FIREBRAND

Microsoft

MCSA Windows Server 2012 Upgrade Certification

Courseware

Version 2.0

www.firebrandtraining.com

MCSA SERVER 2012 REVIEW MATERIAL

ADDITIONAL MATERIAL FOR EXAMS 70-410, 70-411, 70-412 AND 70-417

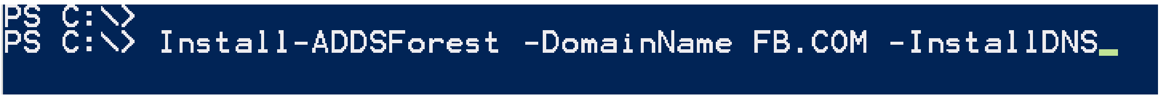
FIREBRAND TRAINING

Table of Contents

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

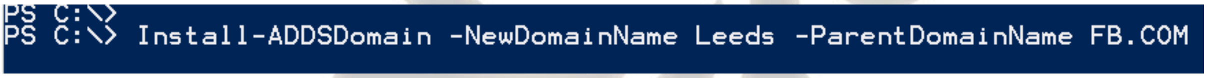
-DomainMode – Sets domain functional level by either using a number or name, examples are 4/ 4/Win2008R2 or 5/Win2012

-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* –ParentDominaName *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

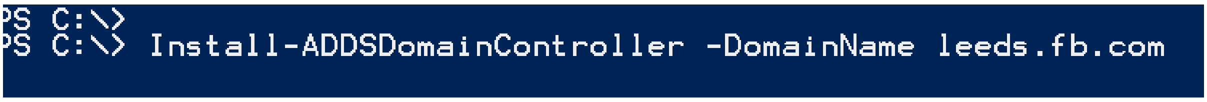
-ReplicationSourceDC – Sets the domain controller that we will copy partition information from.

-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 Deployment CmdLets

Add-ADDSReadOnlyDomainContorllerAccount – Creates a read-only domain Controller account that can be used to install an RODC

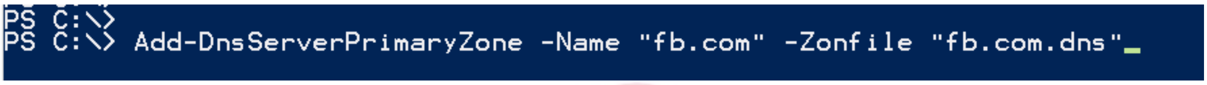
Uninstall-ADDSDomainController – Uninstalls a domain controller in Active Directory

Managing DNS from PowerShell and DNSCMD

PowerShell

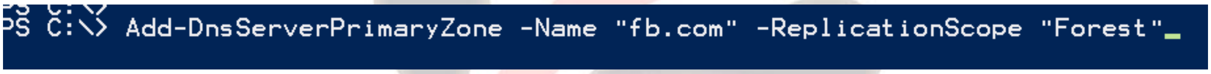
We can use PowerShell to create DNS zones, DNS Records and to manage the DNS server itself.

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"
```

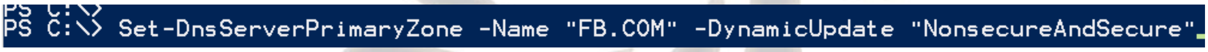
If we use the same cmdlet but don't specify a zone file we can specify a replication scope and create an ADI zone, the example below create and ADI zone called FB.Com replicated to the whole forest.



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

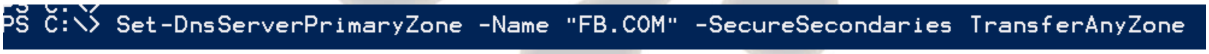
-ReplicationScope can be Forest, Domain, Legacy or Custom if you want to replicate the ADI zone to a custom application partition.

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"
```

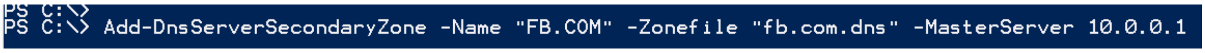
The Example below changes Zone transfer setting for a zone called FB.COM



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

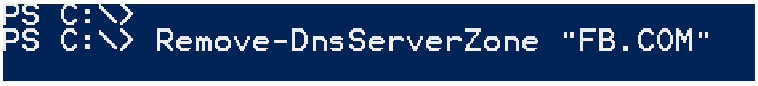
The –SecureSecondaries switch can be set to NOTransfer, TransferAnyServer, TransferToZoneNameServer and TransferToSecureServers

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



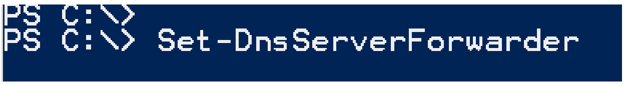
```
PS C:\>
PS C:\> Add-DnsServerSecondaryZone -Name "FB.COM" -Zonefile "fb.com.dns" -MasterServer 10.0.0.1
```

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

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



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

DNSCMD

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

For a more complete list of DNSCMD switches go to:

http://technet.microsoft.com/en-us/library/cc772069.aspx#BKMK_22

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 2	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.

Applocker

Applocker allows you to create rules to allow or deny applications from running based on unique identities of files and to specify which users or groups can run those applications. AppLocker was introduced in Windows Server 2008 R2 and Windows 7 that advances the application control features and functionality of Software Restriction Policies.

Using AppLocker, you can:

1) Control the following types of applications: executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, and .bat), Windows Installer files (.mst, .msi and .msp), and DLL files (.dll and .ocx), and packaged apps and packaged app installers (appx).
2) Define rules based on file attributes derived from the digital signature, including the publisher, product name, file name, and file version. For example, you can create rules based on the publisher attribute that is persistent through updates, or you can create rules for a specific version of a file.
3) Assign a rule to a security group or an individual user.
4) Create exceptions to rules. For example, you can create a rule that allows all Windows processes to run except Registry Editor (Regedit.exe).
5) Use audit-only mode to deploy the policy and understand its impact before enforcing it.
6) Import and export rules. The import and export affects the entire policy. For example, if you export a policy, all of the rules from all of the rule collections are exported, including the enforcement settings for the rule collections. If you import a policy, all criteria in the existing policy are overwritten.

PowerShell Applocker CMDLets

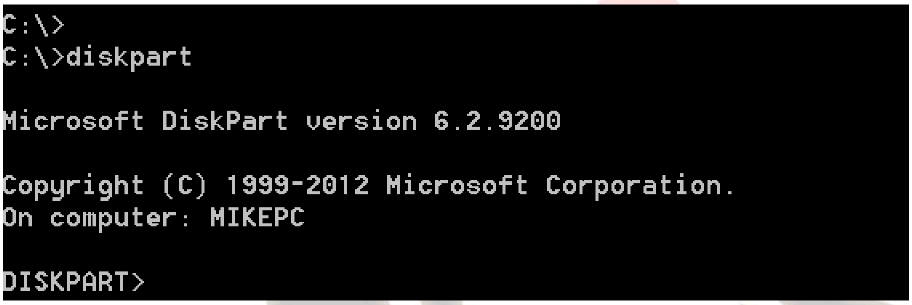
CMDLet Name	Description
New-AppLockerPolicy	Creates a new AppLocker policy from a list of file information and other rule creation options.
Set-AppLockerPolicy	Sets the AppLocker policy for the specified Group Policy Object (GPO).
Test-ApplockerPolicy	Specifies the AppLocker policy to determine whether the input files will be allowed to run for a given user.

Virtual Disk Management using PowerShell and DiskPart

DiskPart

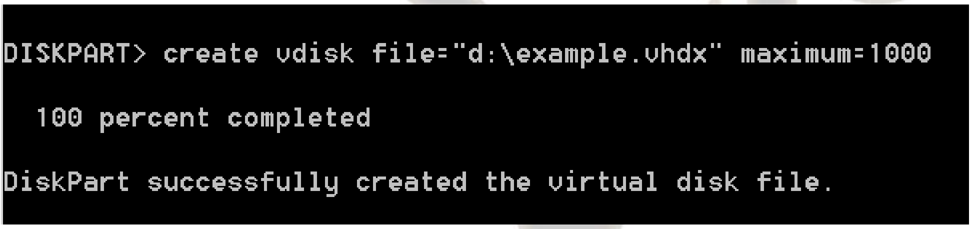
DiskPart is a text-mode command interpreter that enables you to manage disks, partitions, volumes or Virtual hard disks. In the following examples we will be using DiskPart to create and manage Virtual Disks.

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.



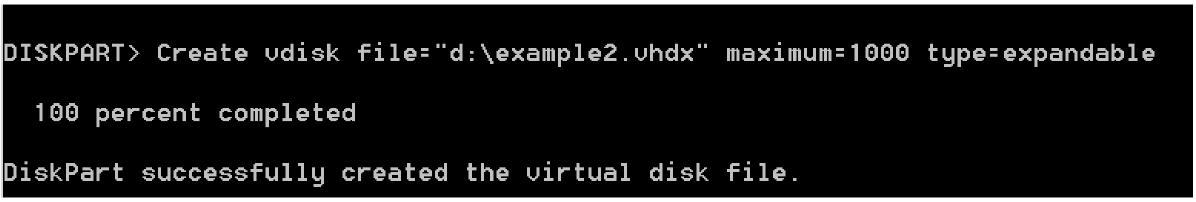
```
C:\>
C:\>diskpart

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

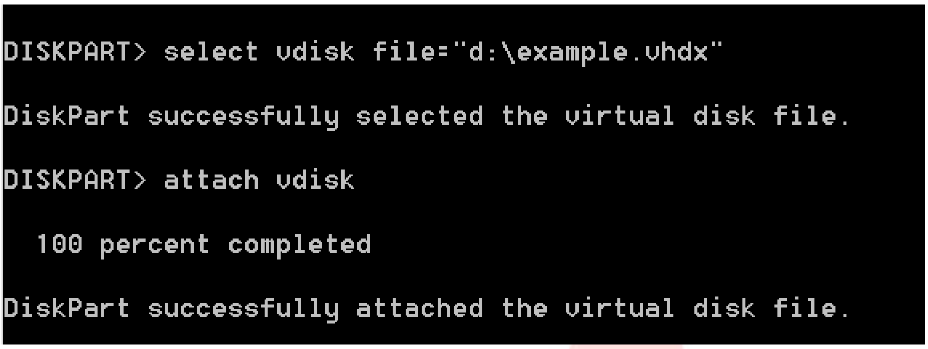


```
DISKPART> Create vdisk file="d:\example2.vhdx" maximum=1000 type=expandable

  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.

