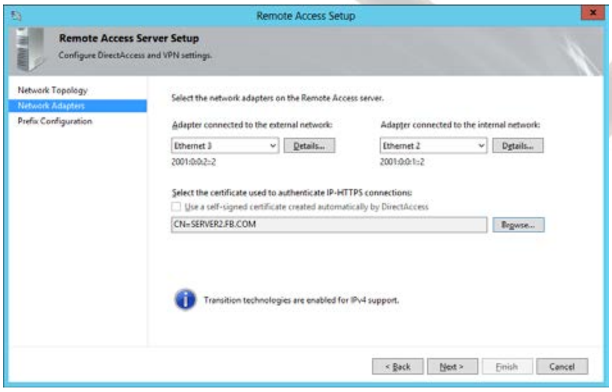
Enable DirectAccess for managed computers in specified security groups, and configure client settings.

Select one or more security groups containing client computers that will be enabled for DirectAccess.

DIRECTACCESS (FB\DIRECTACCESS)

□ Enable DirectAccess for mobile computers only

With this setting enabled, all mobile computers in the specified security groups will be enabled as DirectAccess clients.



Remote Access Server Setup

Configure DirectAccess and VPN settings.

Select the network adapters on the Remote Access server.

Adapter connected to the external network: Ethernet 3
2001:0:0:2::2

Adapter connected to the internal network: Ethernet 2
2001:0:0:1::2

Select the certificate used to authenticate IP-HTTPS connections:

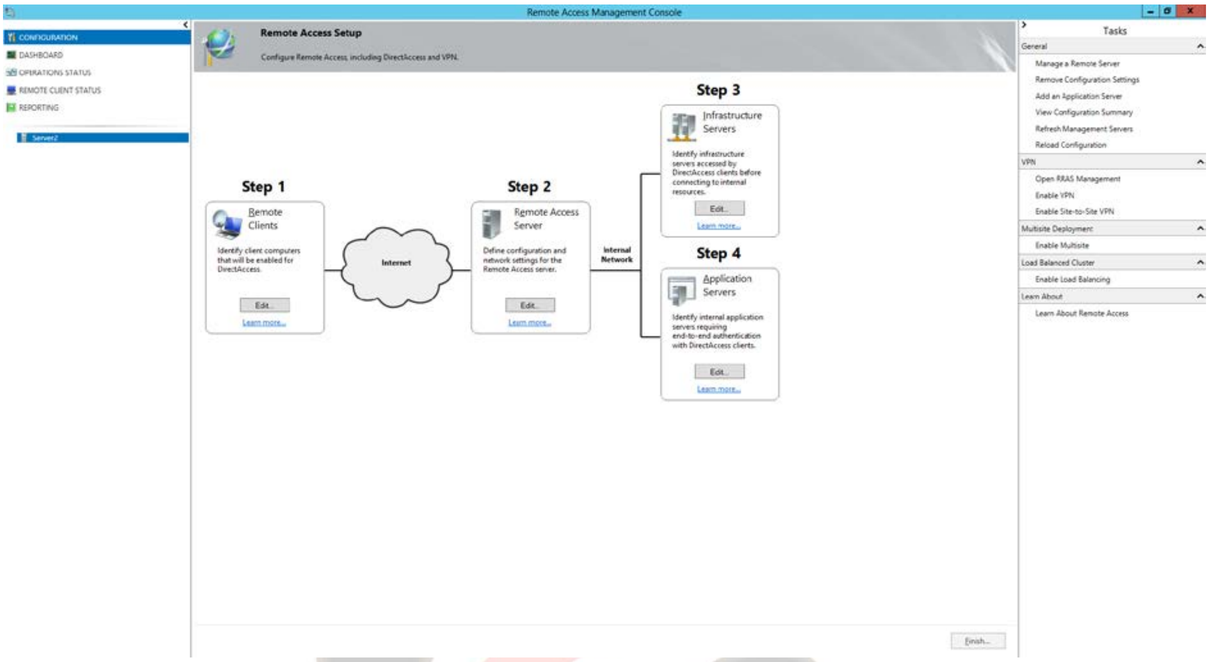
□ Use a self-signed certificate created automatically by DirectAccess

CN=SERVER2.FB.COM

Transition technologies are enabled for IPv4 support.

If you chose to edit the server setup you can choose which interfaces are the internal and external interfaces, and if you are using a certificate for authentication you can choose it here. Remember if you are going to use digital certs as part of your deployment you must also make sure you publish both AIA and CDP points accessible to your clients.

Once you have finished your setup, you will see a screen similar to the one below. Form here you can customise and part of your direct access setup. This includes domain name suffixes that would be considered internal and what DNS servers should be used for those suffixes.



Configure Remote Access, including DirectAccess and VPN.

Identify client computers that will be enabled for DirectAccess.

Define configuration and network settings for the Remote Access server.

Identify infrastructure servers accessed by DirectAccess clients before connecting to internal resources.

Identify internal application servers requiring end-to-end authentication with DirectAccess clients.

If you are using Windows 7 clients you must also use Digital certificates for authentication, if you are using windows 8 clients you can use Kerberos authentication

All clients that you intend to use DirectAccess must be domain joined, so either join them to the domain internally so the DirectAccess GPO's can be applied or if the client machines are outside your network you can use Djoin to add them to the domain and configure the DirectAccess client components.

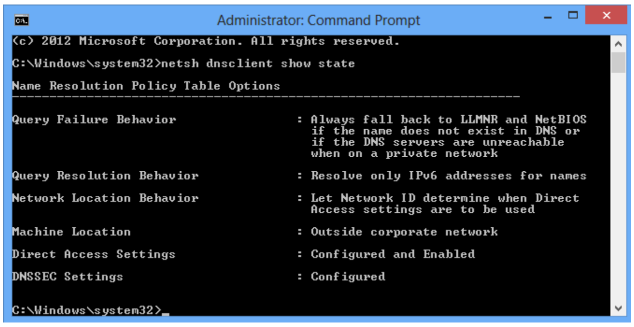
EXAM PREP – make sure you are happy with the wizard, the GPO settings, the WMI filter, the group used to apply the GPO to you clients.

CLIENTS

When a client connects to the network it will attempt to access the Network Location Server (NLS) if it can connect then the client is internal and does not configure DirectAccess if it can't connect to the NLS service then it is external and a DirectAccess is connection is established.

On the client you can use NETSH to verify DirectAccess connectivity.

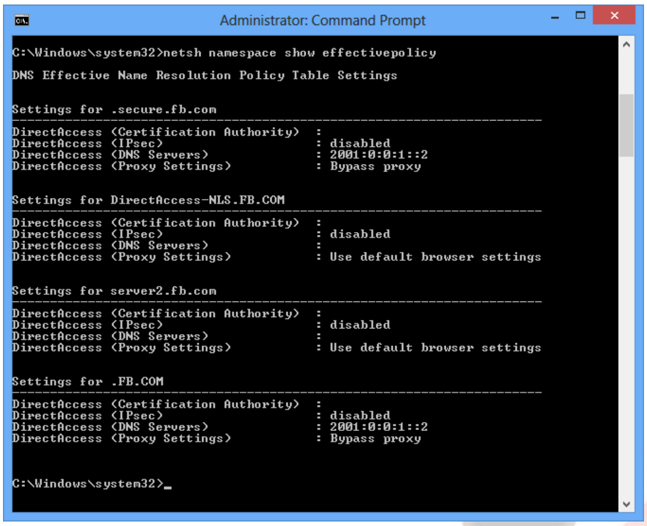
NetSH DNSCLIENT SHOW STATE



```
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh dnsclient show state

Name Resolution Policy Table Options
--------------------------------------------------------------------

Query Failure Behavior                  : Always fall back to LLMNR and NetBIOS
                                          if the name does not exist in DNS or
                                          if the DNS servers are unreachable
                                          when on a private network

Query Resolution Behavior               : Resolve only IPv6 addresses for names

Network Location Behavior               : Let Network ID determine when Direct
                                          Access settings are to be used

Machine Location                        : Outside corporate network

Direct Access Settings                  : Configured and Enabled

DNSSEC Settings                         : Configured

C:\Windows\system32>_
```

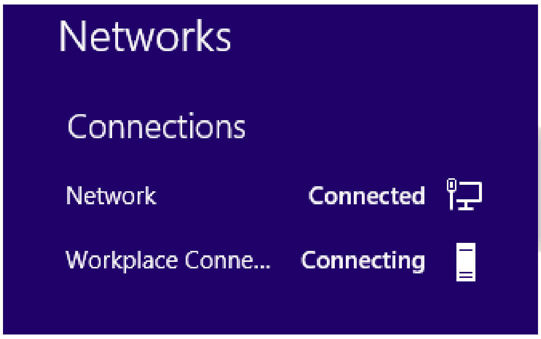
By using NetSh we can see we have a DirectAccess connection Configured and Enabled

NetSH NAMESPACE SHOW EFFECTIVEPOLICY



```
C:\Windows\system32>netsh namespace show effectivepolicy

DNS Effective Name Resolution Policy Table Settings


Settings for .secure.fb.com
----------------------------------------------------------------------
DirectAccess (Certification Authority)  :
DirectAccess (IPsec)                    : disabled
DirectAccess (DNS Servers)              : 2001:0:0:1::2
DirectAccess (Proxy Settings)           : Bypass proxy


Settings for DirectAccess-NLS.FB.COM
----------------------------------------------------------------------
DirectAccess (Certification Authority)  :
DirectAccess (IPsec)                    : disabled
DirectAccess (DNS Servers)              :
DirectAccess (Proxy Settings)           : Use default browser settings


Settings for server2.fb.com
----------------------------------------------------------------------
DirectAccess (Certification Authority)  :
DirectAccess (IPsec)                    : disabled
DirectAccess (DNS Servers)              :
DirectAccess (Proxy Settings)           : Use default browser settings


Settings for .FB.COM
----------------------------------------------------------------------
DirectAccess (Certification Authority)  :
DirectAccess (IPsec)                    : disabled
DirectAccess (DNS Servers)              : 2001:0:0:1::2
DirectAccess (Proxy Settings)           : Bypass proxy


C:\Windows\system32>_
```

With this NetSH command we can see the setting of the NRPT table.



Networks

Connections

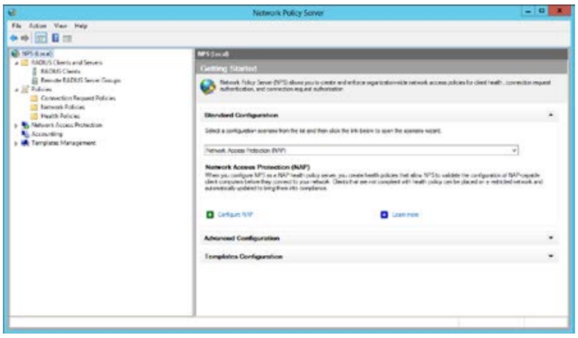
Network Connected

Workplace Conne... Connecting

Finally we can see the Networks view, notice the default name for the DirectAccess connection is Workplace Connection and the icon is a Server

NPS Basic Setup

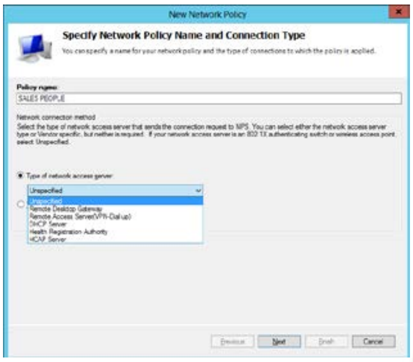
Remember that all RAS Servers have Network policies that can be configured locally on the RAS server, these policies are used when our RAS server is using Windows Authentication and Windows Accounting, if however we choose to configure our RAS Server with RADIUS Authentication and RADIUS Accounting then authentication and Logging information is sent to an NPS Server. Our RAS Server becomes a RADIUS Client and our NPS Server becomes the RADIUS Server.



Here we have the NPS Server Snapin, the first section allows us to detail RADIUS Clients and Remote RADIUS Server Groups. The RADIUS clients are RAS server (and other types of server) that will be passing authentication and accounting requests to our NPS Server. The Remote RADIUS Serve group section allows us to create named groups of RADIUS servers that we will pass Authentication and Accounting information to when we are configuring our NPS Server as a RADIUS Proxy.

Policies

When we want to control authentication and accounting for a particular set of RADIUS clients we have to configure **Network Policies** to allow certain Users/Groups/Clients access.


New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

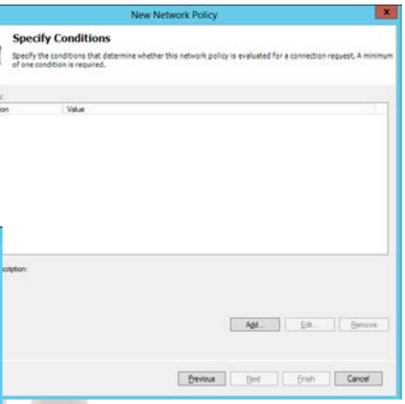
Policy name:
SALES PEOPLE

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:
Unspecified
- Unspecified
- Remote Desktop Gateway
- Remote Access Server(VPN-Dial up)
- DHCP Server
- Health Registration Authority
- HCAP Server

When you right click Network Policies and select New we are first asked to Name the policy, here I have named a policy Sales People. You can also select the type of clients passing requests to this RADIUS server and whom this policy is designed to effect.

Next you get to specify a condition. A condition can be one of many things but some of the more common are Data and Time, windows group Membership, Protocol and client type.

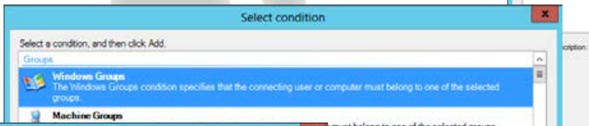

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value

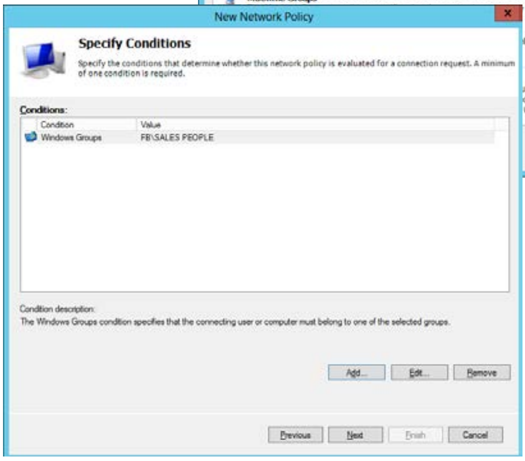

Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Machine Groups


New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

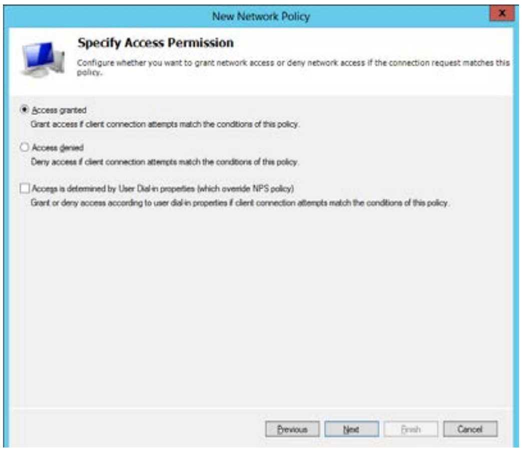
Conditions:

Condition	Value
Windows Groups	FB\SALES PEOPLE

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

ition of Windows Group with a s People. This means that in order for this policy to match a connection then the person connecting must be a member of the Sales People Security group. You can add multiple conditions to this list. If you do then al conditions must be met in order for this policy to take effect.

On the next screen we can select whether this policy Grants Access of Denies Access based on the previous conditions.


New Network Policy

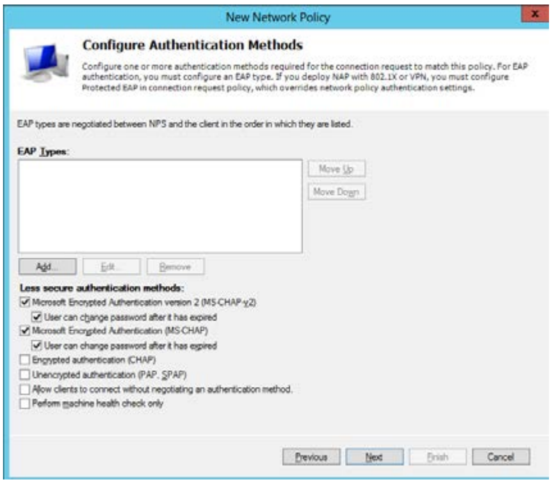
Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● Access granted
Grant access if client connection attempts match the conditions of this policy.

○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

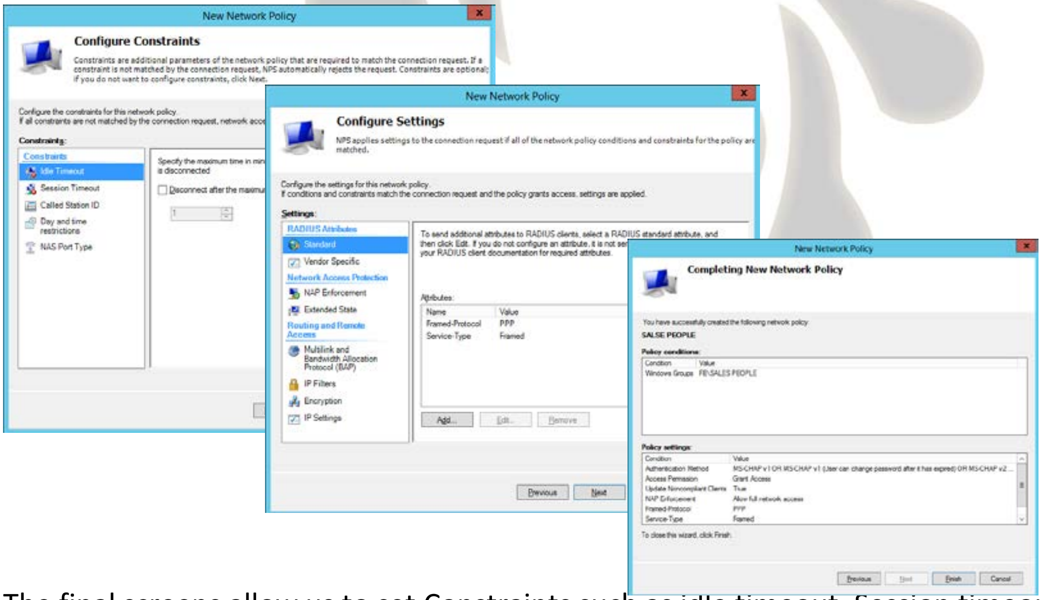
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  ☑ User can change password after it has expired
☑ Microsoft Encrypted Authentication (MS-CHAP)
  ☑ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.
☐ Perform machine health check only

Once we have chosen an Access Permission we can then select the Authentication types that will be allowed. We can select multiple authentication methods and if a client connecting in supports multiple authentication methods they will use the strongest one.



Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network acce

Constraints:

Specify the maximum time in min
is disconnected

☐ Disconnect after the maximu

1

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not ser
your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Completing New Network Policy

You have successfully created the following network policy:

SALSE PEOPLE

Policy conditions:

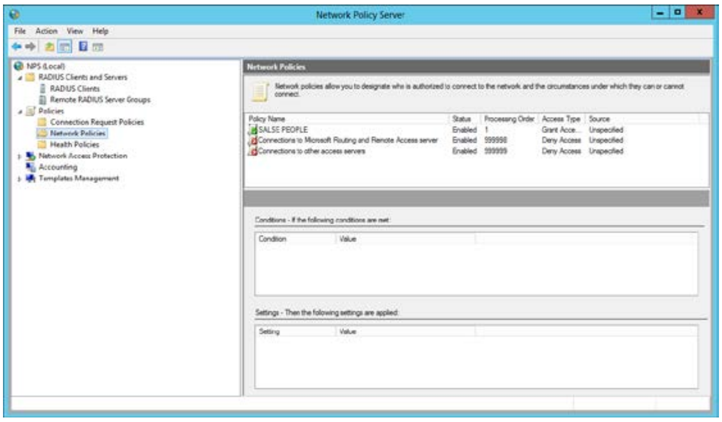
Condition	Value
Windows Groups	FB\SALES PEOPLE

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

The final screens allow us to set Constraints such as idle timeout, Session timeout, Day and time restrictions, plus settings such as IP Filters, Nap Enforcement etc. Finally we get to see all the settings we have selected and confirm the settings



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
SALSE PEOPLE	Enabled	1	Grant Acce...	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

Conditions - If the following conditions are met:

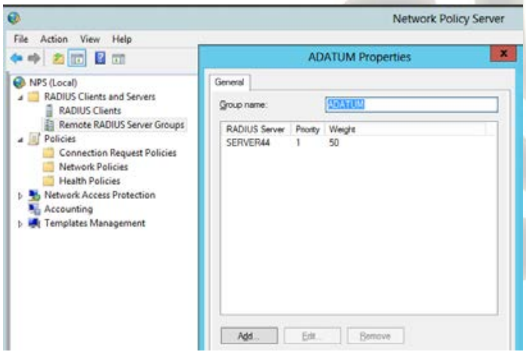
Condition	Value

Settings - Then the following settings are applied:

Setting	Value

Here we can see the network policy we have created, the order in which the policies are processed is very important. There are two default polices both have different settings configured but amount to denying everyone 24/7. The policies are processed in order from top to bottom. So policies that allow access should be placed near the top of the list and those that deny access lower down the list. If we put the deny policies near the top then you risk you allow policies never taking effect because they will never be read. Here I have 1 policy that allows the members of the Sales group to Authenticate, if you were trying to access a RAS Server who is passing authentication requests to this NPS server and you are a member of the Sales group you will be allowed access. If you were not a member of the Sales group then the conditions of the policy are not met and the next policy in the list will be processed, then the next and then the next until a policies condition are met or we get to the two default policies that say 24/7 deny access. As soon as you meet a policies condition then processing stops and that policy is applied to you.