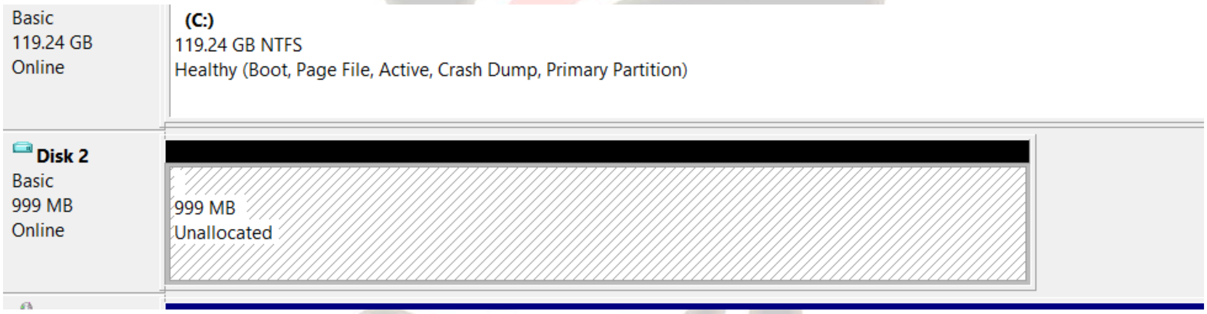
One other useful feature of DiskPart is its ability to attach a VHD/VHDX file to a computer, making available as a local disk in the machine. Once attached we could create partitions, format them and assign drive letters and then copy data to it. Also we can use DISM to add an image file to the attached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

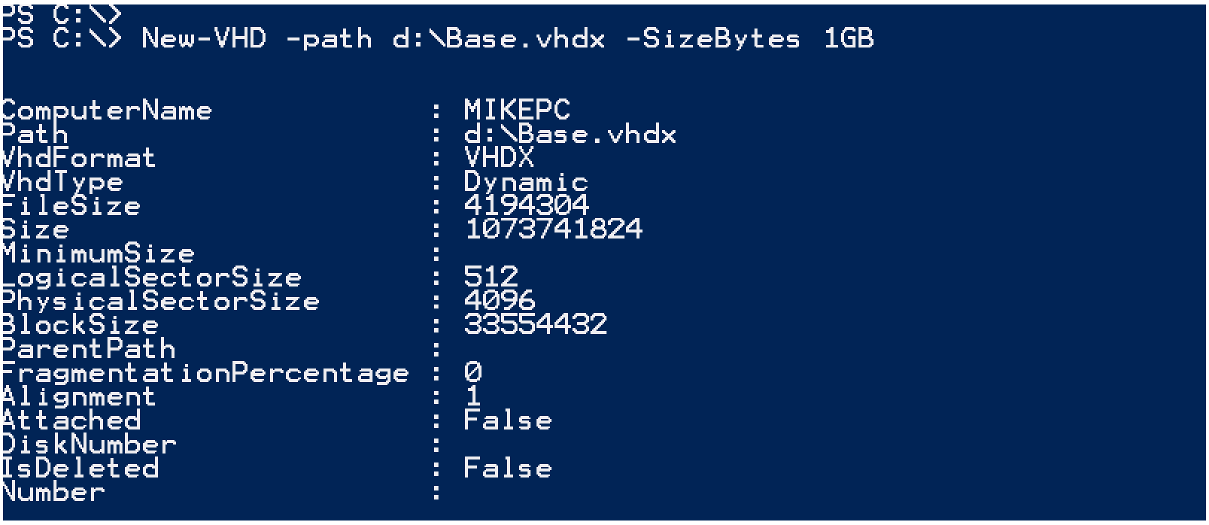
Disk 2
Basic
999 MB
Online

999 MB
Unallocated

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

PowerShell

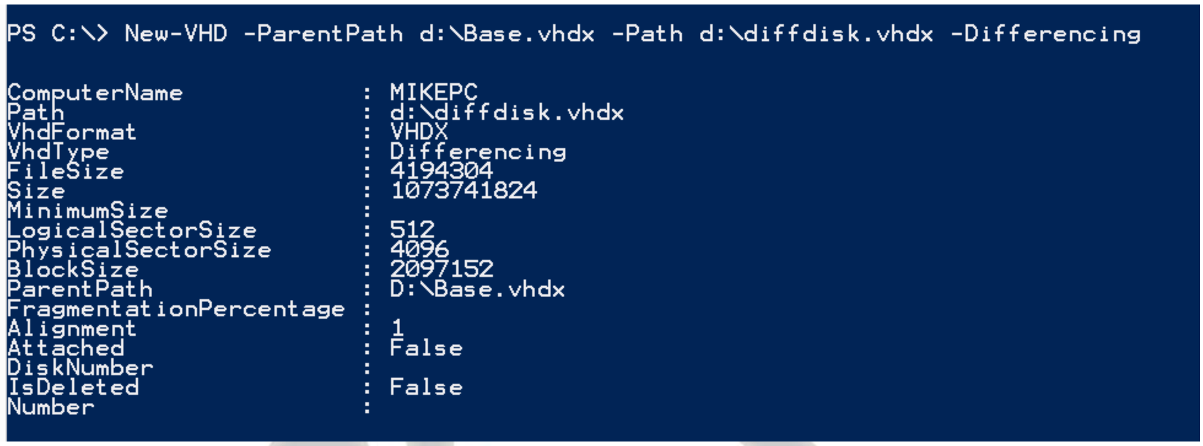
New-VHD can be used to create vhd/vhdx files from PowerShell, below we have created a .VHDX file called Base.vhdx that is 1GB in size



```
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                  :
```

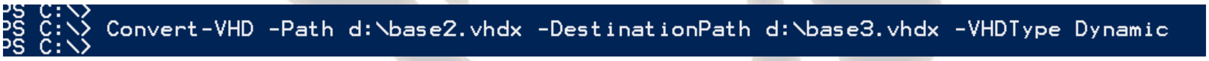
One useful way to conserve disk space is to use Differencing disks, each differencing disk is based on a parent. The parent disk would usually include a syspreped operating system and each differencing disk is then used to create a Virtual machine, the differencing disk is then used to save the changes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



```
PS C:\>
PS C:\> Convert-VHD -Path d:\base2.vhdx -DestinationPath d:\base3.vhdx -VHDType Dynamic
PS C:\>
```

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.

<u>Other CMDLets used for creating and managing storage pools are:</u>

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

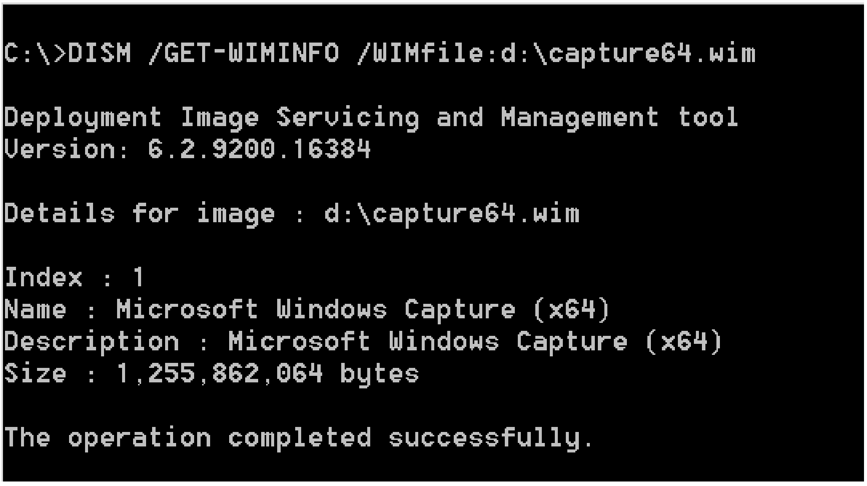
DISM – Online and Offline Servicing

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.