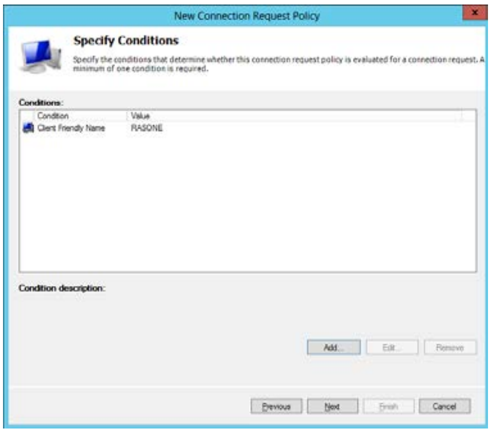
If you want you NPS server to act as a RADIUS Proxy then you must configure **Connection Request Policies.**



Group name: ADATUM

RADIUS Server	Priority	Weight
SERVER44	1	50

Before you configure a Connection Request Policy you should configure at least 1 Remote RADIUS Server Group. This named group identifies other RADIUS servers that we will pass different type of connections to. Here we have configured a group called Adatum which includes 1 server. We can now configure our first Connection Request Policy



Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

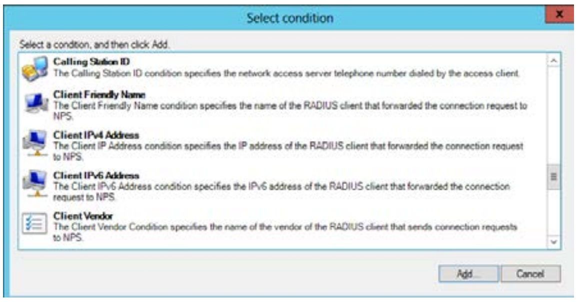
Conditions:

Condition	Value
Client Friendly Name	RASONE

Condition description:

The first screen allows us to Specify a name for our policy the on the Specify Condition screen we can choose conditions that must be met before we pass the connection on to another RADIUS Server. Conditions can be based on lots of pieces of information passed to the RADIUS proxy.

The following screen shots list several methods that can be used to choose whether or not to pass a connection on to another RADIUS Server.



Select a condition, and then click Add.

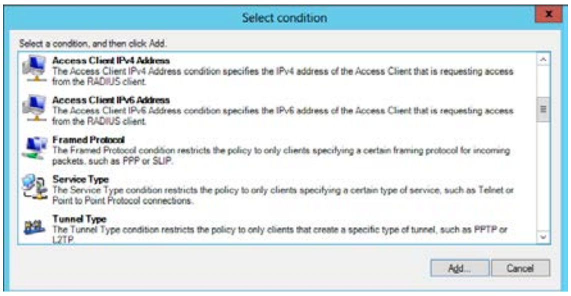
Calling Station ID
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.

Client Friendly Name
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.

Client IPv4 Address
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

Client IPv6 Address
The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the connection request to NPS.

Client Vendor
The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connection requests to NPS.



Select condition

Select a condition, and then click Add.

Access Client IPv4 Address
The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.

Access Client IPv6 Address
The Access Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access from the RADIUS client.

Framed Protocol
The Framed Protocol condition restricts the policy to only clients specifying a certain framing protocol for incoming packets, such as PPP or SLIP.

Service Type
The Service Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or Point to Point Protocol connections.

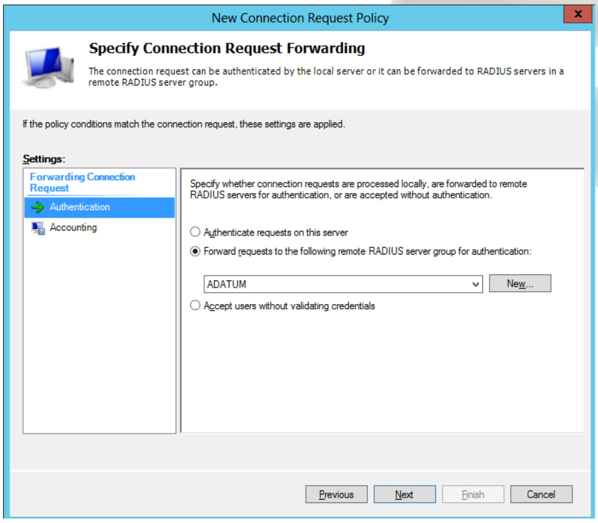
Tunnel Type
The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.

We can choose Client Friendly Names and addresses these are the details of the RADIUS client who is sending us the connection attempt

We can choose Access Client IP Address and Names; these are the details of the Remote Client requesting access from the RADIUS client.

We can choose the Frame Protocol (PPP) or tunnel type (L2TP or PPTP) that is being used to access the RADIUS Server.

If the conditions are met then the next screen allows us to decide whether our NPS Server handles the connection or whether we pass it on to another RADIUS Server based on remote Radius server group name.



New Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

○ Authenticate requests on this server

● Forward requests to the following remote RADIUS server group for authentication:

ADATUM

○ Accept users without validating credentials

Here we can see ive choosed to pass this request on to a Group previously created called ADATUM. Also notice you can choose to send the Authentication or Accounting information on the another server or indeed both.

RAS/NPS/NAP Videos

[RAS/NPS/NAP Video 1]

Or

https://www.youtube.com/watch?v=toejB3R0Uw4&list=PL2QNrvCUc_M9iXOQ7XcE40yUSXfuVwXpx&index=1

RAS/NPS/NAP Video 2

Or

https://www.youtube.com/watch?v=kEm_umwFsQw&list=PL2QNrvCUc_M9iXOQ7XcE40yUSXfuVwXpx&index=2

Administering Active Directory Backup and Recovery

The link below will take you to a TechNet article on AD backup and recovery

https://technet.microsoft.com/library/cc794826(v=ws.10).aspx

Managed Service Accounts

The Link Below will take you to a TechNet article on Managed Service Accounts

https://technet.microsoft.com/library/ff641731(v=ws.10).aspx

SetSPN

Although Managed service accounts will create Service Principle Names for you there will be times when you have to create your own SPNs for your service accounts. SetSPN.exe is used to create Service Principal Names.

Example 1: List currently registered SPNs

```
setspn -l daserver1
```

```
Registered ServicePrincipalNames for
CN=DASERVER1,CN=Computers,DC=reskit,DC=contoso,DC=com:
HOST/daserver1
HOST/daserver1.reskit.contoso.com
```

Example 2: Reset default registered SPNs

```
setspn -r daserver1
```

```
Registering ServicePrincipalNames for
CN=DASERVER1,CN=Computers,DC=reskit,DC=contoso,DC=com
HOST/daserver1.reskit.contoso.com
HOST/daserver1
Updated object
```

Example 3: Add a new SPN

```
    setspn -s http/daserver1.reskit.contoso.com daserver1
```

```
Registering ServicePrincipalNames for
CN=DASERVER1,CN=Computers,DC=reskit,DC=contoso,DC=com
http/daserver1.reskit.contoso.com
Updated object
```

Example 4: Remove an SPN

```
    setspn -d http/daserver1.reskit.contoso.com daserver1
```

```
Unregistering ServicePrincipalNames for
CN=DASERVER1,CN=Computers,DC=reskit,DC=contoso,DC=com
http/daserver1.reskit.contoso.com
Updated object
```

The link below gives more information on creating SPNs

https://technet.microsoft.com/en-us/library/cc731241.aspx#BKMK_examples

Day 5 Fill in the Details

Please fill in the Blanks

1. When restoring an object that has been accidently deleted from AD you can use ___________ or __________ or ___________
2. To create and mount an Active Directory Snapshot you would use the following steps: ____
    1. ____
    2. ____
    3. ____
    4. ____
    5. ____
3. To use an NPS Server as a RADIUS Proxy you would need to configure ______________ and _______________________ and ______________________
4. If you want to prevent Windows 7 clients from connecting use a VPN connection you would use the __________________ Network Policy condition.
5. If you want all traffic from Direct Access Clients to flow through your Direct Access server you should configure ________________________________
6. A Direct Access clients uses ____________________ to determine what traffic should be passed to the direct access server and what traffic should be passed to the clients ISP

7. When configuring the built in SHV the _____________ setting cannot be configured for XP clients.
8. To reset the Default GPOs we can use the __________ cmdline tool
9. To fix you GPOs after you have renamed your domain you would use the ________ cmdline tool.

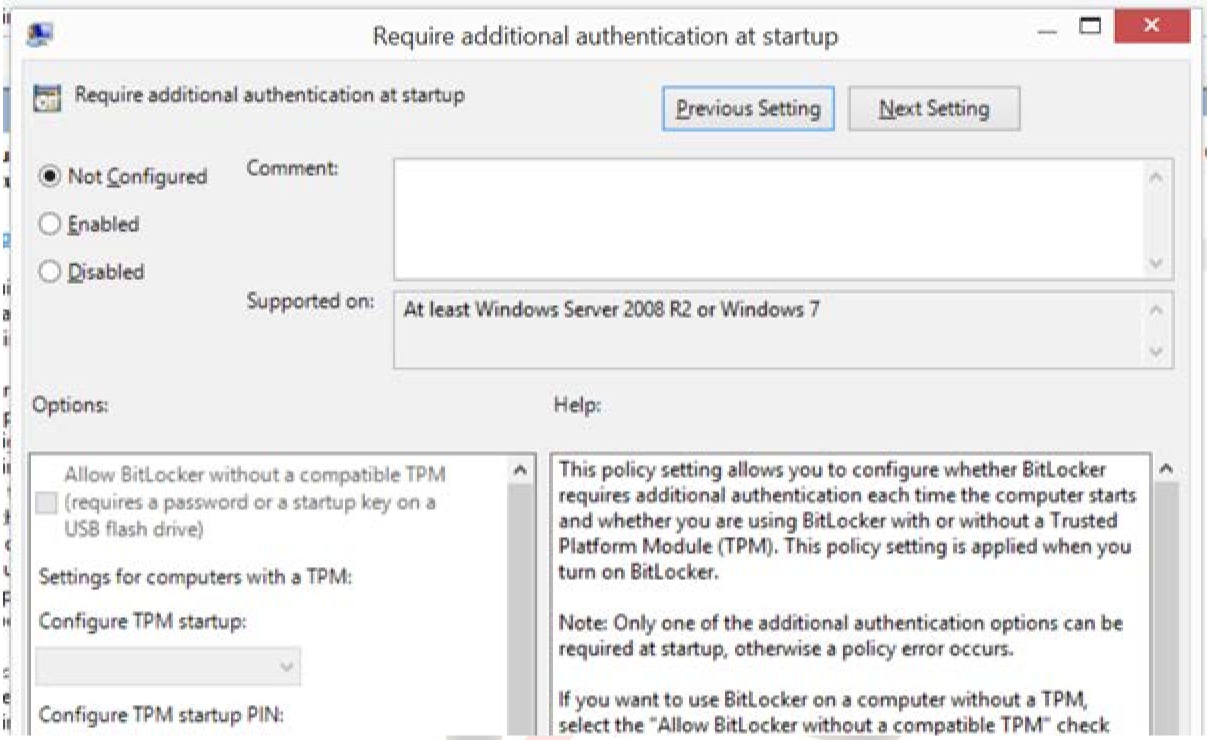
Day 5 Additional Labs

1) Make sure DC1, DC2 RAS1 and WKS1 are started and logon to each as fb\administrator
2) On RAS1 install the Remote Access role making sure you install both the remotes access and routing roles
3) Configure RAS1 as a VPN server
4) Make sure that only members of the LEEDSAdmin group and the DomainAdmins groups can use the VPN connection
5) Make sure that WKS1 is connected to the Internet Network then login to WKS1 as a member of the LeedsAdmin group and attempt to connect to RAS1 with a VPN connection.

DAY 6

Bitlocker Drive Encryption – PowerShell

Although BitLocker has been around for a while Microsoft still consider it a vital part of their security toolkit. Configuring bitLocker on Windows Server requires that you install the bitLocker feature first. You will also need to consider whether the machine you are enabling bitlocker on has a TPM chip or not. If not you will have to configure an alternate protection method.



Require additional authentication at startup

Require additional authentication at startup

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

□ Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup:

Configure TPM startup PIN:

Help:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

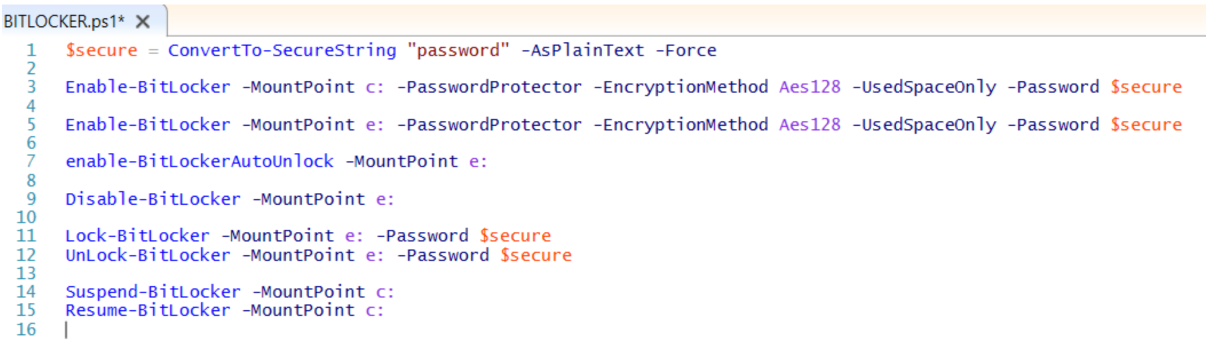
If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check

If you don't have a TPM chip in your server (which you probably won't if you are using a VM) you will need to enable the **Allow BitLocker without a compatible TPM** setting through either Local Group policy or a domain/OU GPO. You can find the path to the setting by searching for the **require additional Authentication at Start-up** GPO setting.

If you enabling bitlocker on a workstation such as Win7 or Win8 then bitlocker will already be installed, if you want to enable BitLocker on a Server you will first need to install the BitLocker feature.

After a reboot you can enable BitLocker by Right clicking the drive you wish to protect or by using the Manage-BDE.exe tool (this looks a bit like a PowerShell CMDLet but it is an .exe).

Using PowerShell you can use the following command to enable and work with BitLocker.



BITLOCKER.ps1*

```
$secure = ConvertTo-SecureString "password" -AsPlainText -Force

Enable-BitLocker -MountPoint c: -PasswordProtector -EncryptionMethod Aes128 -UsedSpaceOnly -Password $secure

Enable-BitLocker -MountPoint e: -PasswordProtector -EncryptionMethod Aes128 -UsedSpaceOnly -Password $secure

enable-BitLockerAutoUnlock -MountPoint e:

Disable-BitLocker -MountPoint e:

Lock-BitLocker -MountPoint e: -Password $secure
UnLock-BitLocker -MountPoint e: -Password $secure

Suspend-BitLocker -MountPoint c:
Resume-BitLocker -MountPoint c:

```

(The Lines in the example above are not intended to be on long script they should be run one at a time as needed)

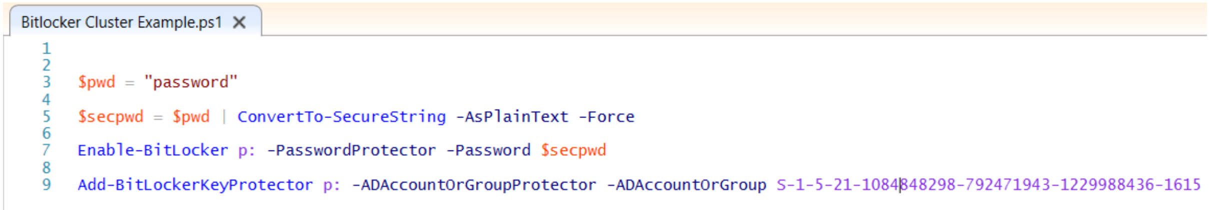
The first line create a secure password to be used as a password protector. We then have two lines enabling BitLocker on an OS drive (C:) and a data drive (D:). We then have the command Enable-BitlockerAutoUnlock. This command only works with Data drives and only after the OS drive has been encrypted. It is used to automatically decrypt data drives after a reboot. Disable-Bitlocker is used on both data and OS drives to disable BitLocker, Suspend-Bitlocker is used on OS drive to temporarily remove the password requirement. This is useful during patching operations.

You can also enable BitLocker on drives that will be used as shared storage for Failover clusters.

Failover Clusters use disks to store data needed by their clustered roles, this storage can be dedicated to a specific cluster role or shared amongst several. When a role fails over to another node in the cluster then the disk storage must be accessible by the node that has taken control of the role. BitLocker Drive Encryption can be used to encrypt the disk that is being used or that will be used by the failover cluster for its storage. If a disk is already assigned to the failover cluster then the disk must be put into maintenance mode before we can apply BitLocker Drive Encryption to it, if the disk hasn’t been assigned yet then we can apply BitLocker drive Encryption fist and then assign it to the failover cluster.

For this exercise I have connected an iSCSI disk to my failover cluster nodes, created a volume on it and given it the drive letter P: I have not added the disk to the Failover cluster.

Here is a PowerShell script used to apply BitLocker Drive Encryption to a disk before it is added to a failover cluster:



```


$pwd = "password"

$secpwd = $pwd | ConvertTo-SecureString -AsPlainText -Force

Enable-BitLocker p: -PasswordProtector -Password $secpwd

Add-BitLockerKeyProtector p: -ADAccountOrGroupProtector -ADAccountOrGroup S-1-5-21-1084848298-792471943-1229988436-1615
```

Before discussing the script we need to spend a little time talking about BitLocker Protectors.

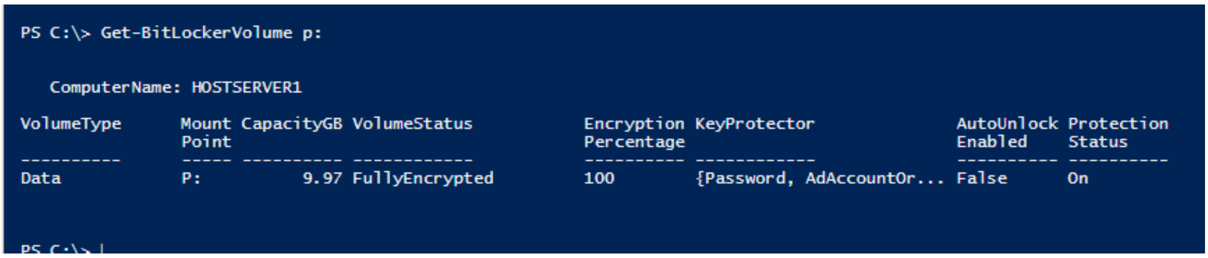
BitLocker Protectors are used to manage access to your BitLocker protected drives, there are many forms of BitLocker protector from TPM chips to recovery passwords and PIN Numbers. In our example we use two BitLocker protectors, the First is a Password Protector that uses a password to decrypt the drive. When you use a Password protector to secure access to a drive, the drive will stay encrypted until you provide the correct password. The Password protector might be OK for a drive that is accessed by a user but for a drive to be used in a failover cluster the cluster itself needs to be able to decrypt the drive. To do this the Cluster Account created for the Failover must be able to decrypt the drive, the Cluster account can be accessed by all members of the failover cluster. We use the new ADAcountOrGroup Protector to give the cluster account the ability to decrypt the BitLocker protected drive. If you don't use the ADAcountOrGroup Protector the failover cluster will not be able to bring the disk resource online when it is imported into the failover cluster.

The first two line of my script define variables that create a new password and convert that password to a secure string, without converting the password to a secure string we cannot use it to protect our drive, the 3rd line in my script is the line that enables BitLocker on drive P: (remember this is an iSCSI drive that will be used by my failover cluster). The **ENABLE-BITLOCKER** CMDLET is used to enable BitLocker, we then identify the volume it is securing and then identify the protector to use, in this line I have chosen the **–PasswordProtector** and then used the **–Password** properties with the **$secpwd** variable to identify the secure password.