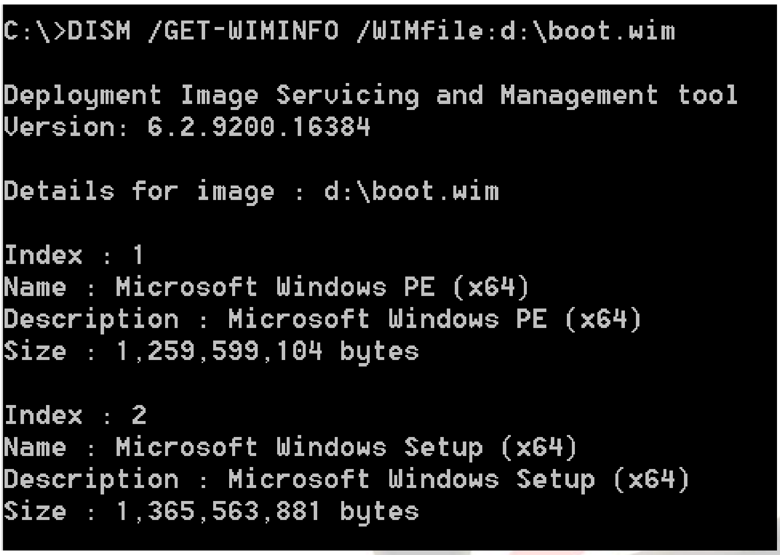
DISM.exe /GET-WIMINFO /WIMFILE:D:\capture.wim



```
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.

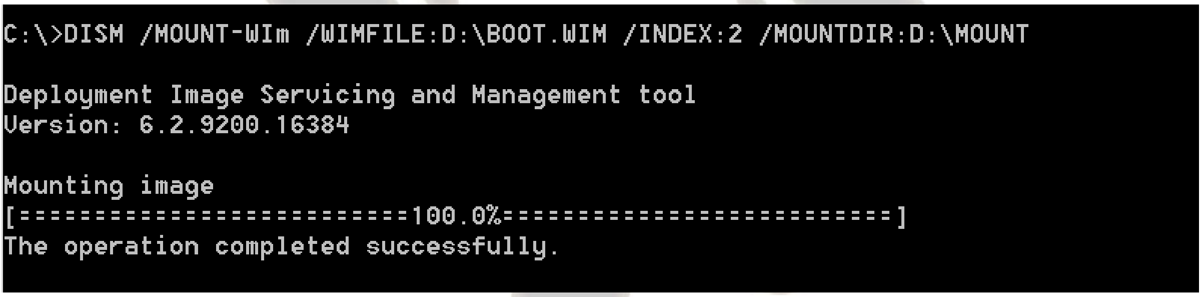
If we run the same command against Boot.wim we can see that there are two images in this file identified as Index 1 and Index 2.



```
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



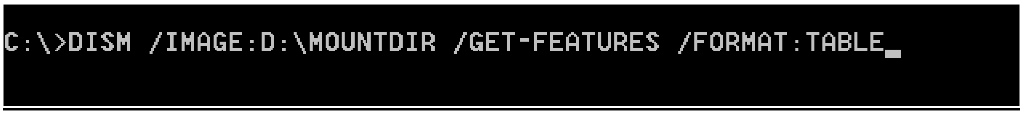
```
C:\>DISM /MOUNT-WIm /WIMFILE:D:\BOOT.WIM /INDEX:2 /MOUNTDIR:D:\MOUNT

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.

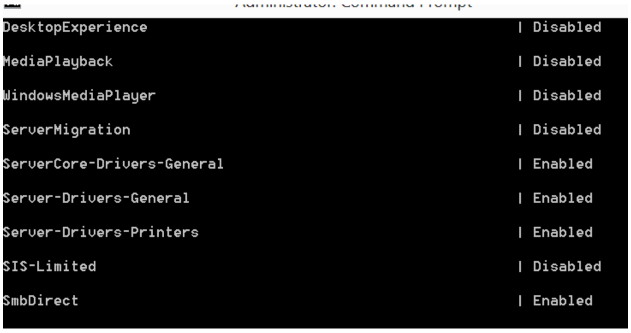
Now we have the image mounted we can work with it.

Using DISM to add a feature to a mounted image

DISM /IMAGE:D:\MOUNTDIR /GET-FEARUTS /FORMTAT:TABLE



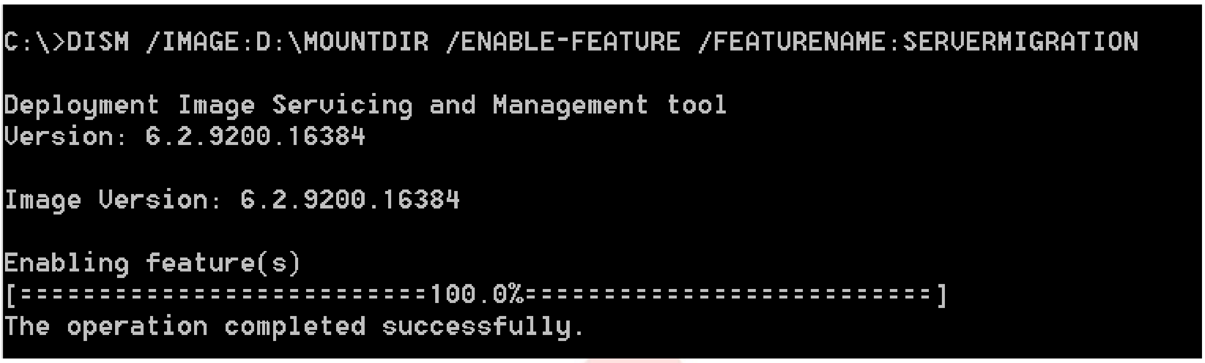
```
C:\>DISM /IMAGE:D:\MOUNTDIR /GET-FEATURES /FORMAT:TABLE_
```



```
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
```

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.

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.

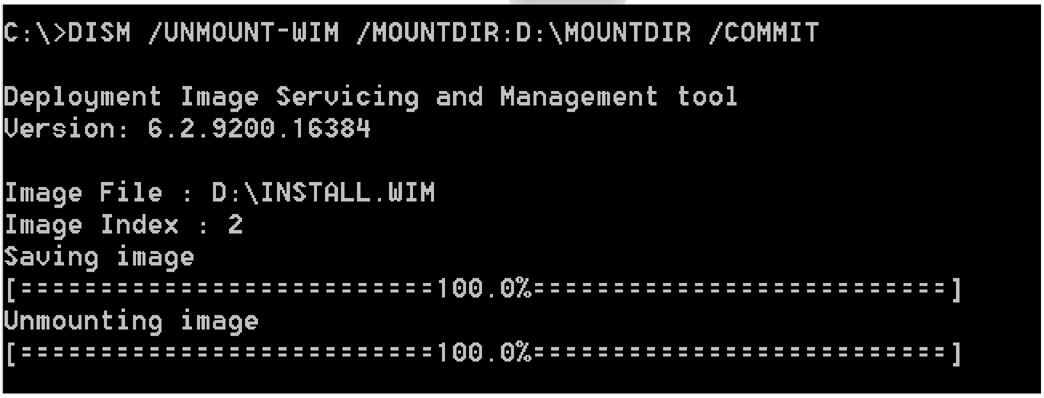
As well as installing roles/features you can also add other packages like update packages. Using the /ADD-Package switch with the /PackagePath switch you can identify the location of the .cab or .msu file that contains the information about the package you would like to install

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*

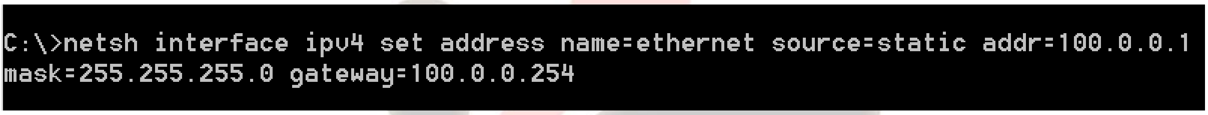
Configuring IP Settings using Netsh and PowerShell

Network shell (netsh) is a command line utility that allows you to configure and display the status of various server roles and components. Here we will look at the Netsh commands used to configure IP settings.

Windows PowerShell is a task-based command line shell and scripting language designed for system administration. Here we will look at the PowerShell commands used to configure IP settings.

To configure static IPv4 address and gateway with NETSH

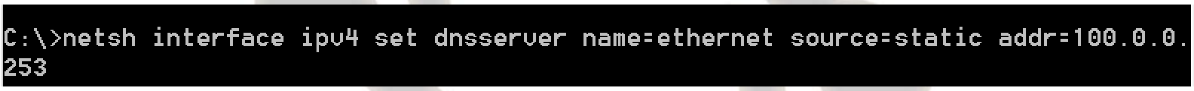
Netsh interface ipv4 set address name=*Interface name* source=static addr=IP Address mask=*MASK* gatway=*Gateway IP*



```
C:\>netsh interface ipv4 set address name=ethernet source=static addr=100.0.0.1
mask=255.255.255.0 gateway=100.0.0.254
```

To configure IPv4 DNS server address with NETSH

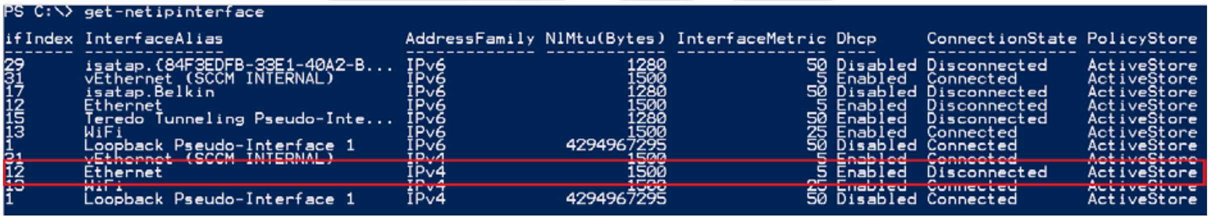
Netsh interface IPv4 set Dnsserver name=*interface name* source=*static* addr=*DNS Server address*