The final line in the script adds a 2nd protector to volume p: using the CMDLET **ADD-BITLOCKERKEYPROTECTOR** the protector I am adding is the ADAcountOrGroup Protector we use the **-ADAcountOrGroupProtector** property to specify the protector and the –**ADAccountOrGroup** property is then used to define the user or group that is linked to this protector, you will notice that I have used a SID instead of a domain\user combination, the SID is the SID of the Cluster Account. I obtained this by identifying the Cluster account name and then using the using the **Get-ADComputer *clusteraccountname***CMDLET on the domain controller. We have to use the Cluster account SID for this protector so that all members of the cluster can decrypt the BitLocker protected drive.

All that remains is to add the now protected disk to the failover cluster.

One other useful command is the Get-BitlockerVolume command we can use this to see the current status of our protected volumes.



```
PS C:\> Get-BitLockerVolume p:


   ComputerName: HOSTSERVER1

VolumeType      Mount CapacityGB VolumeStatus           Encryption KeyProtector              AutoUnlock Protection
                Point                                   Percentage                           Enabled    Status
----------      ----- ---------- ------------           ---------- ------------              ---------- ----------
Data            P:          9.97 FullyEncrypted         100        {Password, AdAccountOr... False      On


PS C:\> |
```

Group Policy Object Migration Tables

Any candidate that wants to be successful on the 70-411 exam must be comfortable working with Group Policy Objects. Part of that process is the Export and Import and Backup and Restore of Group Policy Objects.

The Group Policy Object migration table is used during the import of a GPO or when you copy a GPO from one domain or forest to another.

The key challenge when migrating Group Policy objects (GPOs) from one domain or forest to another is that some information in the GPO is actually specific to the domain or forest where the GPO is defined. When transferring the GPO to a new domain or forest, it may not always be desirable, or even possible, to use the same settings. You can use a migration table to reference users, groups, computers, and UNC paths in the source GPO to new values in the destination GPO.

You can create migration tables using the Migration Table Editor.

Follow the link below to read a TechNet article on how to populate a Migration table from a Group Policy Object

https://technet.microsoft.com/en-us/library/cc771963.aspx

And the link below has information on creating a Migration Table

https://technet.microsoft.com/en-us/library/cc771452.aspx

Group Policy Object PowerShell CMDLets

It is also vitally important that you learn how to manage GPOs from PowerShell

CMDLET	Description
Backup-GPO	Backs up one GPO or all the GPOs in a domain.
Copy-GPO	Copies a GPO
Import-GPO	Imports the Group Policy settings from a backed-up GPO into a specified GPO
Invoke-GPUPDATE	Updates Group Policy on a local computer or remote computer.
New-GPLink	Links a GPO to a site, domain, or OU.
New-GPO	Used to Create a New GPO.

Set-GPInheritance	Blocks or unblocks inheritance for a specified domain or OU
Set-GPPermission	Grants a level of permissions to a security principal for one GPO or for all the GPOs in a domain
Set-GPLink	Sets the properties of the specified GPO link

The table above shows some of the most common GPO CMDLets.

NEW-GPO Examples

Example 1

```
New-GPO -Name TestGPO -comment "This is a test GPO."
```

Example 2

```
New-GPO -Name FromStarterGPO -StarterGPOName "Windows Vista EC Computer Starter GPO"
```

Example 3

```
New-gpo -name TestGPO | new-gplink -target "ou=marketing,dc=contoso,dc=com" | set-gppermissions -permissionlevel gpoedit -targetname "Marketing Admins" -targettype group
```

Example 1 create a new GPO called TestGPO and gives it a description

Example 2 creates a new GPO called FromStarterGPO and basis it on a starter GPO "Windows Vista EC Computer Starter GPO"

Example 3 creates a new GPO called TestGPO and then pipes that to the NEW-GPLINK cmdlets that links the new GPO to the Marketing OU then a pipe is used to pass the GPO to the set-gppermissions CMDLet where the GPOEDIT permission is assigned to the group “Marketing Admins”

SET-GPINHERITANCE Examples

Example 1

```
Set-GPinheritance -Target "ou=MyOU,dc=contoso,dc=com" -IsBlocked Yes
```

Example 2

```
Set-GPinheritance -Target "ou=MyOU,dc=contoso,dc=com" -IsBlocked No
```

Example 1 targets an OU called MyOU and blocks inheritance

Example 2 targets an OU called MyOU and un-blocks inheritance

Examples of all the GPO CMDLets can be found at the link below:

https://technet.microsoft.com/en-us/library/ee461027.aspx

DFS replication Improvement in Windows Server 2012

The following TechNet article gives an overview of the DFS replication improvements introduced in Windows Server 2012:

http://blogs.technet.com/b/filecab/archive/2012/11/12/dfs-replication-improvements-in-windows-server-2012.aspx

Update improvements in Windows Server 2012

The Following Channel 9 Video covers improvements to WSUS and the new Cluster Aware Updating feature in Windows Server 2012.

https://channel9.msdn.com/events/teched/northamerica/2012/wsv322

Auditpol.exe

For information on Auditpol.exe follow the link below:

https://technet.microsoft.com/en-us/library/cc731451.aspx

Day 7

The Morning of day 7 is about review and the 70-411 and getting ready for the exam at around 10:30AM

Configuring Advanced Windows Server 2012 Services

Dynamic Access Control

I think to understand Dynamic Access Control (DAC) we should break it down in to its component parts. If we can identify what components are needed and what order they should be created it should lead to a better understanding of the technology.

The goal of DAC is to give us control of who can access our resources in a more granular way than we can achieve with Share and NTFS permissions alone. For instance let’s say we have a Sales report called “Sales Report 1” and you want to give access to the report but only if a user is a member of the Sales department and his Manager is BOB. We can’t do this with NTFS permissions alone, but with DAC it is a relatively simple thing. For the remainder of this document we will be using the above problem as an example to illustrate what DAC can do for us. If you want to run through the following steps make sure you have a Folder on c: called Sales reports that contains a file called Sales Report 1.

Components of DAC

Resource Properties – These are used to classify files and folders so that file management tasks can be run against them or so DAC can use the properties to Target Resources. There is a list of default properties most of which are disabled

Resource Property Lists – These are Lists of properties that can be consumed by Applications, there is a default property list that contains all properties.

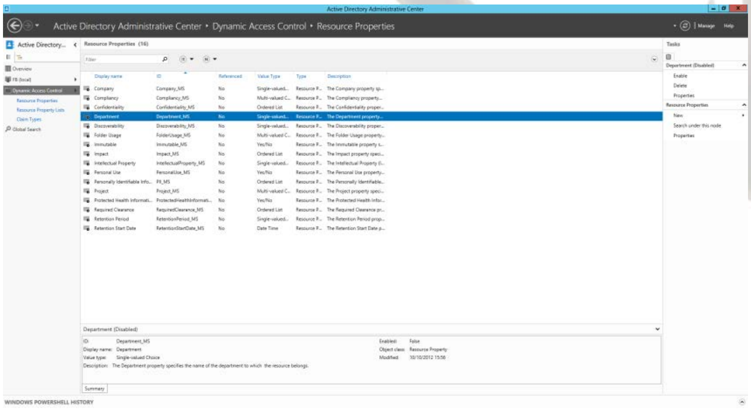
Claim Types – As Microsoft administrators we are used to providing access to our resources based on the information inside access tokens. This would typically be users SIDs and Group SIDs but there is a wealth of other information that can be used, if you look at an average user account and take a look at the organisation tab for example you can see properties for Department, Manager, Job title etc. then there are all the other properties on all the other tabs plus you can create custom attributes. All of this information can be used in Claims. So if we can record in the Users access token his user and group SID's and also his department and his manager then we can make access decisions based on any of those claims.

Central Access Rule – a Central Access Rule is a rule that will provide access to a resource or audit access to a resource based on claims and optionally Resource Properties

Central Access Policies – are groupings of Central Access Rules, we can then reference a Central Access Policy in a GPO to make it available for use.

1) Resource Properties and File Classifications

Although file classification isn't required to implement DAC it is one of its most powerful features. We will start with creating Resource Properties and then use FSRM to apply classifications based on those properties to a collection of files.



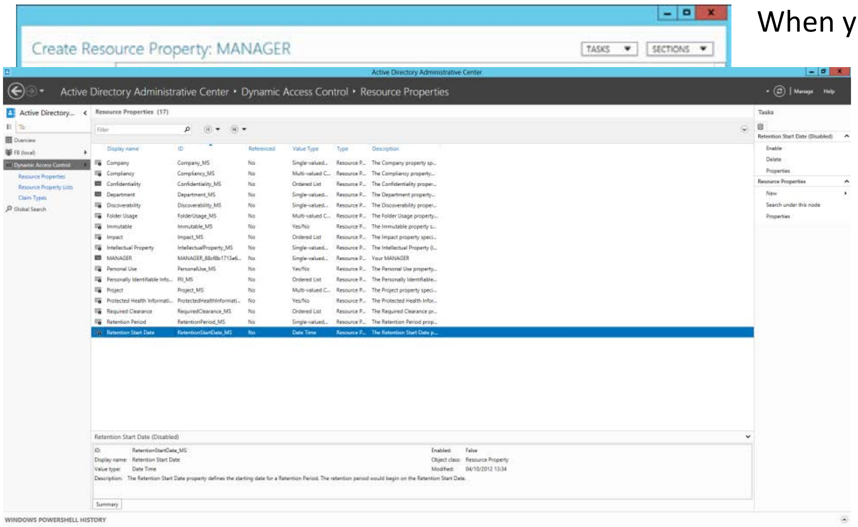
Resource Properties (16)

Display name	ID	Referenced	Value Type	Type	Description
Company	Company_MS	No	Single-valued...	Resource P...	The Company property sp...
Compliancy	Compliancy_MS	No	Multi-valued C...	Resource P...	The Compliancy property...
Confidentiality	Confidentiality_MS	No	Ordered List	Resource P...	The Confidentiality proper...
Department	Department_MS	No	Single-valued...	Resource P...	The Department property...
Discoverability	Discoverability_MS	No	Single-valued...	Resource P...	The Discoverability proper...
Folder Usage	FolderUsage_MS	No	Multi-valued C...	Resource P...	The Folder Usage property...
Immutable	Immutable_MS	No	Yes/No	Resource P...	The Immutable property s...
Impact	Impact_MS	No	Ordered List	Resource P...	The Impact property speci...
Intellectual Property	IntellectualProperty_MS	No	Single-valued...	Resource P...	The Intellectual Property (I...
Personal Use	PersonalUse_MS	No	Yes/No	Resource P...	The Personal Use property...
Personally Identifiable Info...	PII_MS	No	Ordered List	Resource P...	The Personally Identifiable...
Project	Project_MS	No	Multi-valued C...	Resource P...	The Project property speci...
Protected Health Informati...	ProtectedHealthInformati...	No	Yes/No	Resource P...	The Protected Health Infor...
Required Clearance	RequiredClearance_MS	No	Ordered List	Resource P...	The Required Clearance pr...
Retention Period	RetentionPeriod_MS	No	Single-valued...	Resource P...	The Retention Period prop...
Retention Start Date	RetentionStartDate_MS	No	Date Time	Resource P...	The Retention Start Date p...

Department (Disabled)

ID: Department_MS
Display name: Department
Value type: Single-valued Choice
Description: The Department property specifies the name of the department to which the resource belongs.
Enabled: False
Object class: Resource Property
Modified: 10/10/2012 15:58

The Active Directory Administrative centre is where we manage DAC components. If you select Dynamic Access control you can then select resource properties, and you should see a list like the one on the left there. Here we can see all of our resource properties, we can edit existing properties and enable and disable properties. We can also see that from the task menu we can choose to create a new resource property. And that is what we will do.



Create Resource Property: MANAGER

Resource Properties (17)

Display name	ID	Referenced	Value Type	Type	Description
Company	Company_MS	No	Single-valued...	Resource P...	The Company property sp...
Compliancy	Compliancy_MS	No	Multi-valued C...	Resource P...	The Compliancy property...
Confidentiality	Confidentiality_MS	No	Ordered List	Resource P...	The Confidentiality proper...
Department	Department_MS	No	Single-valued...	Resource P...	The Department property...
Discoverability	Discoverability_MS	No	Single-valued...	Resource P...	The Discoverability proper...
Folder Usage	FolderUsage_MS	No	Multi-valued C...	Resource P...	The Folder Usage property...
Immutable	Immutable_MS	No	Yes/No	Resource P...	The Immutable property s...
Impact	Impact_MS	No	Ordered List	Resource P...	The Impact property speci...
Intellectual Property	IntellectualProperty_MS	No	Single-valued...	Resource P...	The Intellectual Property (I...
MANAGER	MANAGER_88cf8b1713e6...	No	Single-valued...	Resource P...	Your MANAGER
Personal Use	PersonalUse_MS	No	Yes/No	Resource P...	The Personal Use property...
Personally Identifiable Info...	PII_MS	No	Ordered List	Resource P...	The Personally Identifiable...
Project	Project_MS	No	Multi-valued C...	Resource P...	The Project property speci...
Protected Health Informati...	ProtectedHealthInformati...	No	Yes/No	Resource P...	The Protected Health Infor...
Required Clearance	RequiredClearance_MS	No	Ordered List	Resource P...	The Required Clearance pr...
Retention Period	RetentionPeriod_MS	No	Single-valued...	Resource P...	The Retention Period prop...
Retention Start Date	RetentionStartDate_MS	No	Date Time	Resource P...	The Retention Start Date p...

Retention Start Date (Disabled)

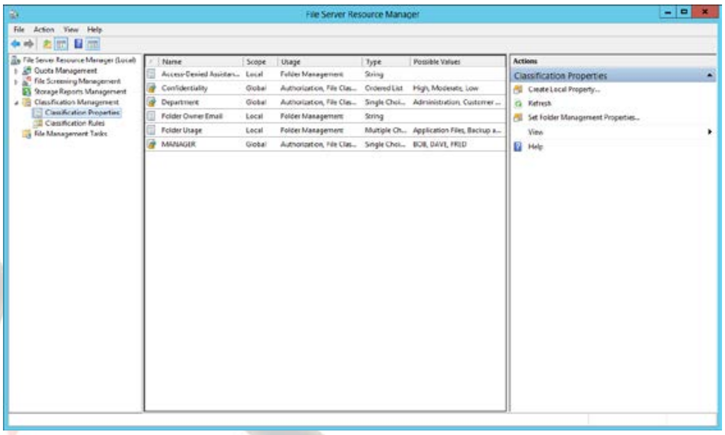
ID: RetentionStartDate_MS
Display name: Retention Start Date
Value type: Date Time
Description: The Retention Start Date property defines the starting date for a Retention Period. The retention period would begin on the Retention Start Date.
Enabled: False
Object class: Resource Property
Modified: 04/10/2012 13:34

When you open the Create Resource Property Screen you can name the property and select its type. I have called my new property **MANAGER** and the type as **Single-**

value Choice. You can also see from here that we can add some suggested values, if you do then they will be available as choices when the property is applied. I have added three people who are managers in our organisation BOB, DAVE and FRED. Once you have completed the Property say ok and it should be added to the list of properties.

Here you can see our **MANAGER** property and that it is enabled, also notice that I have enabled two of the default properties, Department and Confidentiality.

Now that we have created and enabled some properties they will be made available through features like FSRM.

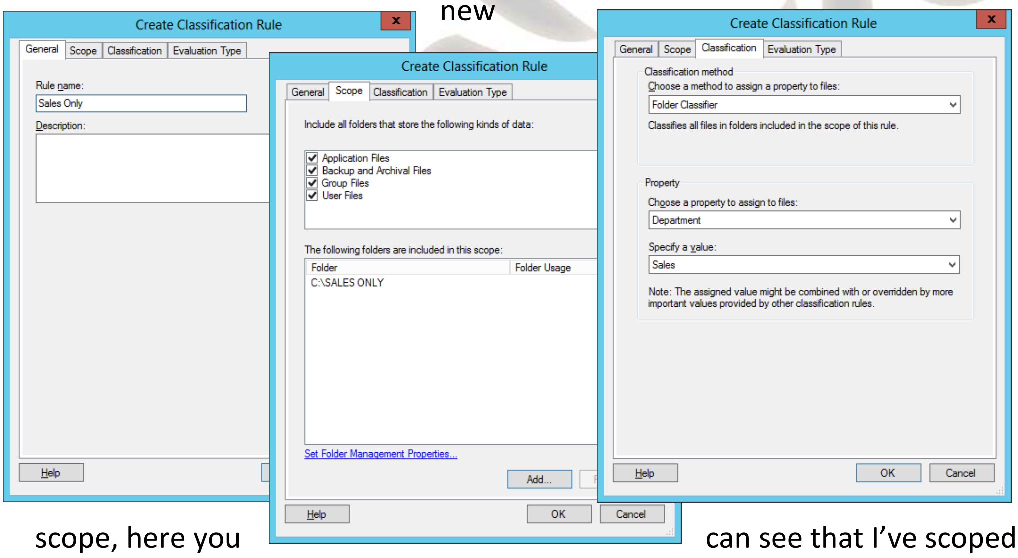


File Server Resource Manager

File Action View Help
File Server Resource Manager (Local)
Quota Management
File Screening Management
Storage Reports Management
Classification Management
Classification Properties
Classification Rules
File Management Tasks
Actions
Classification Properties
Create Local Property...
Refresh
Set Folder Management Properties...
View
Help

Name	Scope	Usage	Type	Possible Values
Access-Denied Assistan...	Local	Folder Management	String	
Confidentiality	Global	Authorization, File Clas...	Ordered List	High, Moderate, Low
Department	Global	Authorization, File Clas...	Single Choi...	Administration, Customer ...
Folder Owner Email	Local	Folder Management	String	
Folder Usage	Local	Folder Management	Multiple Ch...	Application Files, Backup a...
MANAGER	Global	Authorization, File Clas...	Single Choi...	BOB, DAVE, FRED

Here you can see that our newly created MANAGER property and the newly enabled default properties are available for use through the FSRM console (you may have to refresh the screen in order to view the new properties), we can use them here when we create classification rules and they will also be available for users when they perform manual classification. We are going to use a classification rule to classify files in a folder called Sales Only as belonging to the SALES department. If you select Classification rules you should be able to select create new classification rule.



Create Classification Rule

General Scope Classification Evaluation Type

Rule name: Sales Only

Description:

Create Classification Rule

General Scope Classification Evaluation Type

Include all folders that store the following kinds of data:

☑ Application Files
☑ Backup and Archival Files
☑ Group Files
☑ User Files

The following folders are included in this scope:

Folder	Folder Usage
C:\SALES ONLY	

Set Folder Management Properties...
Add...
Help OK Cancel

Create Classification Rule

General Scope Classification Evaluation Type

Classification method

Choose a method to assign a property to files: Folder Classifier

Classifies all files in folders included in the scope of this rule.

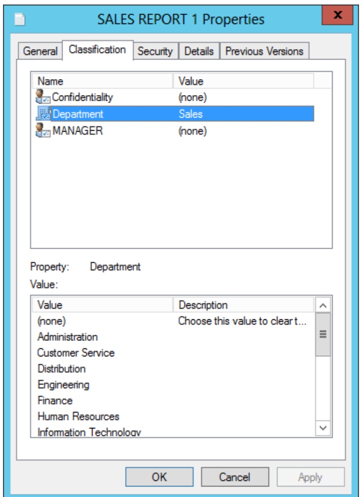
Property

Choose a property to assign to files: Department

Specify a value: Sales

Note: The assigned value might be combined with or overridden by more important values provided by other classification rules.

When the Wizard starts you can give your new rule a name, select the type of files it will apply to and crucially choose a scope, here you can see that I've scoped it to a folder c:\SALES ONLY. On the Classifications tab you can choose the classification Method, for this example I selected **Folder Classifier** and then I choose a property of **Department** and a value of **Sales**.



SALES REPORT 1 Properties

Name	Value
Confidentiality	(none)
Department	Sales
MANAGER	(none)

Property: Department

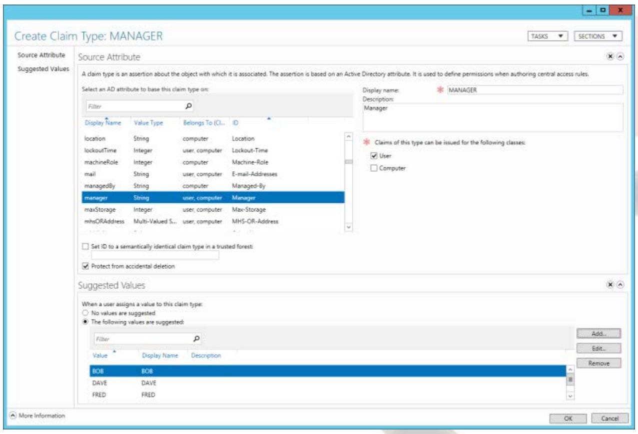
Value:

Value	Description
(none)	Choose this value to clear t...
Administration	
Customer Service	
Distribution	
Engineering	
Finance	
Human Resources	
Information Technology	

Classifications run on a schedule or you can run a classification automatically, once you have created your classification rule you could choose to run classification now. A report will be generated confirming that the files have been classified. If you want to further confirm you can go to the file and access its file classification tab to view the new classifications

2) Claims, Access Rules and Central Access Policies

The next part of a DAC deployment is creating Claims; remember a claim is something that is made against an object. So a claim might be that bob belongs to the Sales Department or the BOB is a Manager or that BOB is both in the Sales Department and a Manager. Claims are added to a user's access token and then presented when the user wants to gain access to a resource. Claims can be user of computer claims and are linked to a property of the User of Computer object.



Source Attribute

A claim type is an assertion about the object with which it is associated. The assertion is based on an Active Directory attribute. It is used to define permissions when authoring central access rules.

Select an AD attribute to base this claim type on:

Display Name	Value Type	Belongs To (Cl...	ID
location	String	computer	Location
lockoutTime	Integer	user, computer	Lockout-Time
machineRole	Integer	computer	Machine-Role
mail	String	user, computer	E-mail-Addresses
managedBy	String	computer	Managed-By
manager	String	user, computer	Manager
maxStorage	Integer	user, computer	Max-Storage
mhsORAddress	Multi-Valued S...	user, computer	MHS-OR-Address

Display name: * MANAGER
Description: Manager

* Claims of this type can be issued for the following classes:
☑ User
☐ Computer

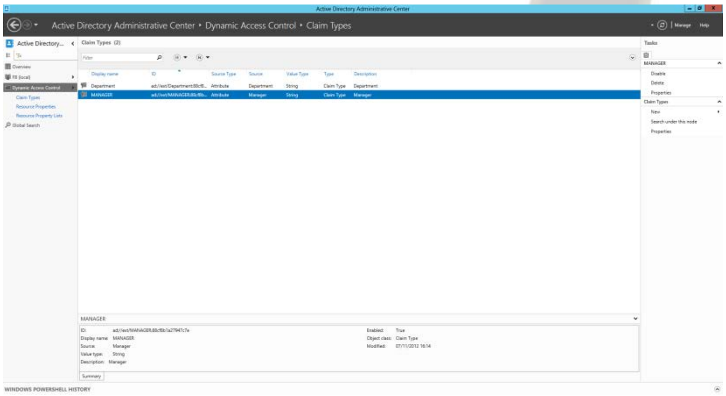
☐ Set ID to a semantically identical claim type in a trusted forest:
☑ Protect from accidental deletion

Suggested Values

When a user assigns a value to this claim type:
○ No values are suggested
● The following values are suggested:

Value	Display Name	Description
BOB	BOB	
DAVE	DAVE	
FRED	FRED	

Back in Active Directory Administrative Centre we can select Dynamic Access Control and select Claims Types, the list should be empty so under tasks choose new claim type. The first thing to do is select whether this will be a user or computer claim. Then select a name and an optional description for your claim. We then choose an attribute to match our new claim against. I kept things simple and created a User Claim called Manager and linked it to the Manager attribute from the attribute list by selecting the Manage attribute. Finally you can offer up some suggested values so that when this claim is used people can select from a list.



Claim Types (2)

Display name	ID	Source Type	Source	Value Type	Type	Description
Department	ad://ext/Department:88cf8...	Attribute	Department	String	Claim Type	Department
MANAGER	ad://ext/MANAGER:88cf8b...	Attribute	Manager	String	Claim Type	Manager

MANAGER

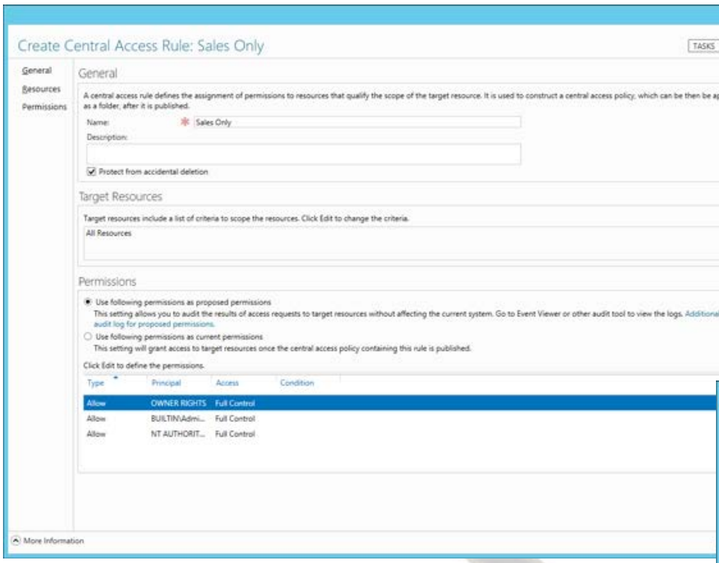
ID: ad://ext/MANAGER:88cf8b1a27947c7e
Display name: MANAGER
Source: Manager
Value type: String
Description: Manager
Enabled: True
Object class: Claim Type
Modified: 07/11/2012 16:14

Here you can see our new Claim has been added to the list of claims. Also I have created a second claim called Department

Once you have claims in pace you can then create Access Rules that will use the Claims to help set permissions. Use DAC to access the Central Access Rule list. Again there won't be any the default rules but we can start creating are own.

When you create and Access rule you must ask yourself a few questions

a. Will this rule enforce permissions or just audit existing permissions and access to a resource
b. Will we target this Access rule at a particular resource property so it will only apply to files and folders that have a particular property set or leave the Access Rule at its default which is All Resources
c. If you are going to enforce your Permissions what will they be and what claims will they use.



Create Central Access Rule: Sales Only

General

A central access rule defines the assignment of permissions to resources that qualify the scope of the target resource. It is used to construct a central access policy, which can be then be applied on a resource, such as a folder, after it is published.

Name: * Sales Only

Description:

☑ Protect from accidental deletion

Target Resources

Target resources include a list of criteria to scope the resources. Click Edit to change the criteria.

All Resources

Permissions

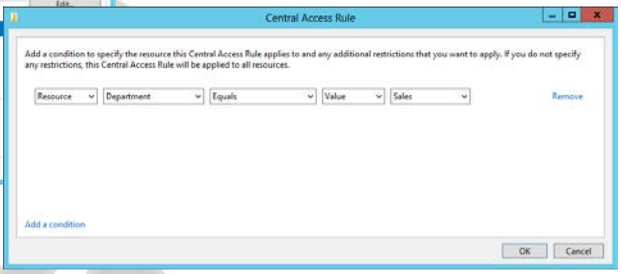
● Use following permissions as proposed permissions
This setting allows you to audit the results of access requests to target resources without affecting the current system. Go to Event Viewer or other audit tool to view the logs. Additional instructions to turn on the audit log for proposed permissions.

○ Use following permissions as current permissions
This setting will grant access to target resources once the central access policy containing this rule is published.

Click Edit to define the permissions.

Type	Principal	Access	Condition
Allow	OWNER RIGHTS	Full Control	
Allow	BUILTIN\Admi...	Full Control	
Allow	NT AUTHORIT...	Full Control	

Here we have a new access rule that I have Named Sales Only, the next thing to do is edit the target resource because I only want this Access Rule to apply when a Files Classification is set to SALES

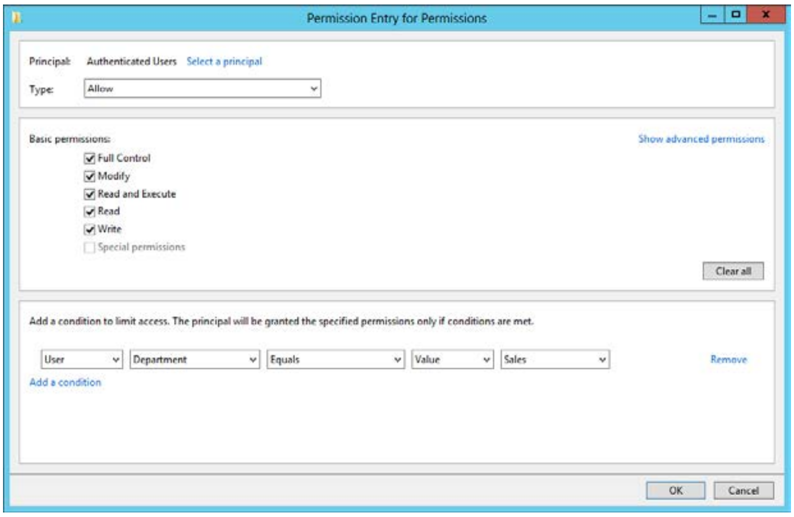


Central Access Rule

Add a condition to specify the resource this Central Access Rule applies to and any additional restrictions that you want to apply. If you do not specify any restrictions, this Central Access Rule will be applied to all resources.

Resource | Department | Equals | Value | Sales

Once you have created a new target resource of Department equals a value of Sales you can turn your attention to the Permission section. Here you will find two radio buttons, the first (and default) is **use the following permissions as proposed permissions**. This is what you select when you want to Audit access to a resource. If you want to enforce new permissions you select **Use the following permissions as current permission** radio button. This is what I selected for this example to work. Now we can edit the permission. I started off by removing all of the default permissions and then adding new ones that I want to apply to the resource.



Permission Entry for Permissions

Principal: Authenticated Users Select a principal

Type: Allow

Basic permissions:

☑ Full Control
☑ Modify
☑ Read and Execute
☑ Read
☑ Write
□ Special permissions

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

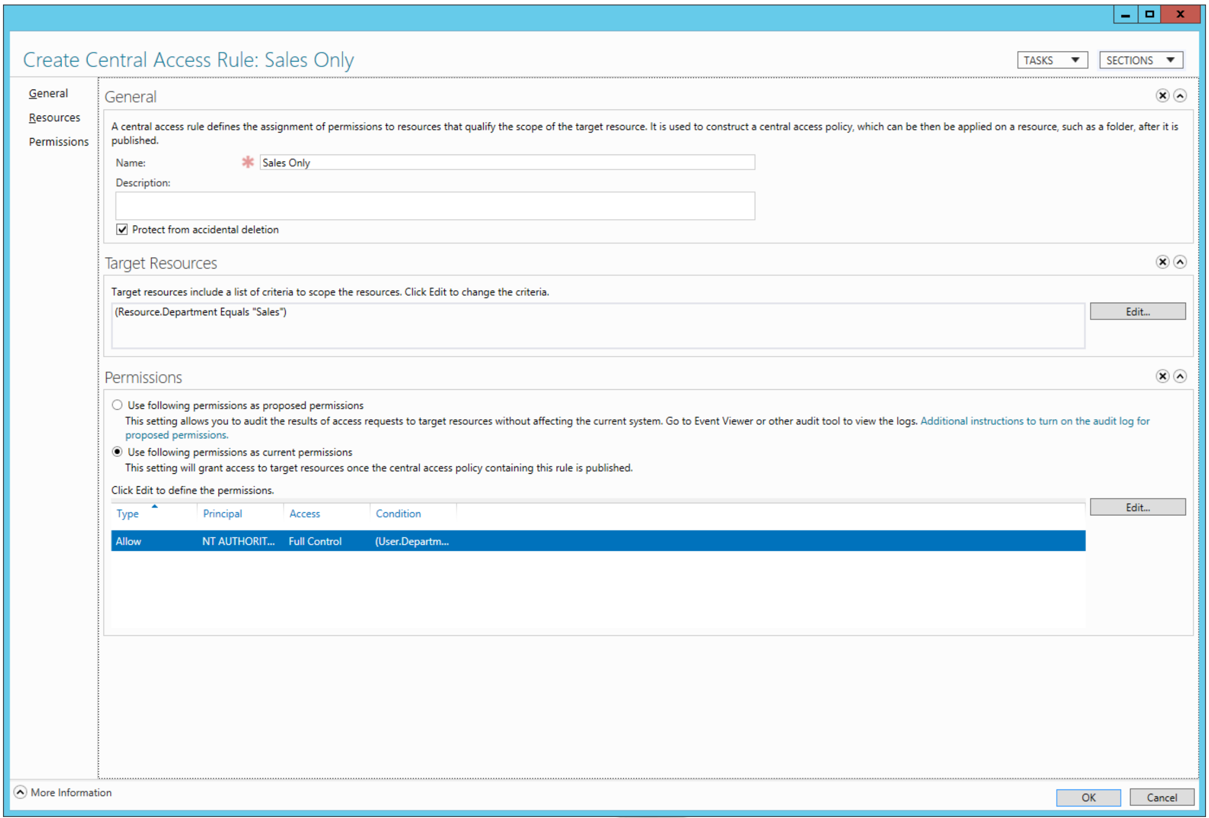
User | Department | Equals | Value | Sales

Here we can see the Permissions entry screen, I've selected authenticated Users as the group I want to give Full control to but <u>only</u> if they meet **the Condition User, Department, Equals, Value, Sales**

The user section refers to user claims, I could have picked Computer there but I haven't configured any. The next box allows us to choose what user claim, here I could have picked Manager, other than Equals we have things like does not equal as well. Then the value Sales is one of the suggested values I added to my claim.

Once completed our Access rule should look like the one above.

As part of the exercise I also created an Access rule Called Manager BOB that allows Full control if the Authenticated users manager is BOB. Everything else remained the same in my 2nd Access rule



Create Central Access Rule: Sales Only

General

A central access rule defines the assignment of permissions to resources that qualify the scope of the target resource. It is used to construct a central access policy, which can be then be applied on a resource, such as a folder, after it is published.

Name: * Sales Only

Description:

☑ Protect from accidental deletion

Target Resources

Target resources include a list of criteria to scope the resources. Click Edit to change the criteria.

(Resource.Department Equals "Sales")

Permissions

○ Use following permissions as proposed permissions

This setting allows you to audit the results of access requests to target resources without affecting the current system. Go to Event Viewer or other audit tool to view the logs. Additional instructions to turn on the audit log for proposed permissions.

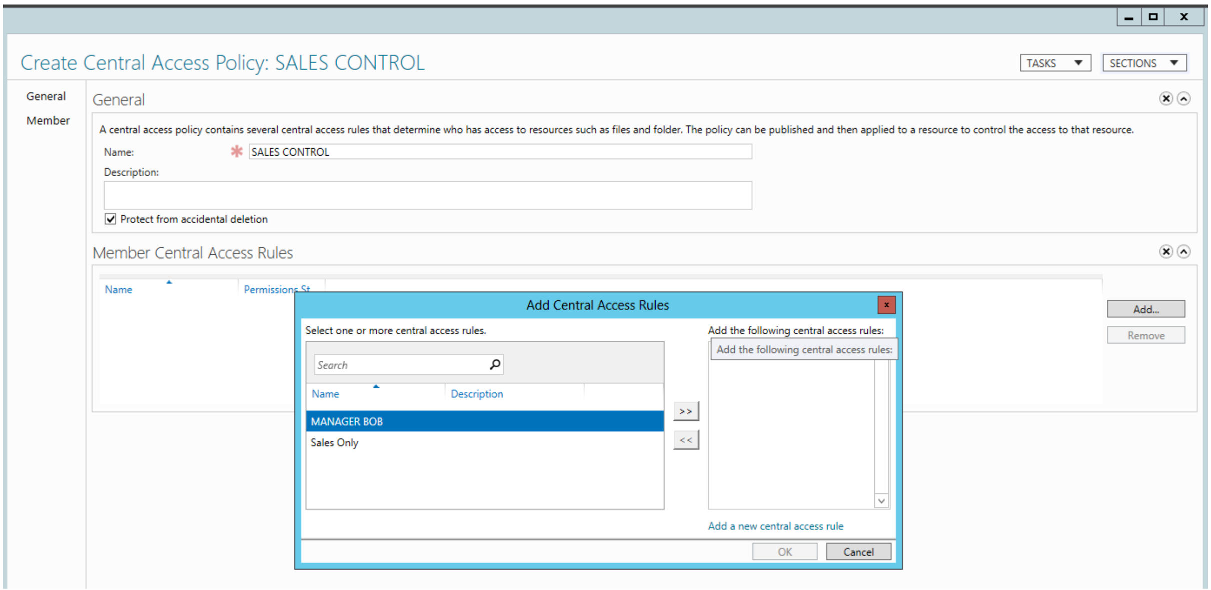
● Use following permissions as current permissions

This setting will grant access to target resources once the central access policy containing this rule is published.

Click Edit to define the permissions.

Type	Principal	Access	Condition
Allow	NT AUTHORIT...	Full Control	(User.Departm...

Once we have Access rules in place we can then move on to create a Central Access Policy. A Central Access Policy will allow us to group together several Access Rules that can then be distributed using a GPO.



Create Central Access Policy: SALES CONTROL

General

A central access policy contains several central access rules that determine who has access to resources such as files and folder. The policy can be published and then applied to a resource to control the access to that resource.

Name: SALES CONTROL

Description:

☑ Protect from accidental deletion

Member Central Access Rules

Add Central Access Rules

Select one or more central access rules.

Name	Description
MANAGER BOB	
Sales Only	

Add the following central access rules:

Use DAC to access the Central Access Policy List and then from the task menu choose to create a new Central Access policy. I have named mine Sales Control and have added my two previously created Access Rules.

You can link several Central Access Policies to a GPO.

It’s always worth keeping in mind the order that things are gone through DAC

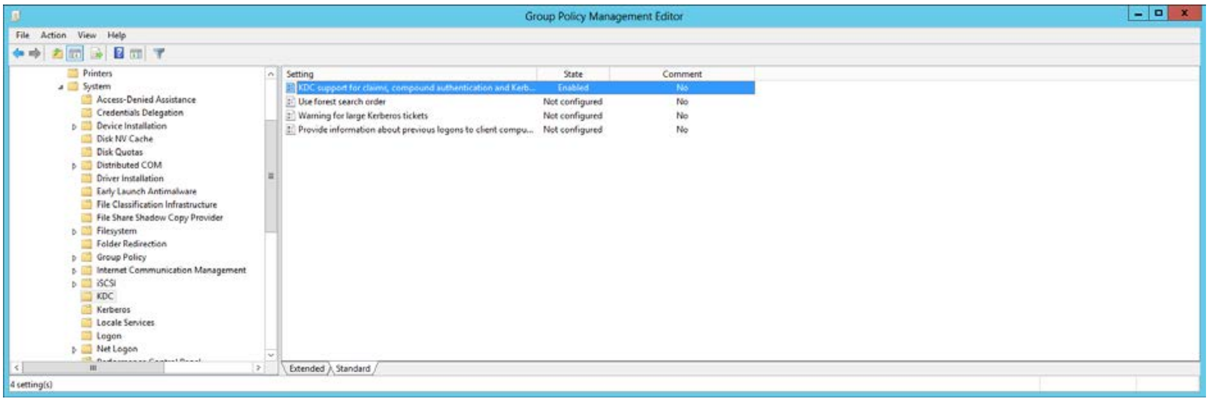
1) We create Claims
2) We Create Access Rules
3) We Create Central Access policies
4) We Create/Edit GPOS
5) We apply Central Access policies to files and folders

3) GPO’s, File Settings and testing

We have to change two settings through GPO’s, the first enables Claim based authentication and should probably be set on the default domain Policy unless you need to limit it use. The second policy setting is used to assign a central Access policy to a group of file servers.