```
C:\>netsh interface ipv4 set dnsserver name=ethernet source=static addr=100.0.0.
253
```

To configure static IPv4 address and gateway with Powershell

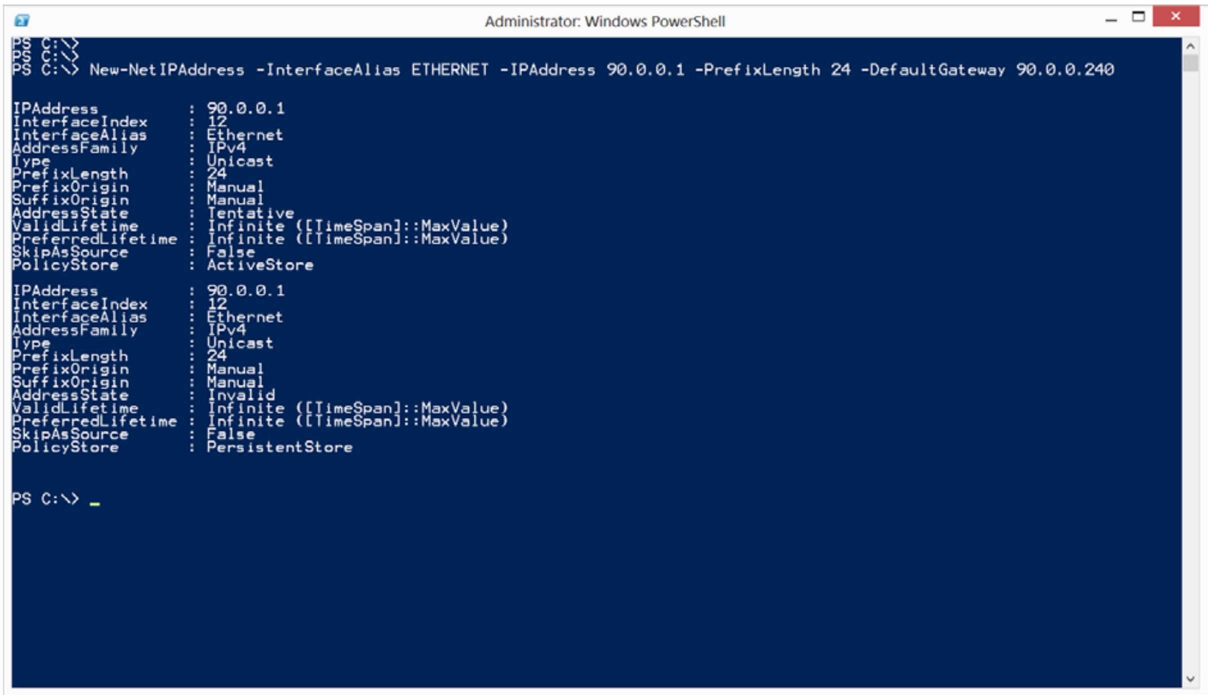
Get-NetIPInterface



```
PS C:\> get-netipinterface

ifIndex InterfaceAlias                  AddressFamily NlMtu(Bytes) InterfaceMetric Dhcp     ConnectionState PolicyStore
------- --------------                  ------------- ------------ --------------- ----     --------------- -----------
29      isatap.{84F3EDFB-33E1-40A2-B... IPv6                  1280              50 Disabled Disconnected    ActiveStore
31      vEthernet (SCCM INTERNAL)       IPv6                  1500               5 Enabled  Connected       ActiveStore
17      isatap.Belkin                   IPv6                  1280              50 Disabled Disconnected    ActiveStore
12      Ethernet                        IPv6                  1500               5 Enabled  Disconnected    ActiveStore
15      Teredo Tunneling Pseudo-Inte... IPv6                  1280              50 Enabled  Disconnected    ActiveStore
13      WiFi                            IPv6                  1500              25 Enabled  Connected       ActiveStore
1       Loopback Pseudo-Interface 1     IPv6            4294967295              50 Disabled Connected       ActiveStore
31      vEthernet (SCCM INTERNAL)       IPv4                  1500               5 Enabled  Connected       ActiveStore
12      Ethernet                        IPv4                  1500               5 Enabled  Disconnected    ActiveStore
13      WiFi                            IPv4                  1500              25 Enabled  Connected       ActiveStore
1       Loopback Pseudo-Interface 1     IPv4            4294967295              50 Disabled Connected       ActiveStore
```

By using the **Get-NetIPInterface** powershell cmdlet we can get a list of all the installed interfaces, this includes the Interface index that we will use to reference the interface when making changes, it includes the interface alias and address family.

New-NetIPAddress



```
PS C:\>
PS C:\>
PS C:\> New-NetIPAddress -InterfaceAlias ETHERNET -IPAddress 90.0.0.1 -PrefixLength 24 -DefaultGateway 90.0.0.240

IPAddress         : 90.0.0.1
InterfaceIndex    : 12
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 90.0.0.1
InterfaceIndex    : 12
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore


PS C:\> _
```

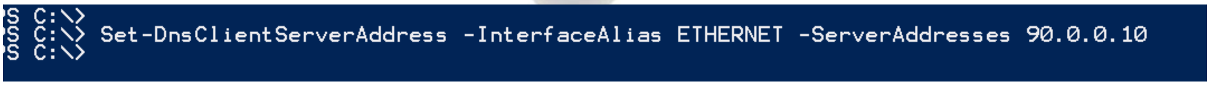
By using the **New-IPaddress** PowerShell cmdlet we can add a new IP address to an interface,

-InterfaceAlias is the name of the interface, -PrefixLength is the number of bits in the subnetmask

Use the **Set-NetIPaddress** to change the details of an address that has been added

Use **Set-NetIPInterface** to change interface settings such as DHCP state.

Set-DnsClientServerAddress



```
S C:\>
S C:\> Set-DnsClientServerAddress -InterfaceAlias ETHERNET -ServerAddresses 90.0.0.10
S C:\>
```

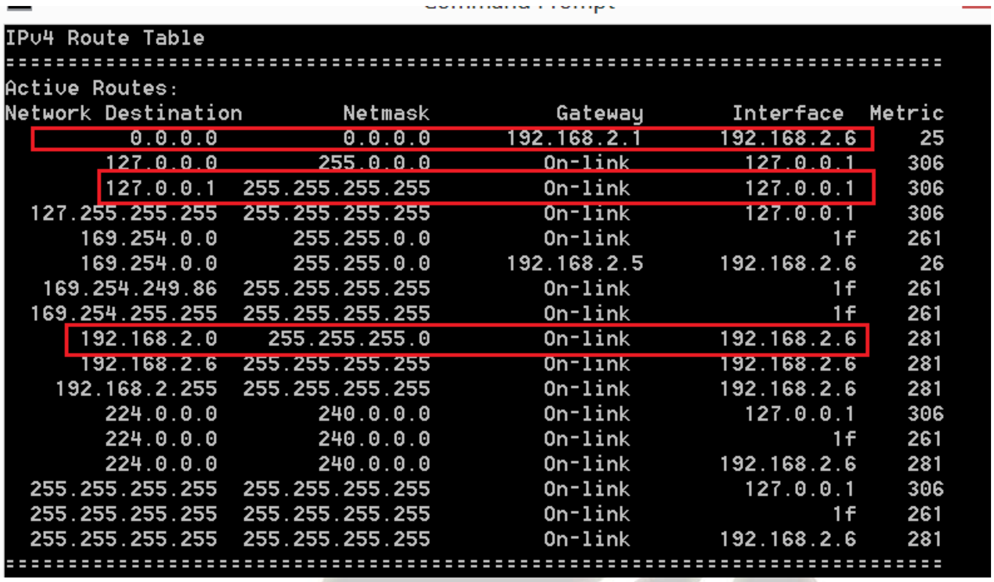
By using the **Set-DnsClientServerAddress** PowerShell cmdlet we can change the preferred and alternate DNS server address for a client/server.

Use **Set-DNSClient** to set suffix information

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
===========================================================================
```

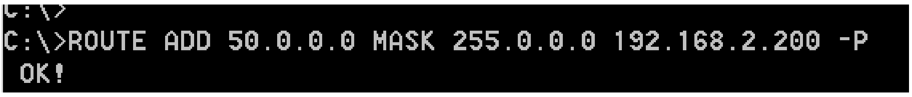
We can use the command **ROUTE PRINT** to see a hosts routing table

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,

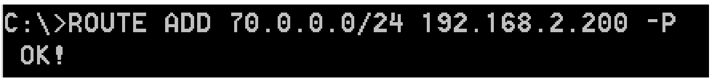
50.0.0.0 = the remote network address

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

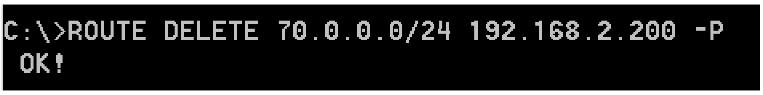
-p = Makes the route persistent in the host routing table

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



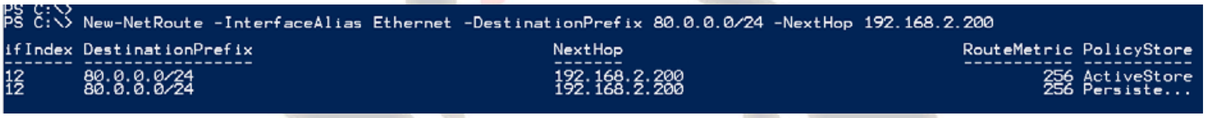
```
C:\>ROUTE DELETE 70.0.0.0/24 192.168.2.200 -P
 OK!
```