GPO SETTING 1 – ENABLE CLAIMS BASED AUTHENTICATION

Computer\Administrative Templates\System\KDC

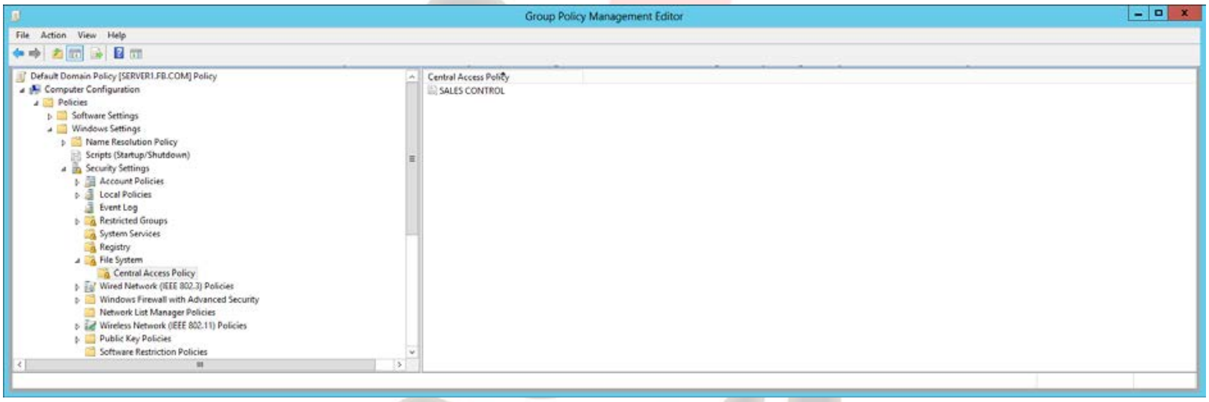


Setting	State	Comment
KDC support for claims, compound authentication and Kerb...	Enabled	No
Use forest search order	Not configured	No
Warning for large Kerberos tickets	Not configured	No
Provide information about previous logons to client compu...	Not configured	No

4 setting(s)

GPO SETTING 2- ASSINGN A CENTRAL ACCESS POLICY THROUGH A GPO

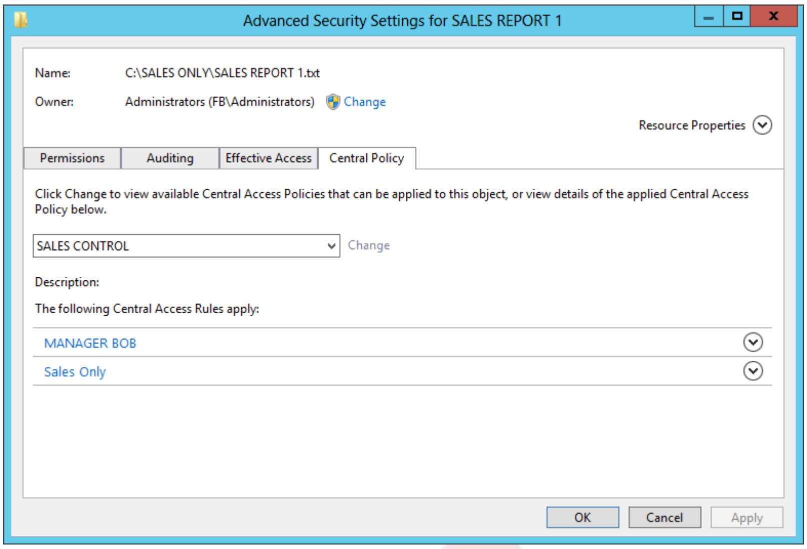
Computer\Windows\Settings\Security\File System


Group Policy Management Editor
File Action View Help
Default Domain Policy [SERVER1.FB.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Central Access Policy
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies

Central Access Policy
SALES CONTROL

Both are computer based settings. Make sure you run GPUPDATE /FORCE or Invoke-GPupdate to refresh GPO settings on the file servers you now want to test the policy on.

If you think back to our classification section, we had applied a classification of Department = Sales to a file call Sales Report 1 that exists in the Sales Only folder. We are now going to apply an access rule to that file.


Advanced Security Settings for SALES REPORT 1

Name: C:\SALES ONLY\SALES REPORT 1.txt

Owner: Administrators (FB\Administrators) Change

Click Change to view available Central Access Policies that can be applied to this object, or view details of the applied Central Access Policy below.

SALES CONTROL

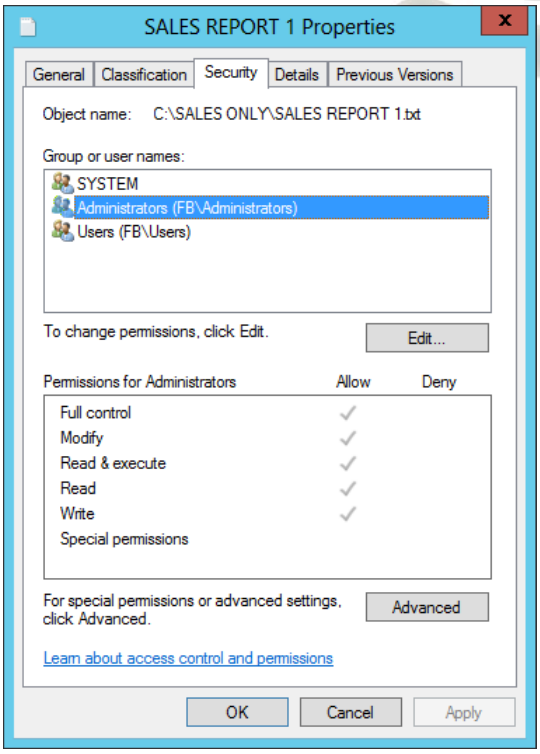
Description:

The following Central Access Rules apply:

MANAGER BOB

Sales Only

This is the Advanced Security Screen of SALES REPORT 1, under the Central Policy tab we can click change and choose our SALES CONTROL central Access Policy. A description of the policy will show you the rules that will be applied. They should include the Sales Only rule that only allows access to Authenticated users who are members of the Sales Department and the Manager BOB rule that only allows access if the Authenticated users Manager is BOB. In an example like this both rules would have to be net in order to gain access so an Authenticated user would have to be a member of the Sales department and have BOB as a manager. Remember these rules will only apply if the Resource is classified as Department = SALES which it does.


SALES REPORT 1 Properties

Object name: C:\SALES ONLY\SALES REPORT 1.txt

Group or user names:

- SYSTEM
- Administrators (FB\Administrators)
- Users (FB\Users)

To change permissions, click Edit.

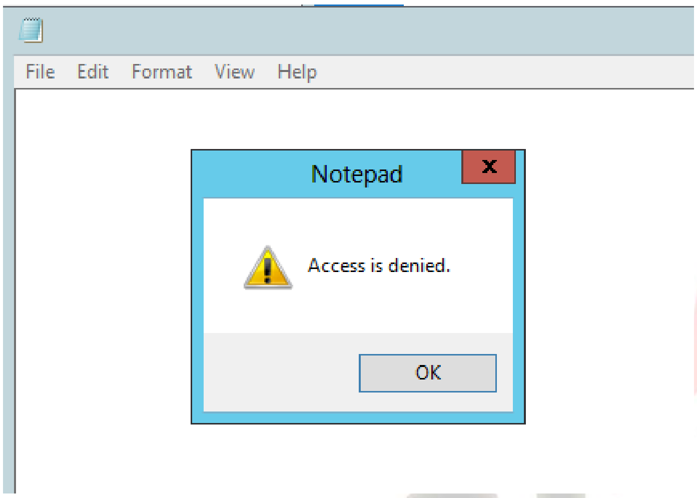
Permissions for Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

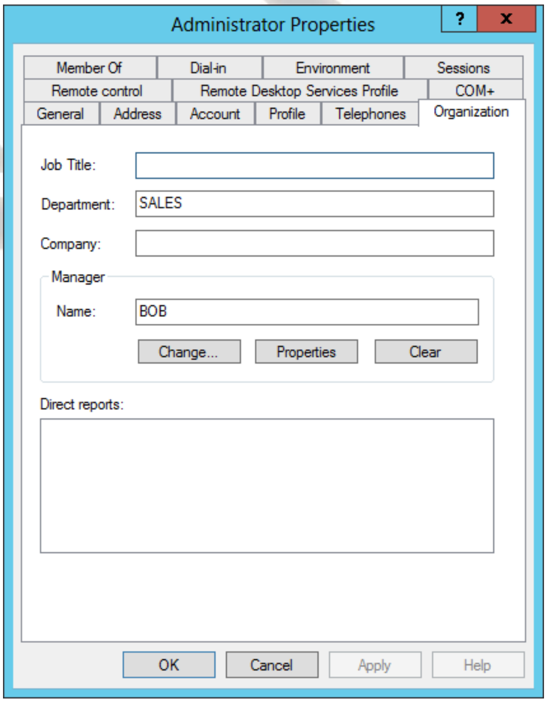
TESTING

Above is the current NTFS permissions of Sales Report 1, they are at their default settings which include Administrators = Full Control. But because the Administrator account is neither a member of the Sales Department or has Bob as a manger when you try to access the document you should receive and access denied message. Like the one below



Access is denied.

For testing I then edited the properties of the Administrator Account and added a department value of SALES and a Manger of BOB (bob has to be a valid AD user)



Job Title:

Department: SALES

Company:

Manager

Name: BOB

Make sure all GPOS have been refreshed and once you have edited your test accounts properties logoff and log back on to make sure your new settings are part of you claim added to you access token.

Now try accessing the Sales Report 1 document and you should have access.

Experiment with removing the classification, what results would you expect?

File and Storage Services

The following Link will take you to a TechNet article on file and storage service:

https://technet.microsoft.com/en-gb/library/hh831487.aspx

IPAM Video

The following link will take you a Virtual Academy video on IPAM in Widows Server 2012R2

https://www.microsoftvirtualacademy.com/en-us/training-courses/windows-server-2012-r2-using-ip-address-management-ipam-8417

Day 8

Windows Server 2012 Hyper-V High Availability and Migration Features

Virtual Machine and Storage Migration

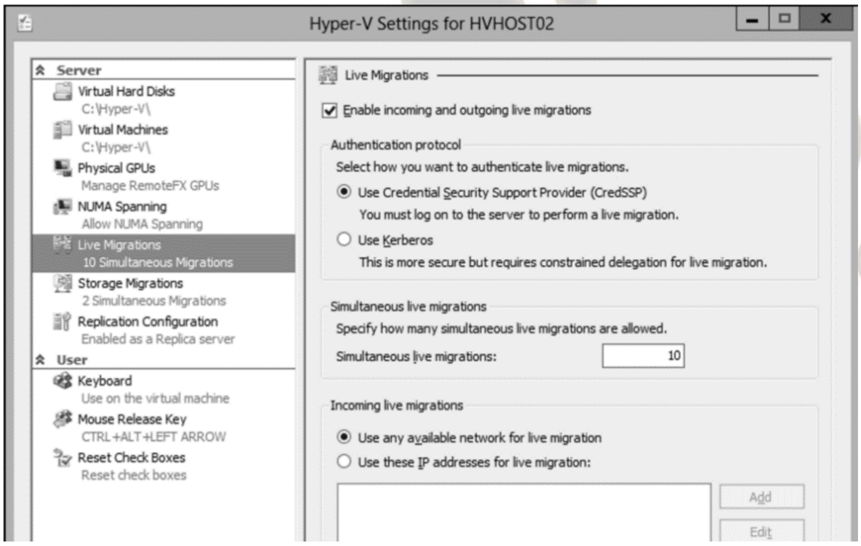
With Windows Server 2012 Microsoft has introduce a new feature that allows you to migrate a running virtual machine and its storage to a new location without first needing to Cluster the Hyper-V host servers. This type of migration is sometimes called shared nothing migration. To enable this type of Migration we need to take two steps.

Step 1 – Enable Live Migration support on a Windows Server 2012 Hyper-V Server

Step 2 – Use the new Move wizard to migrate a Virtual Machine and its Storage

Step 1

If you access Hyper-V Settings on both the Hyper-V host server you wish to migrate to and the Hyper-V host server you wish to replicate from, you will see a screen shot similar to the one below. Here we can see a Hyper-V host Server that has been configured to allow Live Migrations (VM and Storage Migration), we can see the type of authentication that has been configured, how many simultaneous live migrations we will allow and the IP Networks we will allow Live Migration on. Once we have configured the destination server and source server we can then go to the Source VM and use the Move wizard to migrate a VM and its storage.



Hyper-V Settings for HVHOST02

Server
- Virtual Hard Disks
  C:\Hyper-V\
- Virtual Machines
  C:\Hyper-V\
- Physical GPUs
  Manage RemoteFX GPUs
- NUMA Spanning
  Allow NUMA Spanning
- Live Migrations
  10 Simultaneous Migrations
- Storage Migrations
  2 Simultaneous Migrations
- Replication Configuration
  Enabled as a Replica server

User
- Keyboard
  Use on the virtual machine
- Mouse Release Key
  CTRL+ALT+LEFT ARROW
- Reset Check Boxes
  Reset check boxes

Live Migrations

☑ Enable incoming and outgoing live migrations

Authentication protocol
Select how you want to authenticate live migrations.
● Use Credential Security Support Provider (CredSSP)
You must log on to the server to perform a live migration.
○ Use Kerberos
This is more secure but requires constrained delegation for live migration.

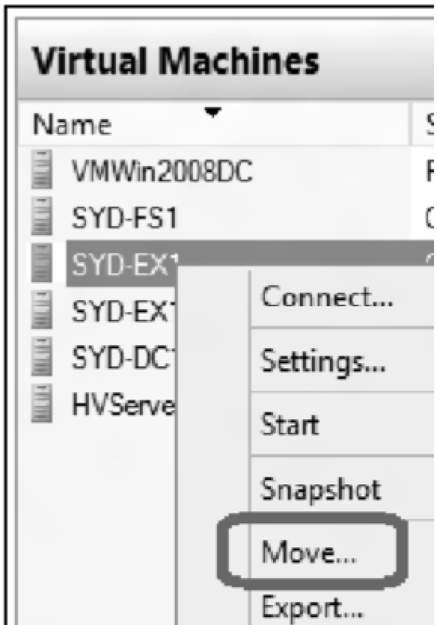
Simultaneous live migrations
Specify how many simultaneous live migrations are allowed.
Simultaneous live migrations: 10

Incoming live migrations
● Use any available network for live migration
○ Use these IP addresses for live migration:

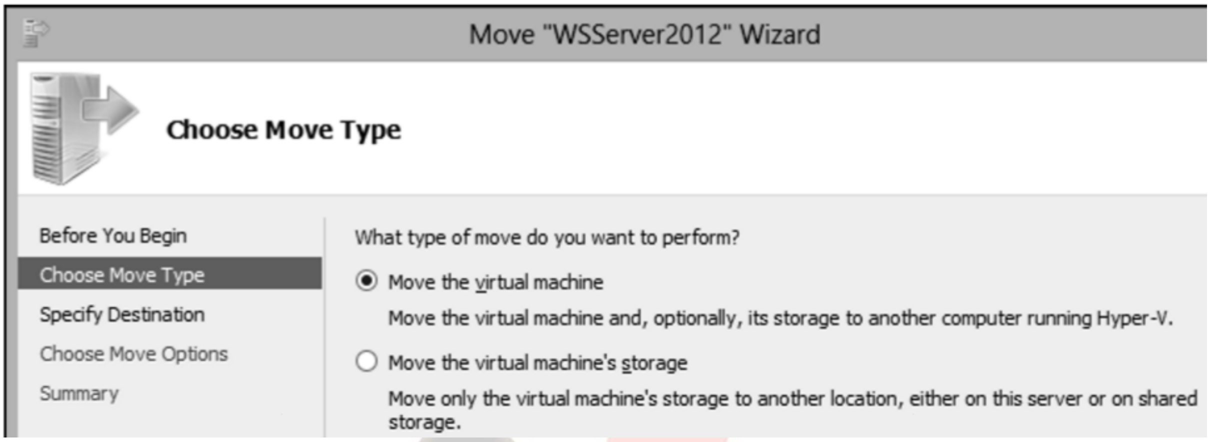
Step 2

The 2nd part of this process involves choosing the virtual machines you wish to Migrate, remember when you choose a Virtual Machine to migrate you can choose to migrate the Virtual Machine and its Storage at the same time or just it's Storage.

Here we have selected a virtual Machine and selected Move.



The next screen we see asks us to choose the move type, here we get to select whether we want to Move the virtual Machines and Optionally its storage to another computer running Hyper-V or just move the Virtual Machines Storage to another location on this or another server.


Move "WSServer2012" Wizard

Choose Move Type

What type of move do you want to perform?

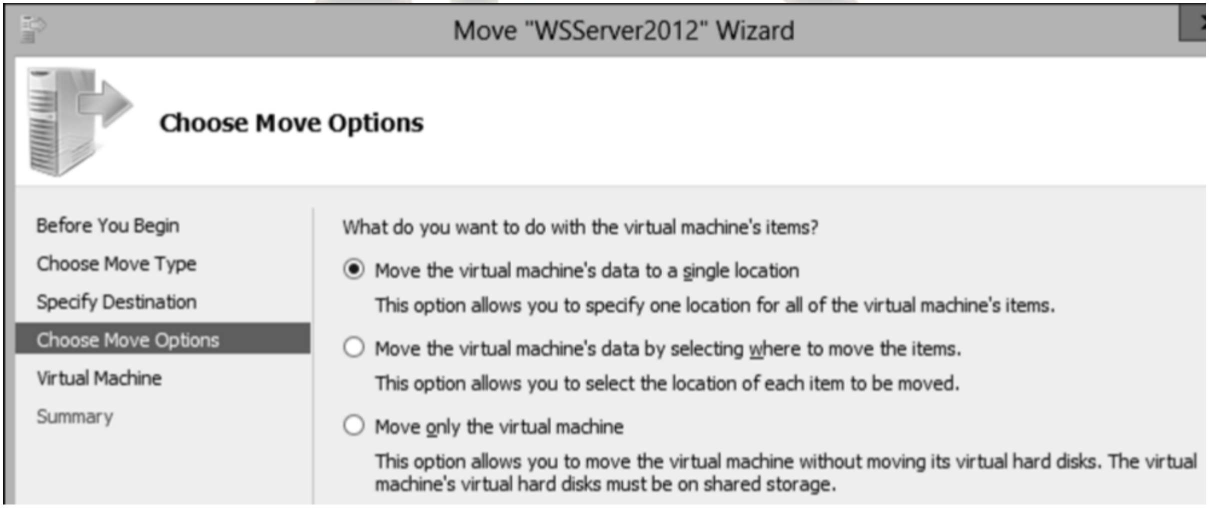
● Move the virtual machine

Move the virtual machine and, optionally, its storage to another computer running Hyper-V.

○ Move the virtual machine's storage

Move only the virtual machine's storage to another location, either on this server or on shared storage.

Once we have chosen an option we are then asked to select a Destination we wish to move the VM or Storage to. We are then asked for Move options, this allows us to choose to move to VM and storage to the same location or to different locations or Move the VM only.


Move "WSServer2012" Wizard

Choose Move Options

What do you want to do with the virtual machine's items?

● Move the virtual machine's data to a single location

This option allows you to specify one location for all of the virtual machine's items.

○ Move the virtual machine's data by selecting where to move the items.

This option allows you to select the location of each item to be moved.

○ Move only the virtual machine

This option allows you to move the virtual machine without moving its virtual hard disks. The virtual machine's virtual hard disks must be on shared storage.

Quick Migration

For the Microsoft exams the term Quick Migration is most likely used to describe the process of Migrating a VM from one node in a cluster to another. For non-clustered VM hosts they will want you to use Virtual Machine and Storage Migration.

When you initiate quick migration, the cluster copies the memory being used by the virtual machine to a disk in storage, so that when the transition to another node actually takes place, the memory and state information needed by the virtual machine can quickly be read from the disk by the node that is taking over ownership. A quick migration can be used for planned maintenance but not for an unplanned failover.

During a Quick Migration there will be down time.

Live Migration

For the Microsoft exams the term Live Migration is most likely used to describe the process of Migrating a VM from one node in a cluster to another. For non-clustered VM hosts they will want you to use Virtual Machine and Storage Migration.

Live migrations are now able to utilize higher network bandwidths (up to 10 Gigabit) to complete migrations faster. You can also perform multiple simultaneous live migrations to enable you to move many virtual machines in a cluster quickly. These changes allow you to implement high levels of mobility and flexibility in private cloud solutions.

You can also perform a live migration of a virtual machine between two non-clustered servers running Hyper-V when you are only using local storage for the virtual machine. (This is sometimes referred to as a "shared nothing" live migration. In this case, the virtual machines storage is mirrored to the destination server over the network, and then the virtual machine is migrated, while it continues to run and provide network services.

When you initiate live migration, the cluster copies the memory being used by the virtual machine from the current node to another node, so that when the transition to the other node actually takes place, the memory and state information is already in place for the virtual machine. The transition is usually fast enough that a client using the virtual machine does not lose the network connection. If you are using Cluster Shared Volumes, live migration is almost instantaneous, because no transfer of disk ownership is needed. A live migration can be used for planned maintenance but not for an unplanned failover.

Hyper-V Replica

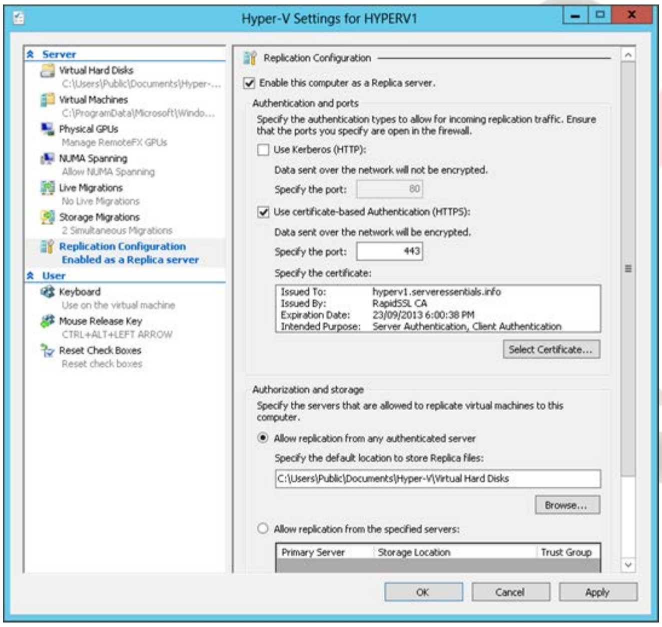
Hyper-V Replica provides asynchronous replication of Hyper-V virtual machines between two hosting servers. It is simple to configure and does not require either shared storage or any particular storage hardware. Any server workload that can be virtualized in Hyper-V can be replicated. Replication works over any ordinary IP-based network, and the replicated data can be encrypted during transmission. Hyper-V Replica works with standalone servers, failover clusters, or a mixture of both. The servers can be physically co-located or widely separated geographically. The physical servers do not need to be in the same domain, or even joined to any domain at all.