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...
```

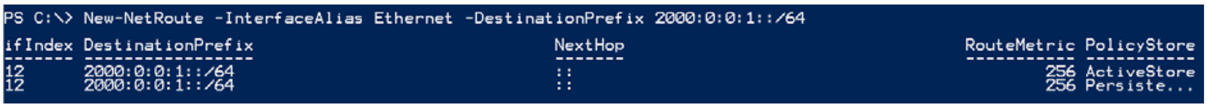
-InterfaceAlias = Interface display name (you could also use –InterfaceIndex), this is the exit interface in the host

-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

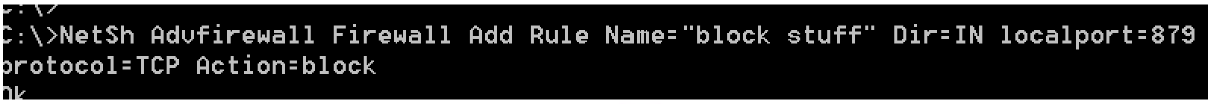
Remove-Netroute = Remove a route from the routing table

Configuring Windows Advanced Firewall with NETSH and PowerShell

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

<u>To configure a firewall rule with NetSH</u>

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

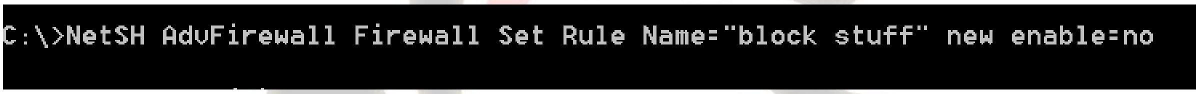


```
C:\>
C:\>NetSh Advfirewall Firewall Add Rule Name="block stuff" Dir=IN localport=879
protocol=TCP Action=block
Ok
```

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

<u>To Update and existing Firewall Rule with Netsh</u>

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

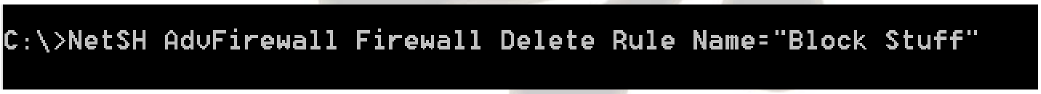


```
C:\>NetSH AdvFirewall Firewall Set Rule Name="block stuff" new enable=no
```

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.

<u>To Delete a Firewall Rule using Netsh</u>

NetSH AdvFirewall Firewall Delete Rule Name=*rulename*

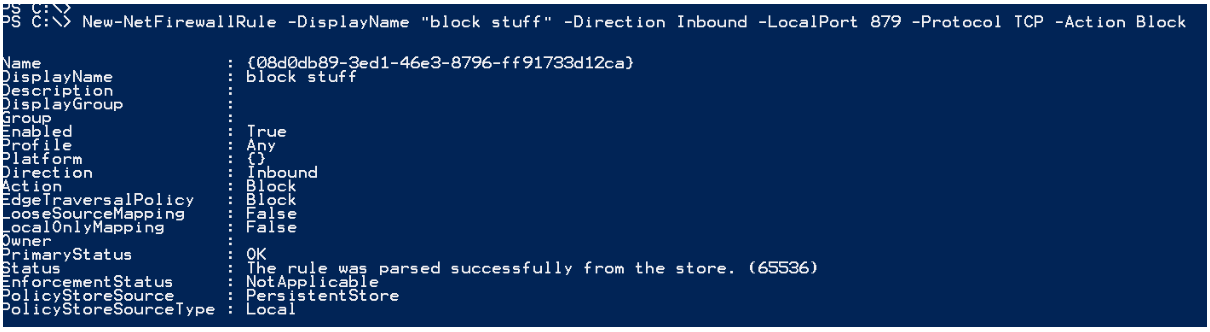


```
C:\>NetSH AdvFirewall Firewall Delete Rule Name="Block Stuff"
```

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

<u>To configure a firewall rule with PowerShell</u>

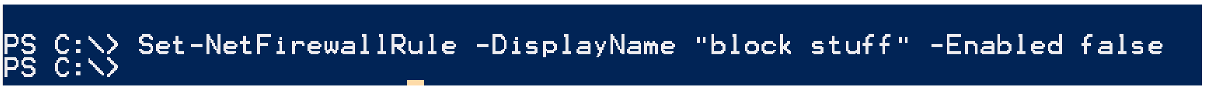
New-NetFirewallRule –displayname *displayname* –Direction *outbound/inbound* –Localport *localport* –Protocol *protocol* –Action *Block/Allow*



```
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*

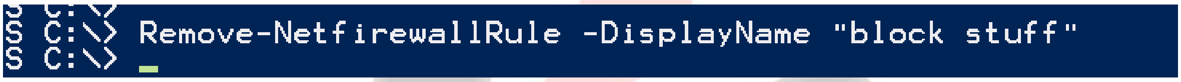


```
PS C:\> Set-NetFirewallRule -DisplayName "block stuff" -Enabled false
PS C:\>
```

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*



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

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

ADPREP.exe

ADPrep Extends the Active Directory® schema and updates permissions as necessary to prepare a forest and domain for a domain controller that run Server 2012. If you are adding a new Server 2012 machine that you will be using to create an additional DC for an existing domain then ADPREP and its relevant switches will be run for you. If you are performing an in place upgrade of an existing 2008 or 2008R2 Dc then you will have to run the ADPREP switches first

The switches include

ADPrep /ForestPrep

ADPrep /Domainprep

WDSUTIL.EXE

WDSUTIL is a command-line utility used for managing your Windows Deployment Services server

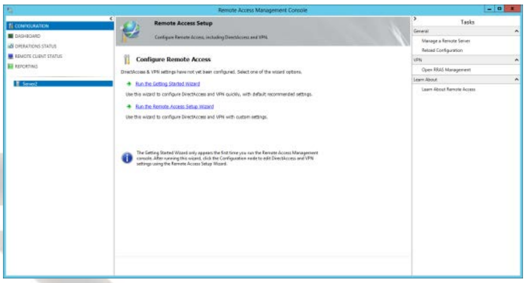
Command	Description
/ADD	Adds objects or prestages computers
/Copy	Copies an image or a driver group.
/Disable	Disables all services for Windows Deployment Services
/Disconnect-Client	Disconnects a client from a multicast transmission or namespace
/Enable	Enables all services for Windows Deployment Services
/Export-Image	Exports an image from the image store to a .wim file.
/Initialize-Server	Configures a Windows Deployment Services server for initial use.
/New	Creates new capture and discover images as well as multicast transmissions and namespaces.
/Replace-Image	Replaces a boot or installation image with a new version of that image.

Direct Access

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.



Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.

Configure Remote Access

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

Run the Getting Started Wizard

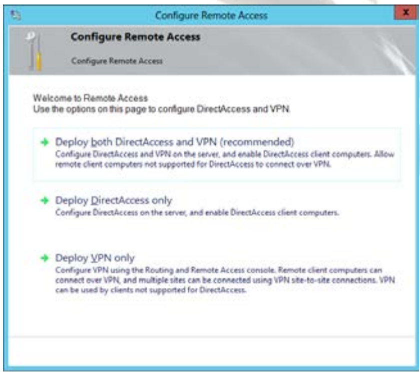
Use this wizard to configure DirectAccess and VPN quickly, with default recommended settings.

Run the Remote Access Setup Wizard

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

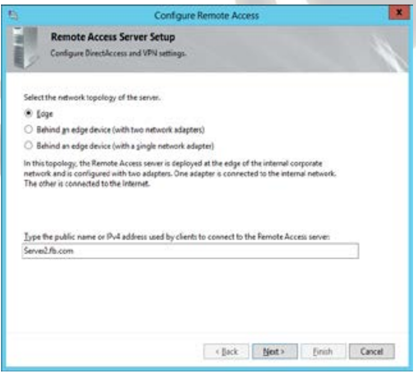
Configure Remote Access

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)

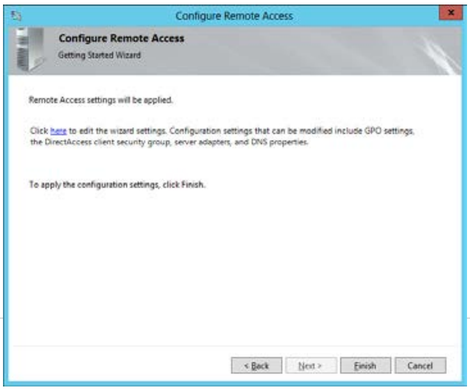
○ Behind an edge device (with a single network adapter)

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

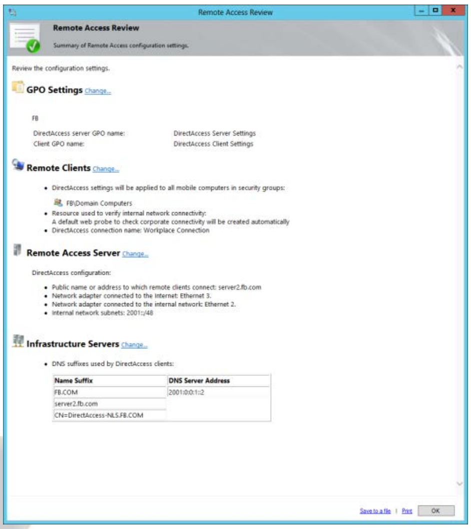
Remote Access settings will be applied.

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:

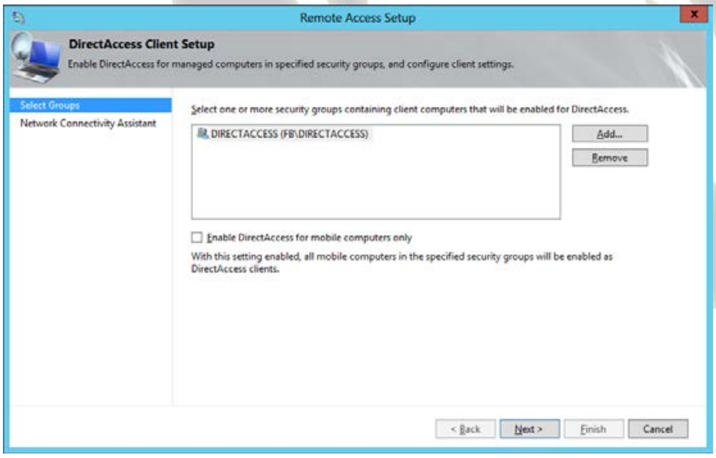
- Public name or address to which remote clients connect: server2.fb.com
- Network adapter connected to the Internet: Ethernet 3.
- Network adapter connected to the internal network: Ethernet 2.
- Internal network subnets: 2001::/48

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

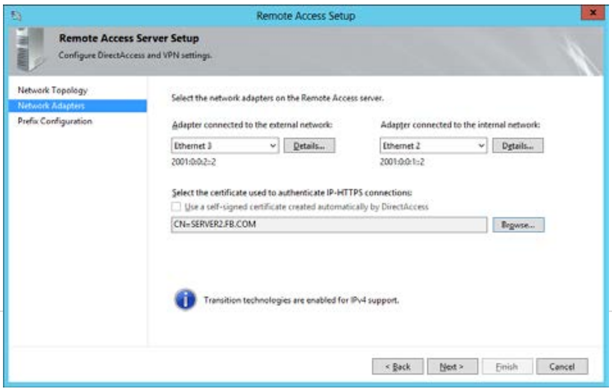
Enable DirectAccess for managed computers in specified security groups, and configure client settings.

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:

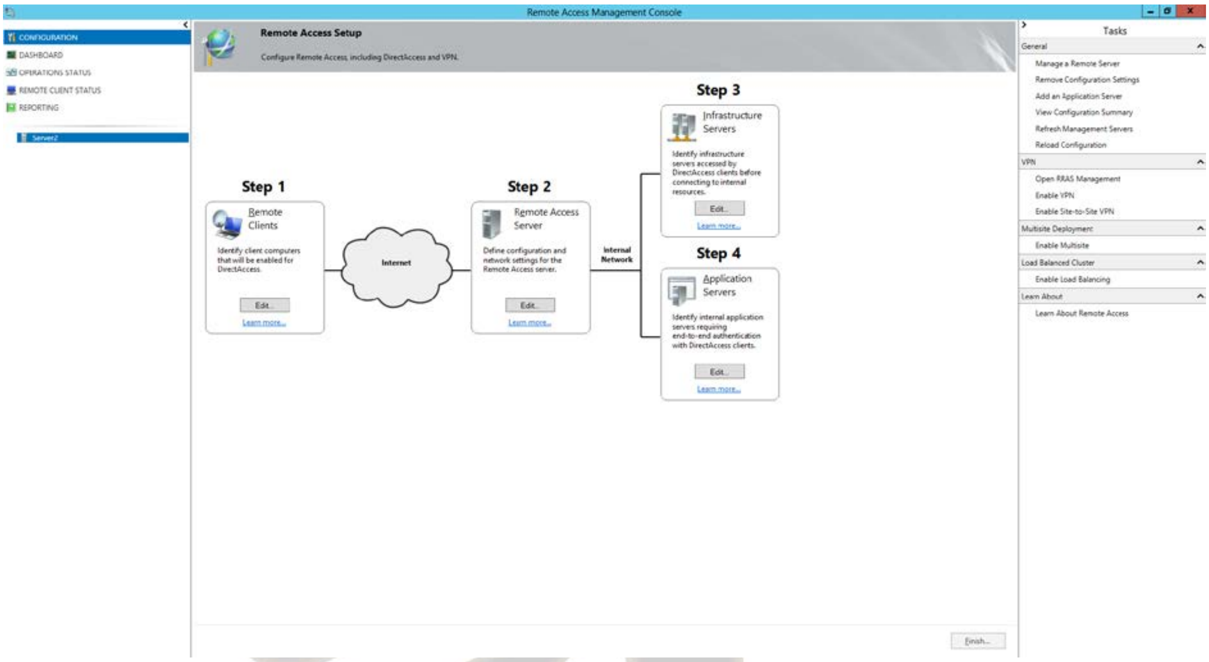
☐ Use a self-signed certificate created automatically by DirectAccess

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.



Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.

Step 1 – Remote Clients: Identify client computers that will be enabled for DirectAccess.

Step 2 – Remote Access Server: Define configuration and network settings for the Remote Access server.

Step 3 – Infrastructure Servers: Identify infrastructure servers accessed by DirectAccess clients before connecting to internal resources.

Step 4 – Application Servers: 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.

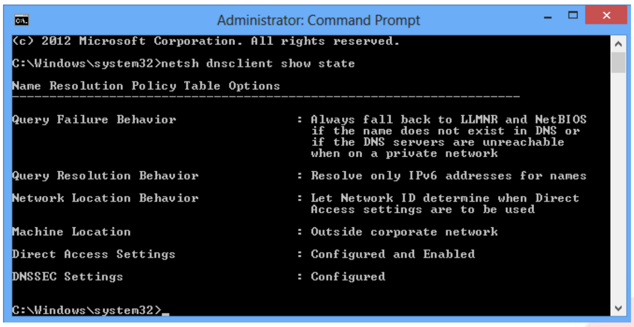
EXAM PREP – make sure you are happy with the wizard, the GPO settings, the WMI filter, the group used to apply the GPO to you clients.

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.

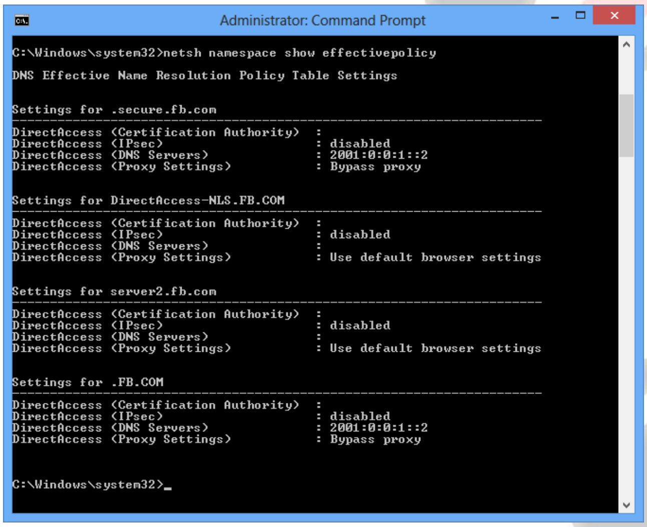
NetSH DNSCLIENT SHOW STATE


Administrator: Command Prompt

```
(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>_
```

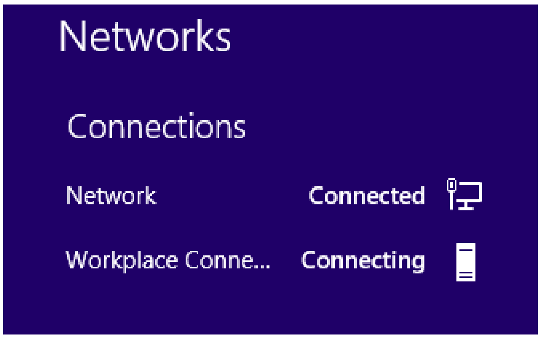
By using NetSh we can see we have a DirectAccess connection Configured and Enabled