Once replication is configured and enabled, an initial copy of data from the primary virtual machines must be sent to the Replica virtual machines. We call this "initial replication" and you can choose to accomplish it directly over the network or by copying the data to a physical device and transporting that to the Replica site.

When replication is underway, changes in the primary virtual machines are transmitted over the network periodically to the Replica virtual machines. The exact frequency varies depending on how long a replication cycle takes to finish (depending in turn on the network throughput, among other things), but generally replication occurs approximately every 5-15 minutes.

You can choose to move operations on any primary virtual machine to its corresponding Replica virtual machine at any time, an action we call “planned failover.” In a planned failover, any un-replicated changes are first copied over to the Replica virtual machine and the primary virtual machine is shut down, so no loss of data occurs. After the planned failover, the Replica virtual machine takes over the workload; to provide similar protection for the virtual machine that is now servicing the workload, you configure “reverse replication” to send changes back to the primary virtual machine (once that comes back online).

If the primary server should fail unexpectedly, perhaps as a result of a major hardware failure or a natural disaster, you can bring up the Replica virtual machines to take over the workload—this is “unplanned failover.” In unplanned failover, there is the possibility of data loss, since there was no opportunity to copy over changes that might not have been replicated yet.



Hyper-V Settings for HYPERV1

Server
- Virtual Hard Disks — C:\Users\Public\Documents\Hyper-...
- Virtual Machines — C:\ProgramData\Microsoft\Windo...
- Physical GPUs — Manage RemoteFX GPUs
- NUMA Spanning — Allow NUMA Spanning
- Live Migrations — No Live Migrations
- Storage Migrations — 2 Simultaneous Migrations
- Replication Configuration — Enabled as a Replica server

User
- Keyboard — Use on the virtual machine
- Mouse Release Key — CTRL+ALT+LEFT ARROW
- Reset Check Boxes — Reset check boxes

Replication Configuration

☑ Enable this computer as a Replica server.

Authentication and ports

Specify the authentication types to allow for incoming replication traffic. Ensure that the ports you specify are open in the firewall.

☐ Use Kerberos (HTTP):

Data sent over the network will not be encrypted.

Specify the port: 80

☑ Use certificate-based Authentication (HTTPS):

Data sent over the network will be encrypted.

Specify the port: 443

Specify the certificate:

Issued To:	hyperv1.serveressentials.info
Issued By:	RapidSSL CA
Expiration Date:	23/09/2013 6:00:38 PM
Intended Purpose:	Server Authentication, Client Authentication

Select Certificate...

Authorization and storage

Specify the servers that are allowed to replicate virtual machines to this computer.

● Allow replication from any authenticated server

Specify the default location to store Replica files:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

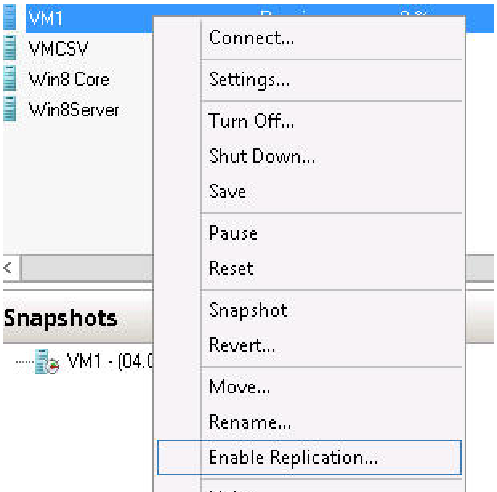
Browse...

○ Allow replication from the specified servers:

Primary Server	Storage Location	Trust Group

OK Cancel Apply

Enabling Hyper-V Replica requires first of all enabling Replication Configuration on the Hyper-V server you wish to replicate to. Here we can see Hyper-V Settings and the Replication Configuration section. Here we can enable this computer as a Replica Server, we can specify the type of authentication you want to use, notice we can user HTTP or HTTPS (HTTPS will require a digital certificate). We must also specify the servers we want to allow replication from.

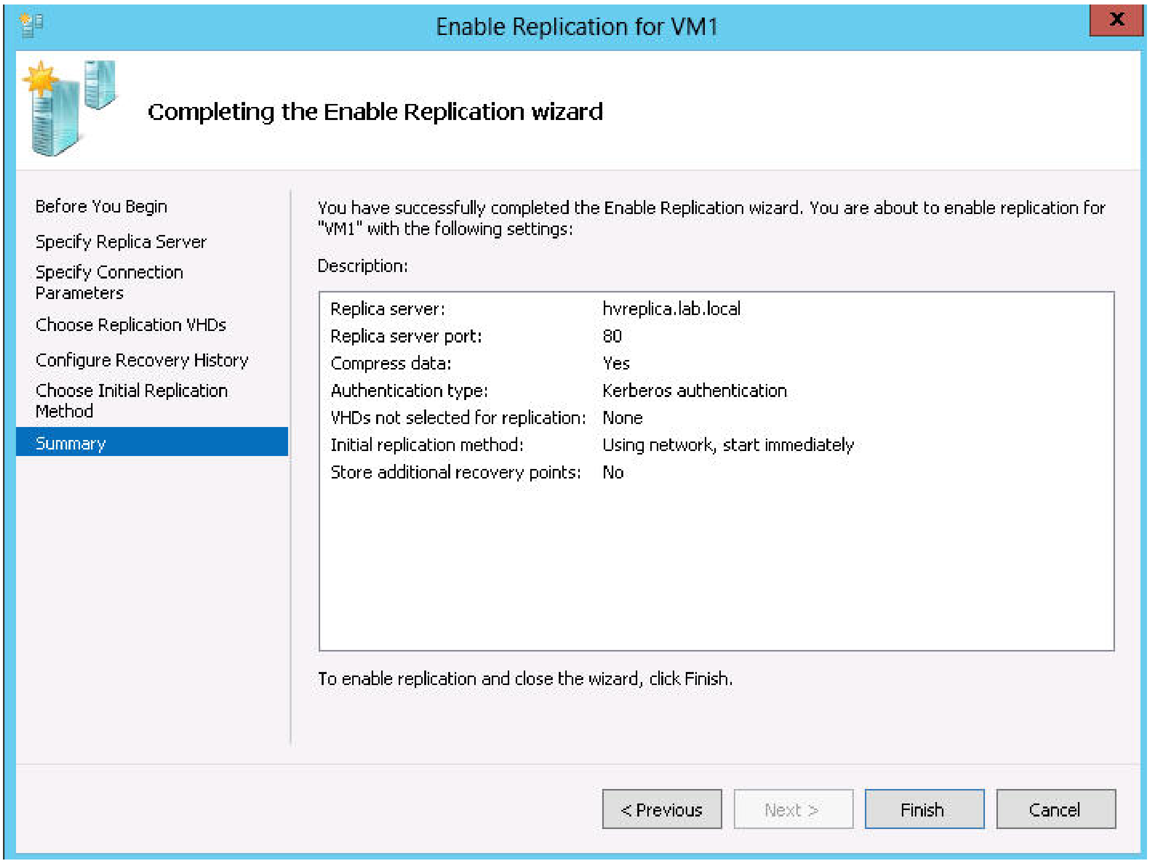


Once we have enabled replication on the destination server we can then choose a VM that we wish to replicate, here I have selected a VM called VM1, right click and you can see an option for Enable

Replication. This will start the replication wizard during which we will be asked

1) Which Server is the Replica Server
2) Specify Ports, Authentication etc.
3) Choose VHD's that I don't want to replicate
4) Choose Recovery Points
5) Choose Initial Replication Method

Finally we will be shown a summary of our choices and when we finish replication can begin.


Enable Replication for VM1
Completing the Enable Replication wizard
Before You Begin
Specify Replica Server
Specify Connection Parameters
Choose Replication VHDs
Configure Recovery History
Choose Initial Replication Method
Summary
< Previous
Next >
Finish
Cancel

You have successfully completed the Enable Replication wizard. You are about to enable replication for "VM1" with the following settings:

Description:

Replica server:	hvreplica.lab.local
Replica server port:	80
Compress data:	Yes
Authentication type:	Kerberos authentication
VHDs not selected for replication:	None
Initial replication method:	Using network, start immediately
Store additional recovery points:	No

To enable replication and close the wizard, click Finish.

Remember that with the introduction of Windows Server 2012 R2, Hyper-V Replica now support the Extended replica feature which allows you to have a 2nd copy of you replica and R2 also introduced the ability to choose a replication interval of 30sec 5mins and 15mins

Import Virtual Machines

Administrators often think of a virtual machine as a single, stand-alone entity that they can move around to address their operational needs. However, a virtual machine consists of several parts, which administrators do not normally need to think about:

- Virtual hard disks, stored as files on the physical storage.

- Virtual machine snapshots, stored as a special type of virtual hard disk file.
- The saved state of the different, host-specific devices.
- The memory file for the virtual machine or its snapshot.
- The virtual machine configuration file, which organizes all of those parts and arranges them into a working virtual machine.

Each virtual machine and every snapshot associated with it must be unique, so globally unique identifiers are used. Additionally, virtual machines store and use some host-specific information, such as the path information for virtual hard disk files. When Hyper-V tries to start a virtual machine, it goes through a series of validation checks before being started. Problems such as hardware differences that might exist when a virtual machine is moved to another host can cause these validation checks to fail. That, in turn, prevents the virtual machine from starting. The administrator is left with files on the disk that take up space and are not useful.

Hyper-V in Windows Server 2012 introduces a new Import wizard that detects and fixes more than 40 different types of incompatibilities. The Import wizard walks you through the steps of addressing incompatibilities when you import the virtual machine to the new host—so this wizard can help with configuration that is associated with physical hardware, such as memory, virtual switches, and virtual processors.

Also, you no longer need to export a virtual machine to be able to import it. You can simply copy a virtual machine and its associated files to the new host, and then use the Import wizard to specify the location of the files. This “registers” the virtual machine with Hyper-V and makes it available for use. You can copy a virtual machine to an NTFS-formatted USB drive, and you can recover virtual machines in cases where the system drive fails but the data drive that stores the virtual machines is intact.

In addition to the new wizard, automation support is available. The new Hyper-V module for Windows PowerShell includes cmdlets for importing virtual machines.

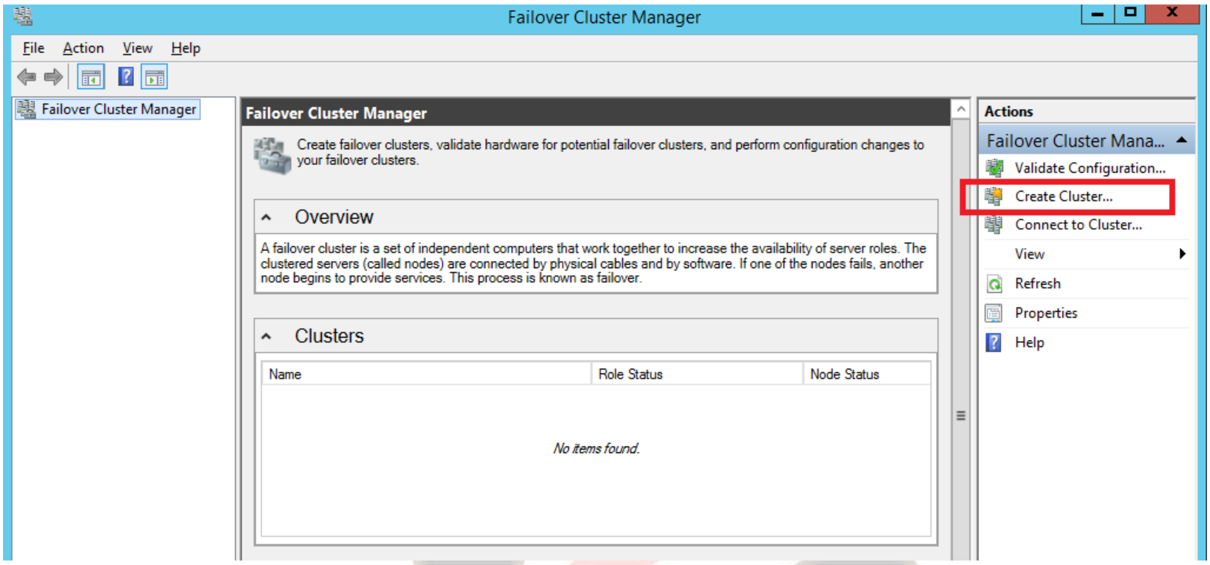
Configuring a Virtual Machine for high availability

https://technet.microsoft.com/en-us/library/dd197474(v=ws.10).aspx

Configuring a Failover Cluster to Host Highly Available Virtual Machines

For the following demonstration I have installed two Windows Server 2012 R2 servers using a GUI install, they are domain joined in the same domain. I have also connected them to the same iSCSI target which has 4 LUNS that I can use as shared storage for my Failover Cluster. I have used a small Qnap SAN device for my shared storage but you could use a third Windows Server 2012 machine with the iSCSI target role installed.

You must start off by installing the Failover Cluster role on both Windows Server 2012 Servers, next as these will be used to host Highly Available virtual machines you must also install the Hyper-V role on both servers, next you should be able to open Failover Cluster Manager, you only need to do this on one of your servers:



Failover Cluster Manager

Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

Overview

A failover cluster is a set of independent computers that work together to increase the availability of server roles. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services. This process is known as failover.

Clusters

Name	Role Status	Node Status
No items found.		

From Failover Cluster Manager you can select Create Cluster, this wizard will allow you to create a domain attached cluster but it might be worth noting that introduced with Windows Server 2012 R2 is the ability using PowerShell to create a Detached Cluster, the difference? Well with an attached cluster the cluster you create relies on domain objects to represent the Cluster and the cluster roles the cluster creates, so if you add the file server cluster role called FILESERVER then an object called FILESERVER will be added to AD as well as an object added to DNS to resolve the name FILESERVER to an IP Address. This works well except in order for these objects to be created you have to give permissions to your Cluster Object to create objects in AD, specifically in the OU that the Cluster Object exists. This can be considered a security risk. A detached cluster does not require that objects are created in AD only that we have objects in AD for name resolution.

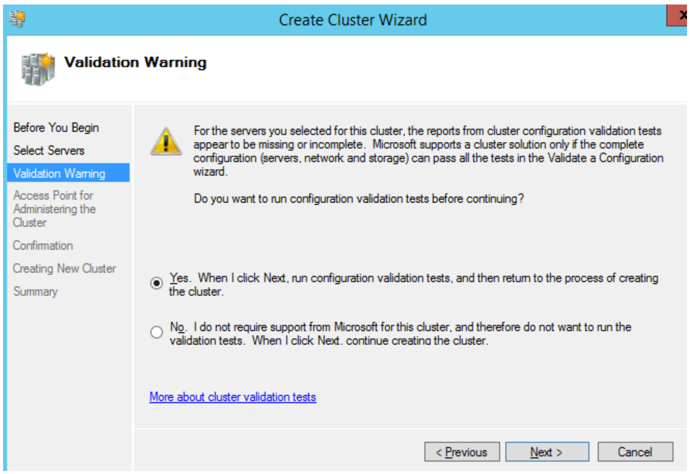
Note. For more general information on Failover Clustering please see the Appendix 1

Select CREATE CLUSTER and the Create Cluster Wizard should start:

On the before you Begin screen click NEXT

The Next Screen is the Select Servers Screen, here you can choose which servers will be part of you Cluster, a server can only be part of a single Failover Cluster at a time, I choose to add my two Windows Servers here. You only have to select your first member of the failover cluster and you can add additional members later on.

The next screen is the Cluster Validation Screen



For the servers you selected for this cluster, the reports from cluster configuration validation tests appear to be missing or incomplete. Microsoft supports a cluster solution only if the complete configuration (servers, network and storage) can pass all the tests in the Validate a Configuration wizard.

Do you want to run configuration validation tests before continuing?

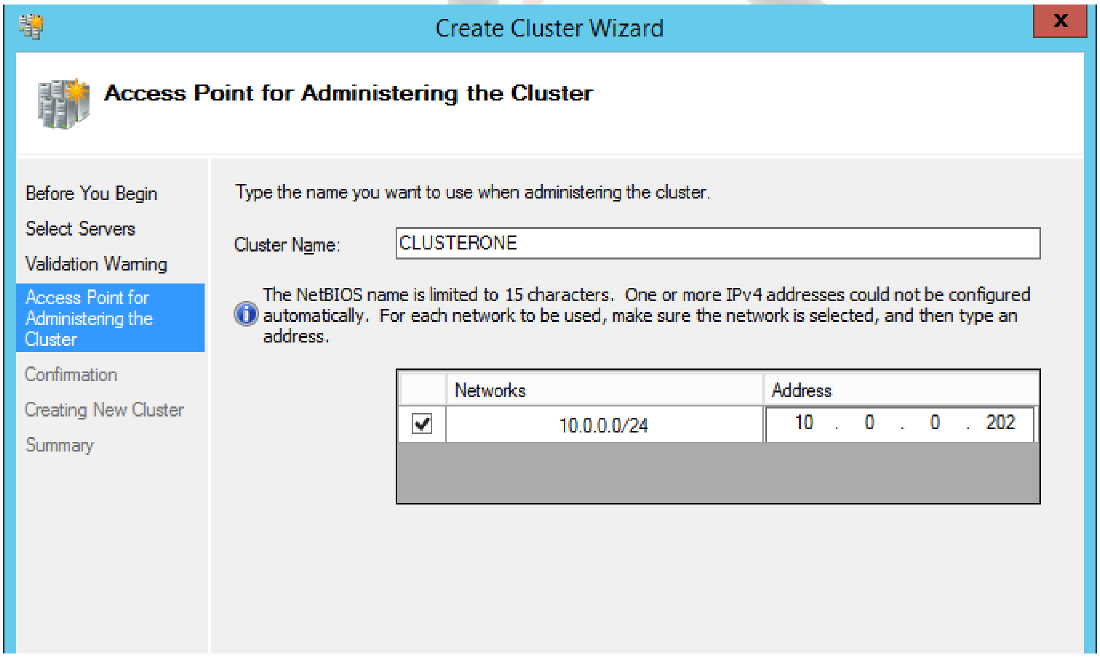
● Yes. When I click Next, run configuration validation tests, and then return to the process of creating the cluster.

○ No. I do not require support from Microsoft for this cluster, and therefore do not want to run the validation tests. When I click Next, continue creating the cluster.

More about cluster validation tests

This screen offers you two choices you can select YES to run the configuration validation tests or NO if you do not require support from Microsoft. This seems like very curious language. The configuration validation tests perform checks to make sure that all the hardware and software installed on the servers you have selected meet the requirements for a Failover Cluster, Microsoft consider this a vital test and as the options suggest if you do not run this check and then need support from Microsoft you will struggle to get it. The good news is that this wizard can be run at any time, it will highlight areas of concern for you to address. Your goal is to be able to run the configuration validation tests without any errors. Also good news, even if your Failover Cluster fails test it doesn't mean Microsoft won't help you it's just that they use the results of your test as a starting off point. Because we are learning and trying to build a test environment I would click NO here and move on. If you are putting this Failover Cluster into production then you must run the test.

The next screen is where ewe configure the Failover Cluster Access Point. In an Attached cluster this will create a Computer Object in AD with the same name as the Cluster Name you choose here. By default it will create this object in the same OU that contains your Windows Servers that will be part of the Failover Cluster. It is also this object that need to be given the permissions to create objects in the OU so that when we create cluster roles the failover cluster object (in my example CLUSTERONE) can create objects In AD.



Type the name you want to use when administering the cluster.