NetSH NAMESPACE SHOW EFFECTIVEPOLICY


Administrator: Command Prompt

```
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

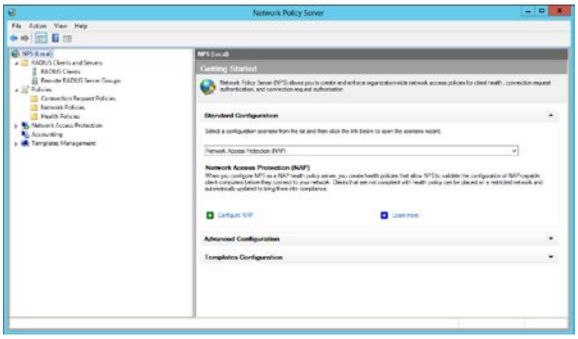
Connections

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

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.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

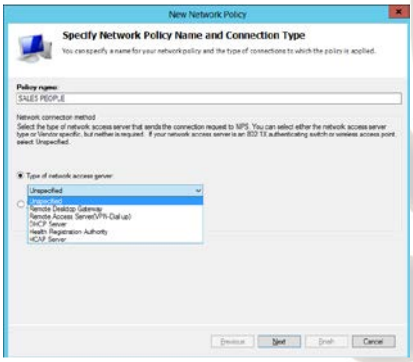
Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

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.



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

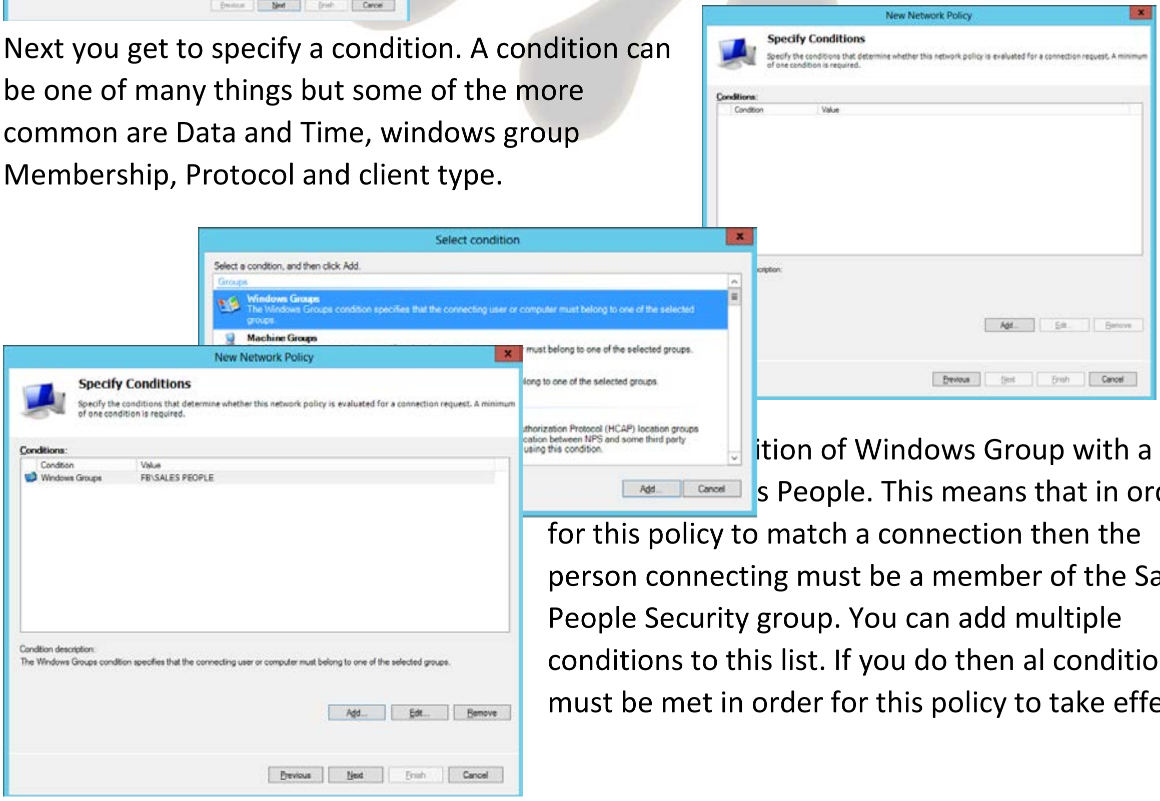
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point select Unspecified.

● 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.



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 a condition, and then click Add.

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

Machine Groups
must belong to one of the selected groups.

long to one of the selected groups.

thorization Protocol (HCAP) location groups cation between NPS and some third party using this condition.

Specify Conditions

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

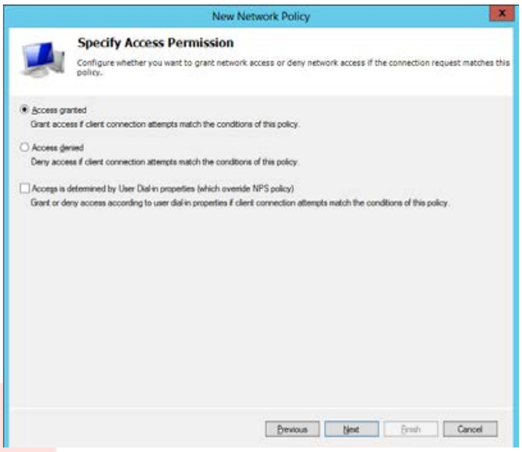
Conditions:

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

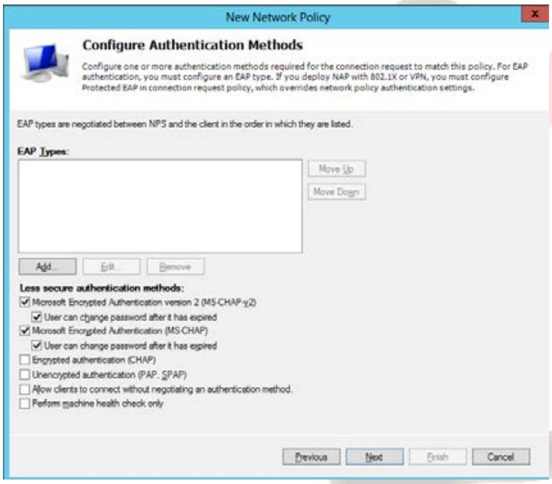
Specify Access Permission

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.



New Network Policy

Configure Authentication Methods

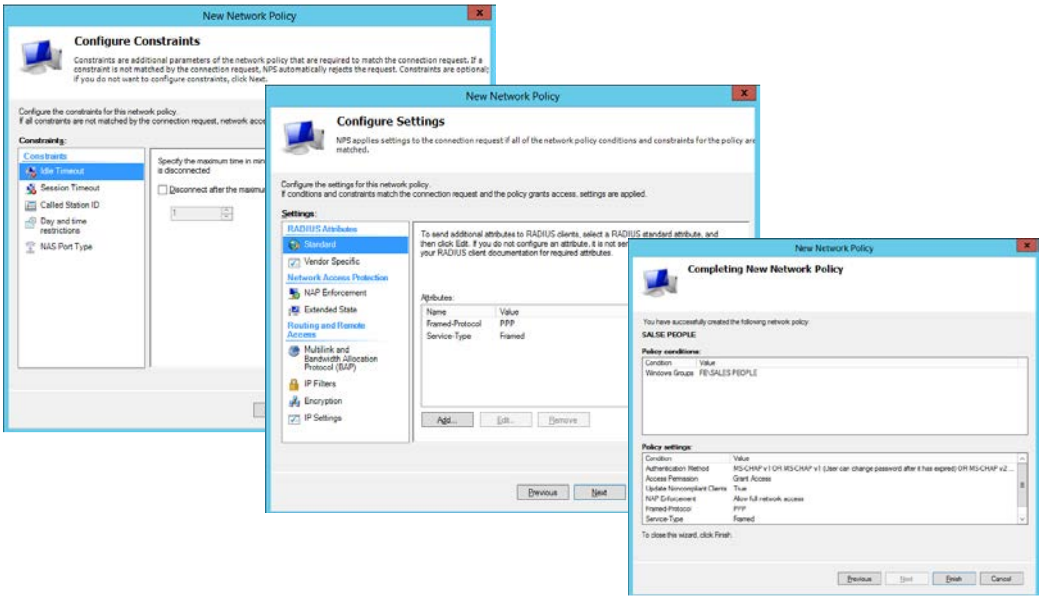
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication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



New Network Policy

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

New Network Policy

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 se
your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

SALSE PEOPLE

Policy conditions:

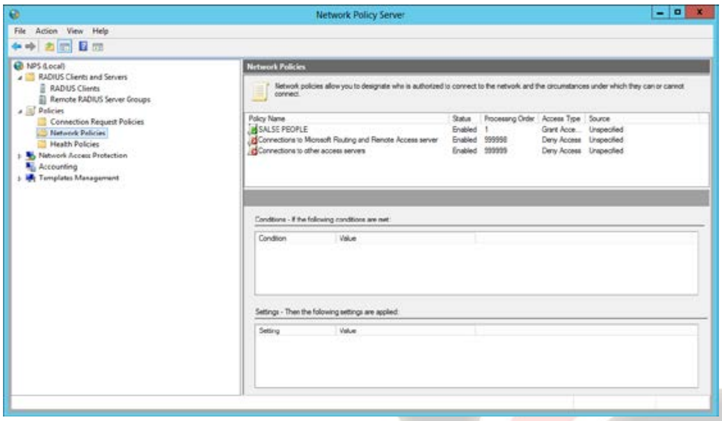
Condition	Value
Windows Groups	FB\SALES PEOPLE

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:

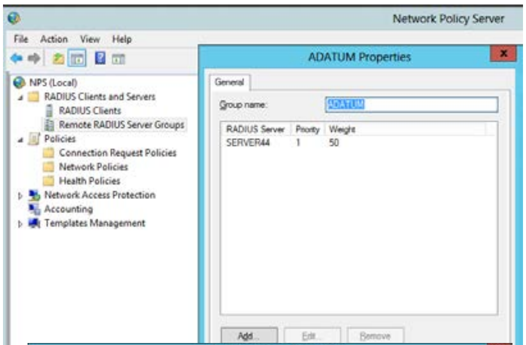
Condition	Value

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.

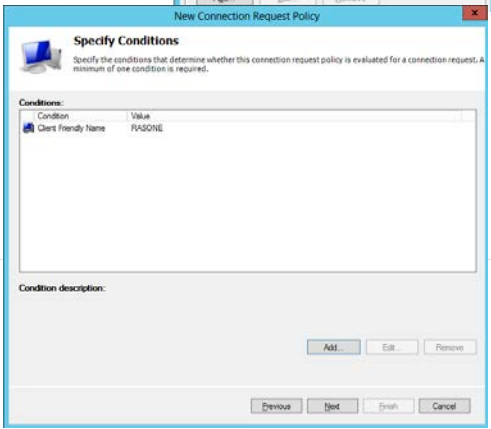
If you want you NPS server to act as a RADIUS Proxy then you must configure **Connection Request Policies.**



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:

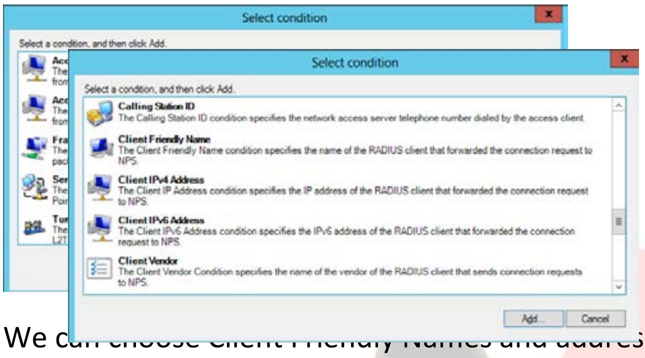
Condition	Value
Client Friendly Name	RASONE

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.

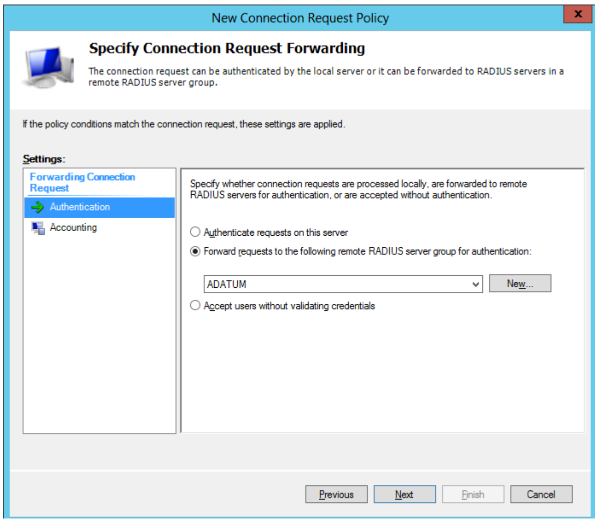
Client Vendor