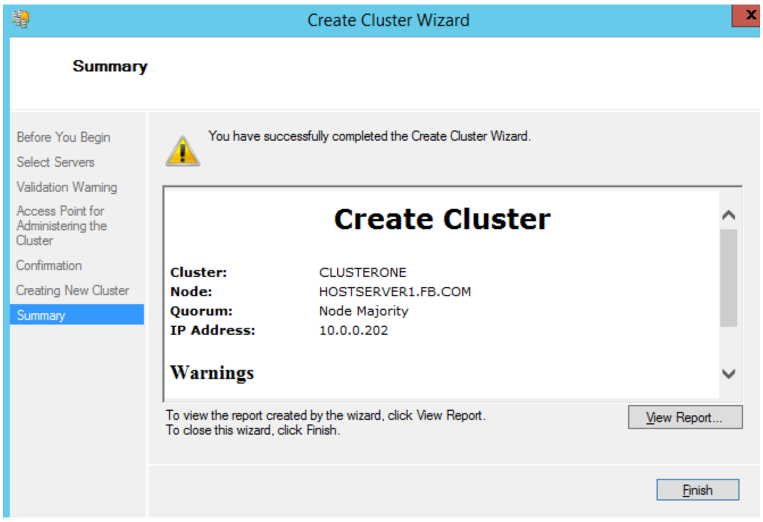
Cluster Name: CLUSTERONE

The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

	Networks	Address
☑	10.0.0.0/24	10 . 0 . 0 . 202

I have called my Cluster CLUSTERONE and assigned it an IP Address, if your Servers are running DHCP then the IP address box might not appear, instead CLUSTERONE would be given a DHCP assigned address.

Once you have chosen a name for your cluster and an IP address click next. Check the setting on the confirmation screen then click next to create you cluster, if all has gone well you should see a screen similar to the one below:



You have successfully completed the Create Cluster Wizard.

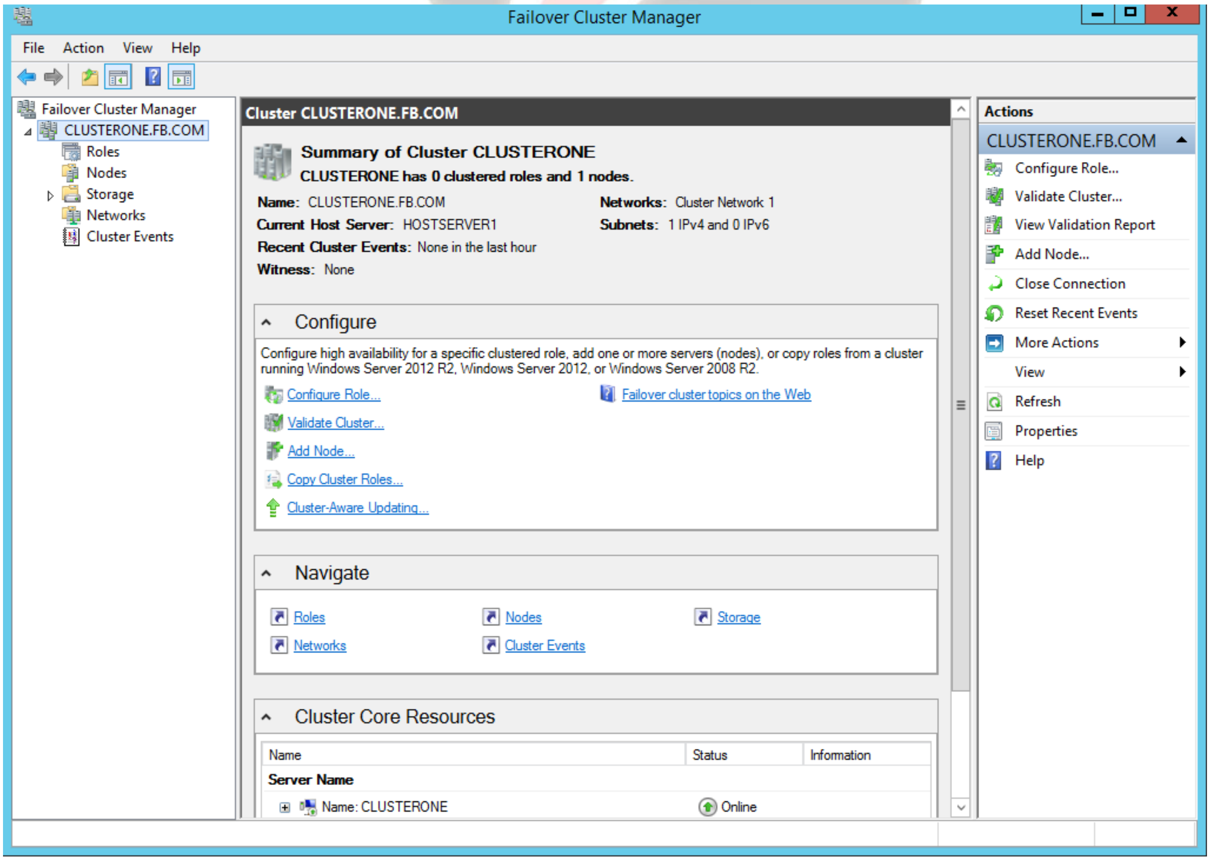
Create Cluster

Cluster:	CLUSTERONE
Node:	HOSTSERVER1.FB.COM
Quorum:	Node Majority
IP Address:	10.0.0.202

Warnings

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Now you have created you Failover Cluster you should be able to see something similar to the screen below in Failover Cluster Manager:



Summary of Cluster CLUSTERONE

CLUSTERONE has 0 clustered roles and 1 nodes.

Name: CLUSTERONE.FB.COM
Current Host Server: HOSTSERVER1
Recent Cluster Events: None in the last hour
Witness: None
Networks: Cluster Network 1
Subnets: 1 IPv4 and 0 IPv6

Configure

Configure high availability for a specific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.

Configure Role...
Validate Cluster...
Add Node...
Copy Cluster Roles...
Cluster-Aware Updating...
Failover cluster topics on the Web

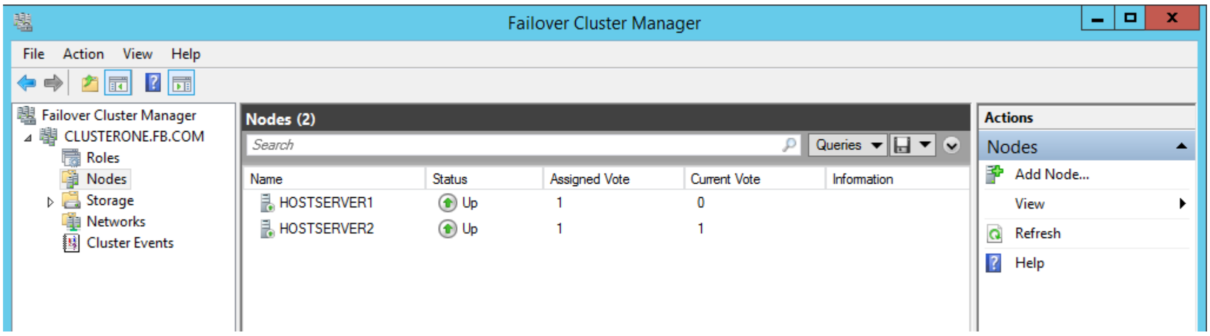
Navigate

Roles
Nodes
Storage
Networks
Cluster Events

Cluster Core Resources

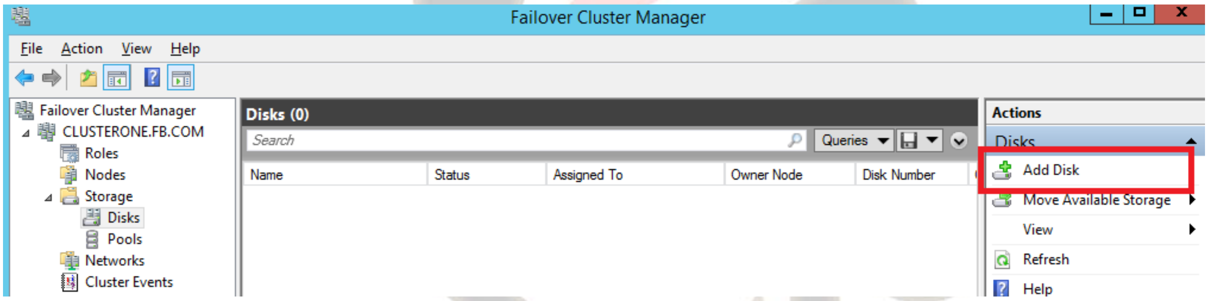
Name	Status	Information
Server Name		
Name: CLUSTERONE	Online	

This screen is very useful in assessing the current state of your cluster, identifying which Host Server you are currently connected to, what type of witness you are using as well as given you suggestions on what elements can be configured. If you select Nodes you should see a list of the members of this failover cluster:

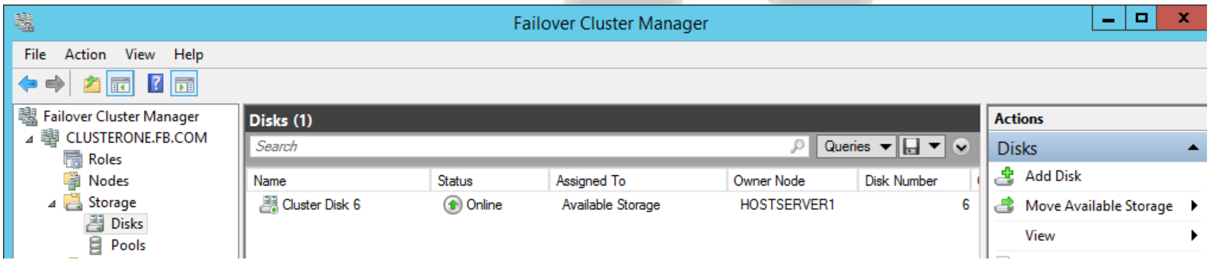


Name	Status	Assigned Vote	Current Vote	Information
HOSTSERVER1	Up	1	0	
HOSTSERVER2	Up	1	1	

If one of your servers isn't listed here or if you want to add additional members in the future then select Add Node from the Actions Pane over on the right of the screen. My list is complete, Next select Storage and the Disks, when the Failover cluster is created any shared Disks should be imported in to the failover cluster to be used as shared storage for the roles this Failover Cluster will host, if you haven't imported the shared disks in during the creation of the cluster then you can select Add Disk to select the disks you want to be used by your failover cluster:



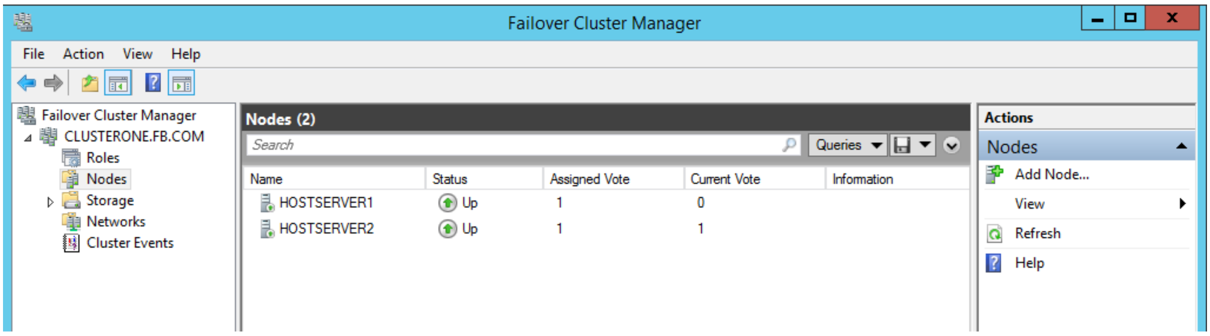
If you haven't got any shared storage ready to import you must do that first, although not all Failover cluster roles require Shared Storage in order to create Highly Available Virtual Machine's you do require shared storage:



Name	Status	Assigned To	Owner Node	Disk Number
Cluster Disk 6	Online	Available Storage	HOSTSERVER1	6

Here I have added one disk to my Failover Cluster.

At this point it is worth talking a little bit about Quorum, in order for a failover cluster to stay up and maintain the availability of its roles then a majority of nodes in the cluster need to be online, I have two node in my cluster and they must agree on which members of the cluster runs which roles.

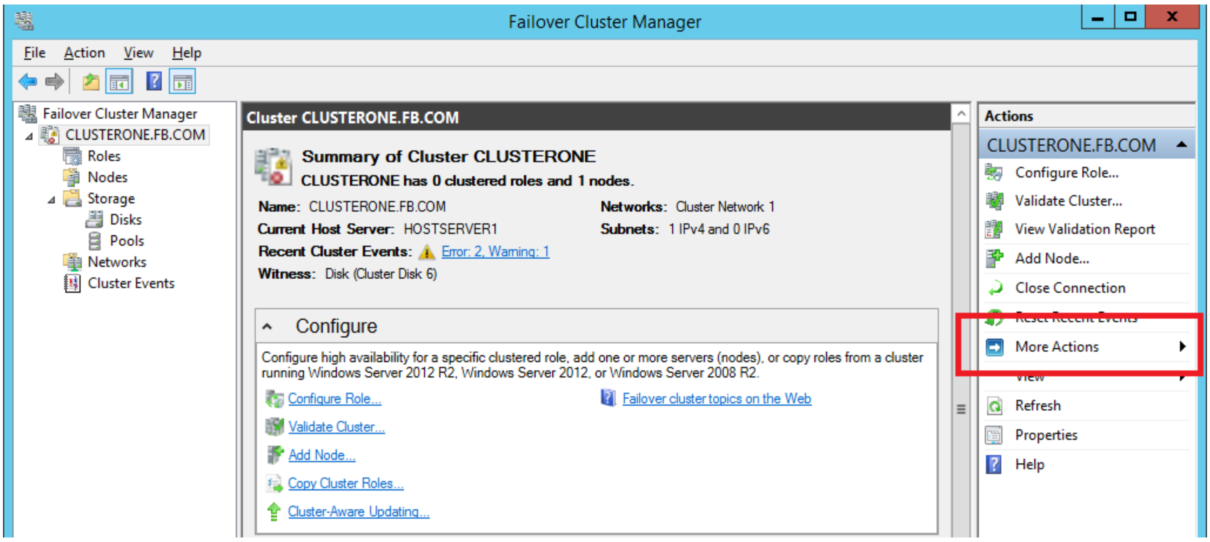


Name	Status	Assigned Vote	Current Vote	Information
HOSTSERVER1	Up	1	0	
HOSTSERVER2	Up	1	1	

Notice here that both of my server are up but only HostServer2 has a vote (look at the Current vote column not the assigned vote column) this means that if the two server lose contact with each other Hostserver2 (1 vote to Hostserver1's 0 Votes) wins and will take over the running of all roles on the cluster, any roles that are currently running on Hostserver1 would be stopped and started on HostServer2. This is expected behaviour to prevent what is called split brain where both members of the cluster try to run the same roles.

Note. A Highly available virtual machine is considered a Failover Cluster role, each highly Available virtual machine must only run on one host server at a time.

With only one voting Node it could lead to a situation where Hostserver1 is up and running and in contact with the network but because it loses contact with Hostserver2 it cannot start any role (for us Virtual Machines) if HostServer2 is down that could mean our cluster goes down (this is not always the case please see the appendix on failover clustering for more details.) in order to give both nodes a vote I am going to add a disk witness, a disk witness add a 3 vote to the Quorum, an important concept of Failover Clustering is that there can only be an odd number of votes, this is why at present one of my servers has add its vote removed. By adding a disk witness both Nodes will have a vote plus the disk witness giving us an odd number of votes again. In the event that the cluster nodes (Hostserver1 and Hostserver2 in my example) lose contact with each other then one of them will grab the vote of the Disk witness giving it 2 votes to the other nodes 1 vote. It is the node with 2 votes that will run the cluster and all its clustered roles.



Summary of Cluster CLUSTERONE

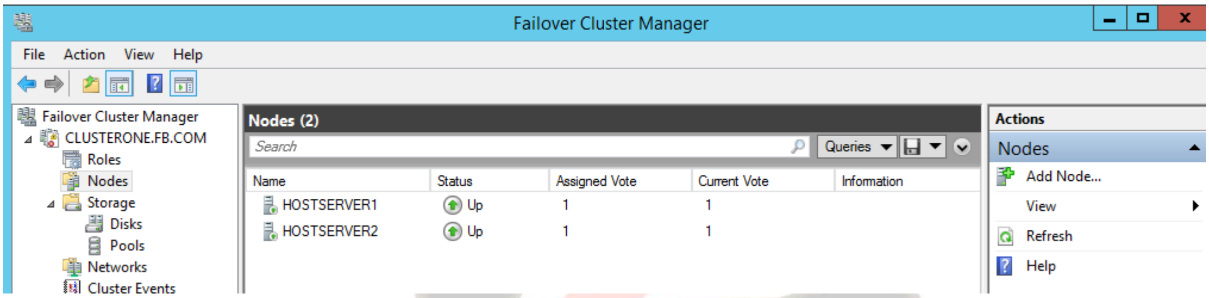
CLUSTERONE has 0 clustered roles and 1 nodes.

Name: CLUSTERONE.FB.COM
Networks: Cluster Network 1
Current Host Server: HOSTSERVER1
Subnets: 1 IPv4 and 0 IPv6
Recent Cluster Events: Error: 2, Warning: 1
Witness: Disk (Cluster Disk 6)

Configure high availability for a specific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.

If you choose more actions you can choose to change your cluster quorum and follow the wizard through, if you select all the defaults your cluster should detect one of you added disks and configure the cluster to use a Disk Witness, in my example I have already run through the wizard and you can see my cluster has been configured to use Disk 6 as a Disk witness. You can choose other types of Quorum models these will be discussed in the appendix. Unlike earlier versions of Failover clustering when you use Windows Server 2012 R2 as the operating system for your Failover Cluster it is recommended you have a witness.

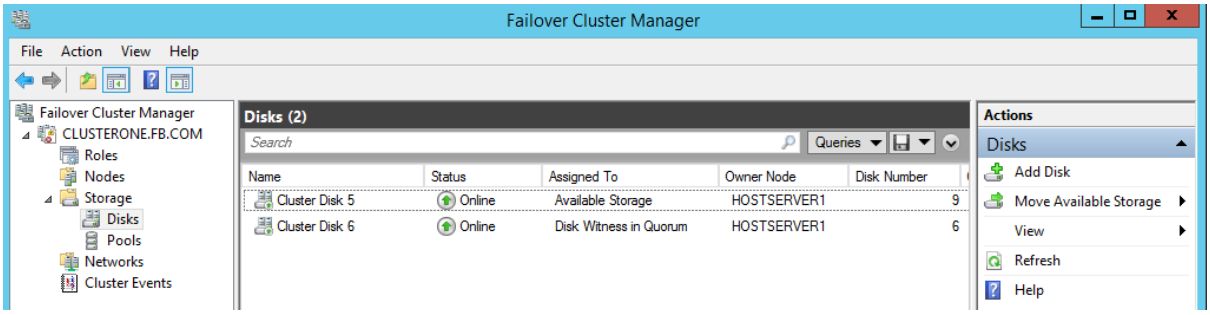
With the witness added you should see that both your nodes now have a vote:



Name	Status	Assigned Vote	Current Vote	Information
HOSTSERVER1	Up	1	1	
HOSTSERVER2	Up	1	1	

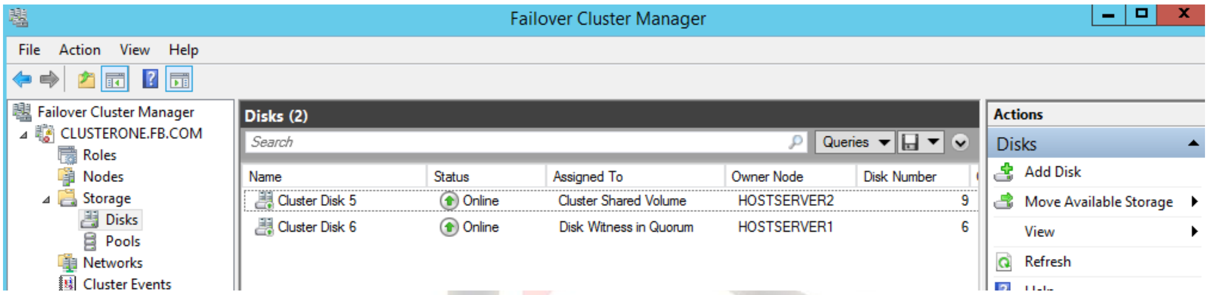
In my example so far I have added one shared disk ad used it for my Disk witness but before I add my fist highly available virtual machine I need to add a second disk. We need somewhere to store the virtual machine files, the .VHD / .VHDX files the virtual machines will use as well as a location for checkpoints. One way to do this would be to assign a LUN to each Node for it to store all the above files on for each of the virtual machines it hosts, then these LUNS needs to be accessible from both Physical servers so that in the event that one node fails control of the LUN and then all of the Virtual machine on that LUN can be given to the remaining NODE. This process will take time, plus if we had three nodes in our cluster or four nodes in our cluster we would need additional LUNS one for each node to control during normal operations (a single LUN can only be written to by one node at a time). So to speed up a failover event and reduced the number of LUNS Microsoft introduced the concept of Cluster Shared Volumes (CSV’S). A CSV is an iSCSI of Fibre channel LUN that all the nodes in the cluster can see, it appears as a mounted volume on the local computer. Crucially all node in the cluster can read and write to the CSV at the same time, this reduces the number of LUNS that need to be created, also during a failover event ownership of the disk resource (the LUN) does not have to be transferred to another NODE, each NODE already owns the CSV so all that happens is that any Virtual Machines that were running on the failed node are restarted on another node In the cluster.

For my CSV I added a second disk to my cluster:



Name	Status	Assigned To	Owner Node	Disk Number
Cluster Disk 5	Online	Available Storage	HOSTSERVER1	9
Cluster Disk 6	Online	Disk Witness in Quorum	HOSTSERVER1	6

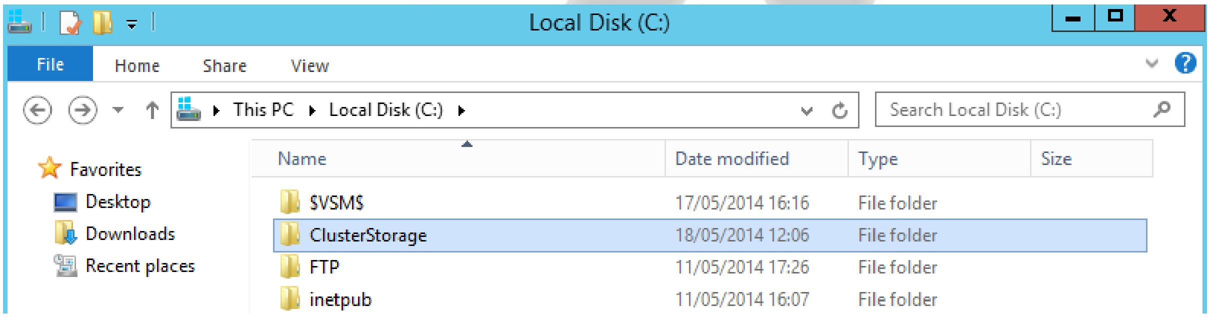
It is important that this disk has already been partitioned with a formatted volume on it, it does not require a drive letter do this before adding it to the failover cluster. Then Right click the newly added disk and chose add to cluster shared volume



Name	Status	Assigned To	Owner Node	Disk Number
Cluster Disk 5	Online	Cluster Shared Volume	HOSTSERVER2	9
Cluster Disk 6	Online	Disk Witness in Quorum	HOSTSERVER1	6

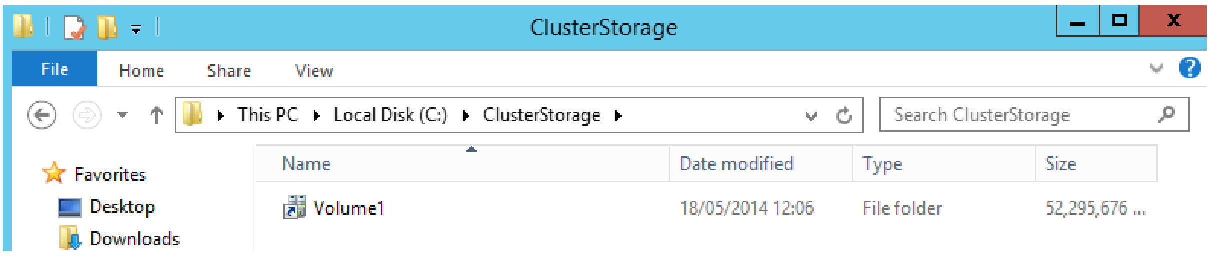
All being well you should see the Assigned to change from Available storage to Cluster Shared volume.

On each of the nodes in your cluster you should see a folder appear on drive C:\ called Clusterstorage:



Name	Date modified	Type	Size
VSM	17/05/2014 16:16	File folder	
ClusterStorage	18/05/2014 12:06	File folder	
FTP	11/05/2014 17:26	File folder	
inetpub	11/05/2014 16:07	File folder	

Inside there you should disk called Volume1



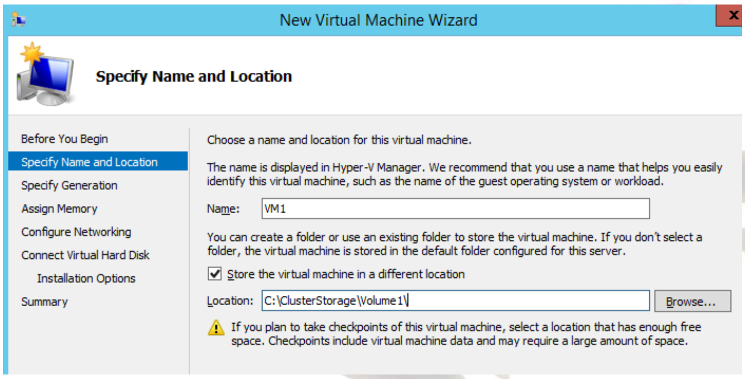
Name	Date modified	Type	Size
Volume1	18/05/2014 12:06	File folder	52,295,676 ...

You will use this volume to store all the files (vhdx .ect) when you create a Highly Available Virtual Machine.

Creating a Highly Available Virtual Machine on a Failover Cluster

Now that you have a working Failover Cluster with the appropriate storage (a CSV) we can now add a virtual machine for the Failover Cluster to manage. First we will create a Virtual Machine from scratch using the New Virtual Machine Wizard seen previously in Part 1 but this time we will start it from within Failover Cluster Manager, we will then use the Failover cluster Manager Tool to make an existing virtual machine a Highly Available Virtual Machine.

From Failover Cluster Manager on one of the members of your failover cluster, **Right Click Roles, Select Virtual Machines and then New Virtual Machine:**



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: VM1

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

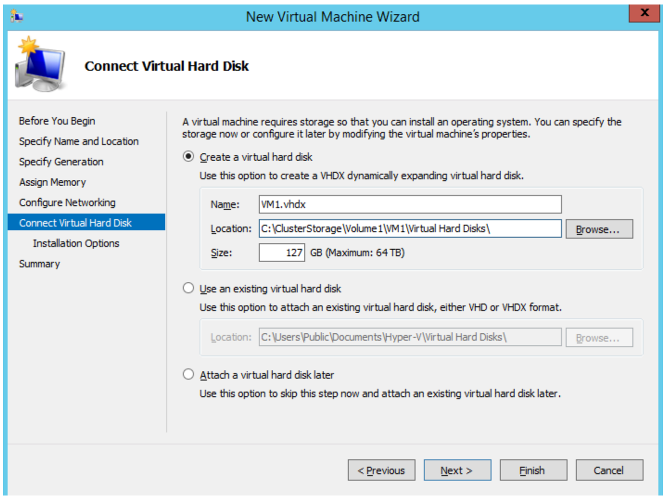
☑ Store the virtual machine in a different location

Location: C:\ClusterStorage\Volume1\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

Here we see the New Virtual Machine wizard, I have chosen a name for my Virtual Machine and then I have selected the tick box Store the virtual; Machine in a Different location. This step is vital, by default the Hyper V Server will want to store the Virtual Machine files in its default storage location, this is typically a local store on the server but maybe an SMB 3.0 file share. In Order to make our new Virtual Machine Highly Available we need to store its Virtual Machine files and its .VHD / .VHDX files on our newly created Cluster Shared Volume (CSV). Once you have chosen your Cluster Shared Volume as the storage locations for the Virtual Machine files click next.

Fill in the details in the Machine Generation screen, the Assign Memory screen and the Configure Networking screen as needed then on the Connect Virtual Hard disk screen we need to make sure that we choose to store our .VHD / .VHDX file on our cluster shared volume. This may be a virtual hard disk that is already created or it may be one you are creating now. In my example I have chosen to create a new virtual hard disk and have chosen the Cluster Shared Volume as its location:



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: VM1.vhdx

Location: C:\ClusterStorage\Volume1\VM1\Virtual Hard Disks\ Browse...

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

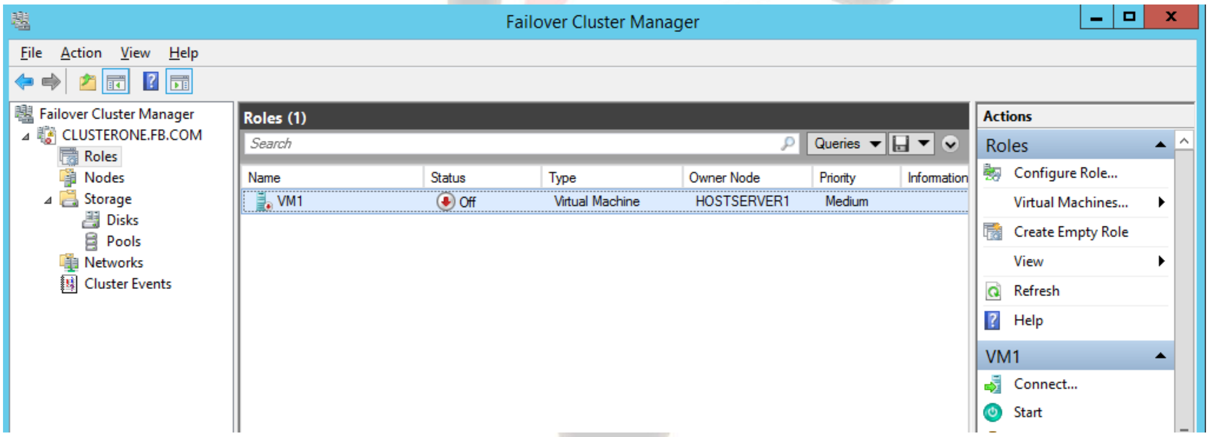
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

Once you happy with your selection click next and the fill in the installation options pane as needed before continuing to the summary pane and clicking finish. Once done, your new virtual machine will appear in Hyper V manager on the Host server you are working on and because we have made it highly available it will also appear inside cluster manager as a clustered resource:

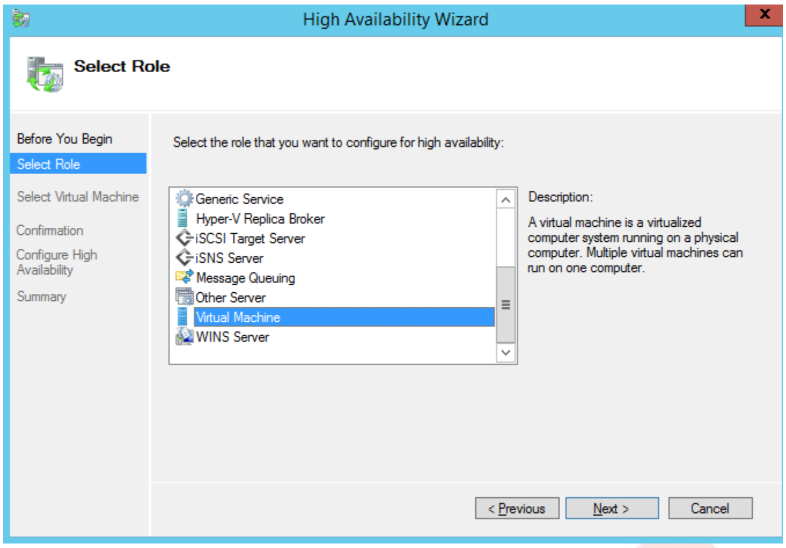


Failover Cluster Manager

Name	Status	Type	Owner Node	Priority	Information
VM1	Off	Virtual Machine	HOSTSERVER1	Medium	

Here we can see VM1, it is switched off at the minute but can be started from Hyper V manager or through Failover Cluster Manger. Notice that the owner of my newly created virtual machine is HOSTSERVER1, this is the member of the failover cluster that is running the virtual machine right now it is the owner of the clustered resource VM1, all connection to VM1 will be managed by the Hyper V service on HOSTSERVER1, but because this machine is highly available if HOSTSERVER1 were to fail then HOSTSERVER2 would become the owner of VM1 and the virtual machine would restarted on HOSTSERVER2.

It is possible that a Hyper V hosts server that is a member of a cluster could have been running some virtual before it became a cluster member, these virtual machines are not highly available and if your host server fails then you will lose access to these virtual machines. Failover Cluster manager gives you the ability to associate an existing virtual machine with you newly created cluster. Through Failover Manager right click roles and select to add a new role:



Select the role that you want to configure for high availability:

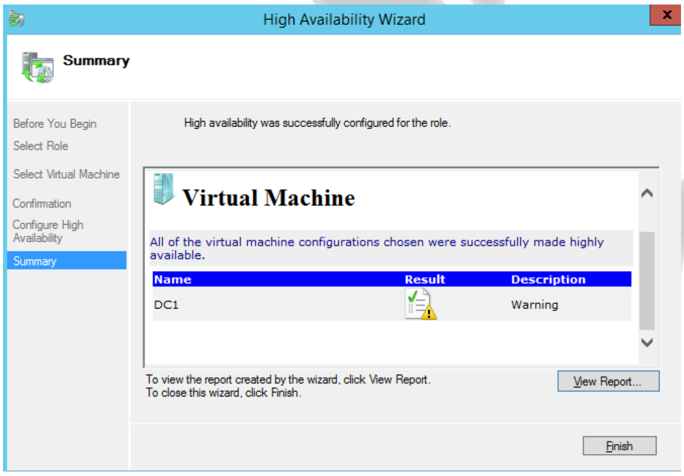
Description:

A virtual machine is a virtualized computer system running on a physical computer. Multiple virtual machines can run on one computer.

You will be presented with a lots of roles that you can configure for high availability, scroll down and select the virtual machine role then click next. You will be presented with a list of Virtual Machines that are running on you host server that are not being managed by the Failover Cluster service, in my list I have several including a virtual machine called DC1.

Note. If you don't see any virtual machines on the list it is probably because the host server you are on doesn't have any, go to Hyper V manager and create a basic virtual machine with is storage on a local drive.

Select your virtual machine from the list and click next:



High availability was successfully configured for the role.

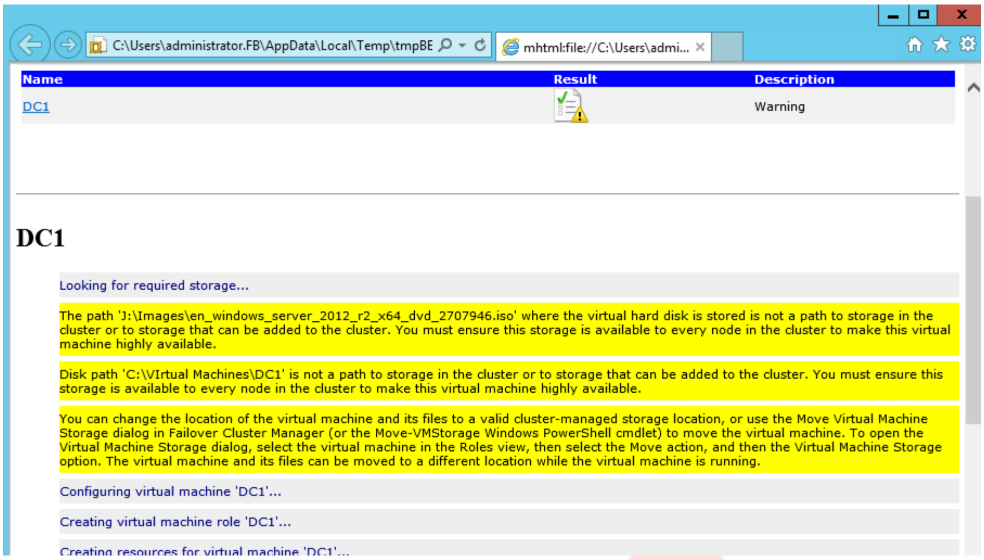
Virtual Machine

All of the virtual machine configurations chosen were successfully made highly available.

Name	Result	Description
DC1	⚠	Warning

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Here you can see that I have chosen DC1 but I have received a warning about my configuration, if this happened click on the View Report button and it will give detail of the waning message.



C:\Users\administrator.FB\AppData\Local\Temp\tmpBE
mhtml:file://C:\Users\admi...

Name	Result	Description
DC1		Warning

DC1

Looking for required storage...

The path 'J:\Images\en_windows_server_2012_r2_x64_dvd_2707946.iso' where the virtual hard disk is stored is not a path to storage in the cluster or to storage that can be added to the cluster. You must ensure this storage is available to every node in the cluster to make this virtual machine highly available.

Disk path 'C:\VIrtual Machines\DC1' is not a path to storage in the cluster or to storage that can be added to the cluster. You must ensure this storage is available to every node in the cluster to make this virtual machine highly available.

You can change the location of the virtual machine and its files to a valid cluster-managed storage location, or use the Move Virtual Machine Storage dialog in Failover Cluster Manager (or the Move-VMStorage Windows PowerShell cmdlet) to move the virtual machine. To open the Virtual Machine Storage dialog, select the virtual machine in the Roles view, then select the Move action, and then the Virtual Machine Storage option. The virtual machine and its files can be moved to a different location while the virtual machine is running.

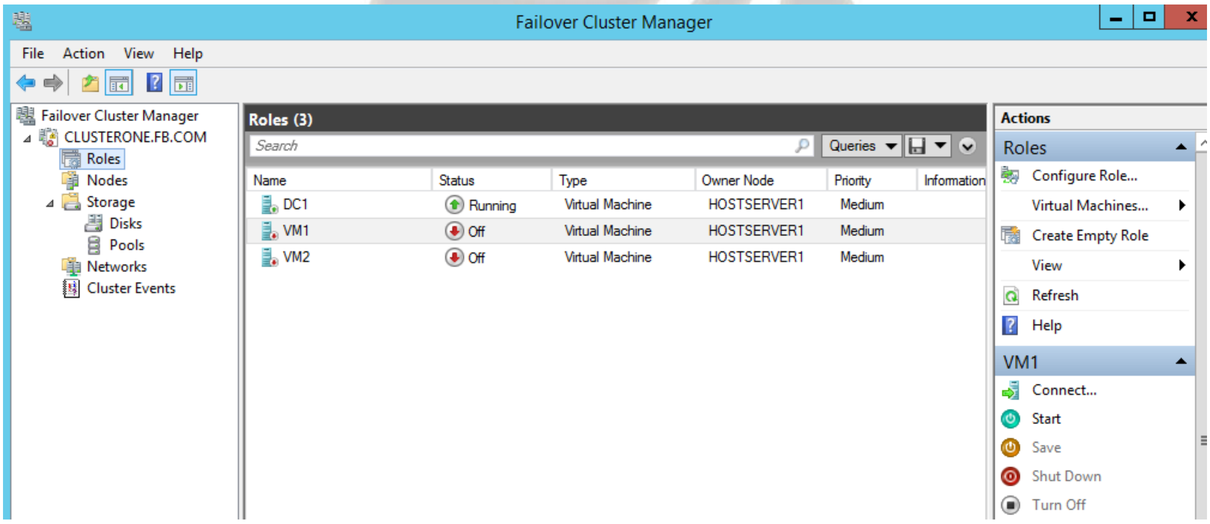
Configuring virtual machine 'DC1'...

Creating virtual machine role 'DC1'...

Creating resources for virtual machine 'DC1'...

Here you see the results of my warning message, it states that the path “J:\images” is not a highly available path, this path leads to a mounted ISO file that I have been using during the installation of this virtual machine, this error is only an issue if the path needs to be permanent, a more pressing issue is that the path “C:\virtual Machines” is also not highly available. In short the drive that contains my Virtual machine files and .vhdx files is a local path. If this virtual machine was added to the Hyper V cluster and a failure was to occur then the surviving host servers would be unable to start the virtual machine because they would not have access to path that contains the virtual machine files.

You can ignore this warning and continue to add the Virtual Machine to the failover cluster, you would get a result similar to the next screen shot:



Name	Status	Type	Owner Node	Priority	Information
DC1	Running	Virtual Machine	HOSTSERVER1	Medium	
VM1	Off	Virtual Machine	HOSTSERVER1	Medium	
VM2	Off	Virtual Machine	HOSTSERVER1	Medium	

Here DC1 is up and running on HOSTSERVER1, it appears that everything is working ok BUT as stated earlier everything is far from OK. If HOSTSERVER1 was to fail then DC1 would not be started on HOSTSERVER2 because it would not be able to access the virtual machine files on the failed Host server. All is not lose though, with the introduction of Windows Server 2012 and now Windows Server 2012 R2 Microsoft have introduced new features that allow us to easily move a virtual machine files and its virtual disk to another location so to make

DC1 truly highly available all we have to do is move its file to our cluster shared volume, an added bonus is that we can perform this move without any down time to DC1, this new feature is Virtual Machine and Storage Migration.

Day 9

Windows Server ADFS Deployment Guide

Follow the link below to a TechNet article on ADFS deployment, this article is very detailed so you should only concentrate on elements listed in the ADFS Module

https://technet.microsoft.com/library/dd807092.aspx

Azure Online Backup PowerShell CMDLets

Have a look for the CMDLets that are needed to configure and schedule an online backup

https://technet.microsoft.com/en-us/library/hh770400(v=wps.630).aspx