The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connection requests to NPS.

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.



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.

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.

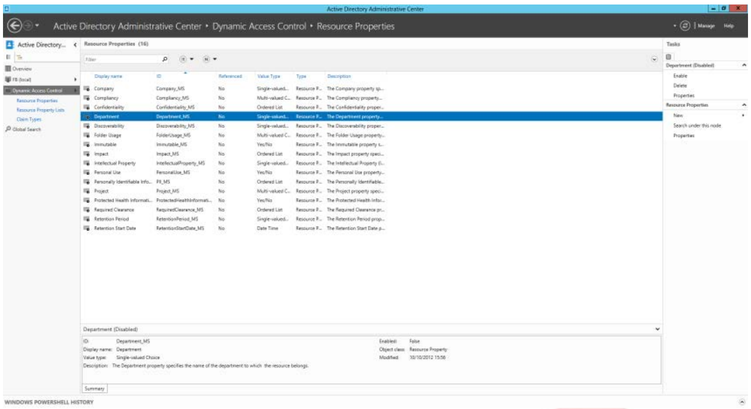
Claim Types – As Microsoft administrators we are used to providing access to our resources based on the information inside access tokens. This would typically be users SIDs and Group SIDs but there is a wealth of other information that can be used, if you look at an average user account and take a look 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.



Active Directory Administrative Center

Active Directory Administrative Center • Dynamic Access Control • Resource Properties

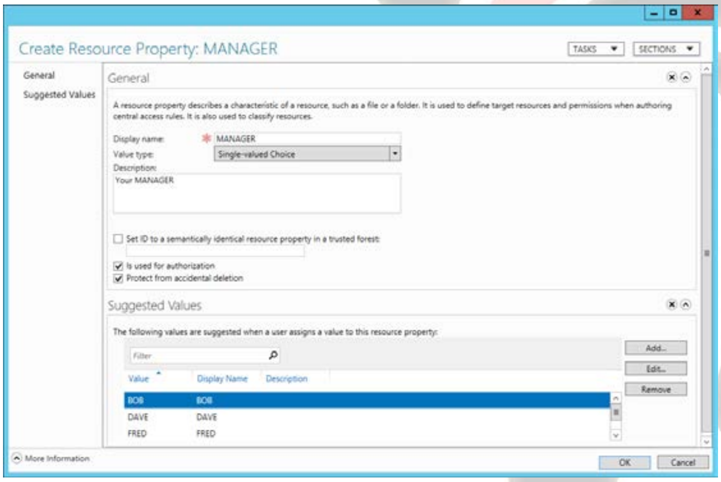
Resource Properties (16)

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 15:56

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

General

A resource property describes a characteristic of a resource, such as a file or a folder. It is used to define target resources and permissions when authoring central access rules. It is also used to classify resources.

Display name: MANAGER
Value type: Single-valued Choice
Description: Your MANAGER

☐ Set ID to a semantically identical resource property in a trusted forest:

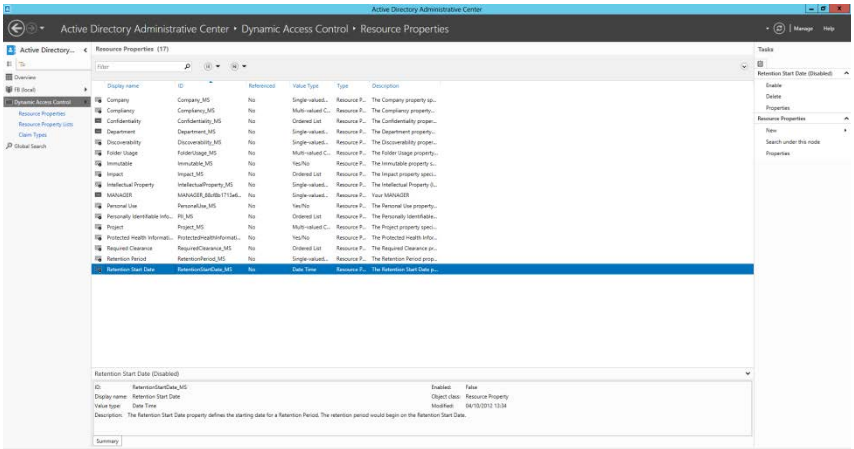
☑ Is used for authorization
☑ Protect from accidental deletion

Suggested Values

The following values are suggested when a user assigns a value to this resource property:

Value	Display Name	Description
BOB	BOB	
DAVE	DAVE	
FRED	FRED	

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.



Active Directory Administrative Center

Active Directory Administrative Center • Dynamic Access Control • Resource Properties

Resource Properties (17)

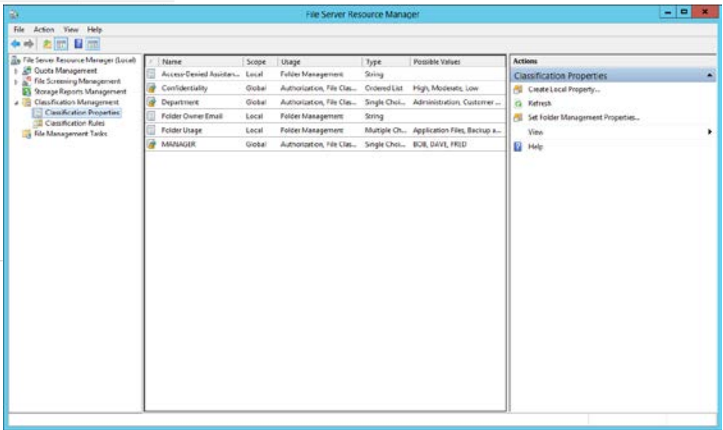
Display name	ID	Referenced	Value Type	Type	Description
Company	Company_MS	No	Single-valued...	Resource P...	The Company property sp...
Compliancy	Compliancy_MS	No	Multi-valued C...	Resource P...	The Compliancy property...
Confidentiality	Confidentiality_MS	No	Ordered List	Resource P...	The Confidentiality 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

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.

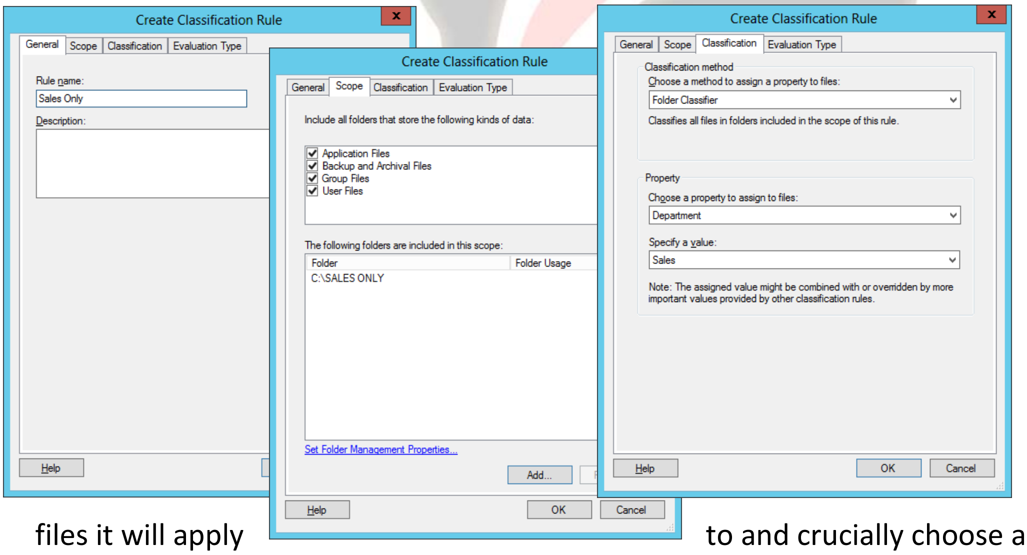


File Server Resource Manager

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

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

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.

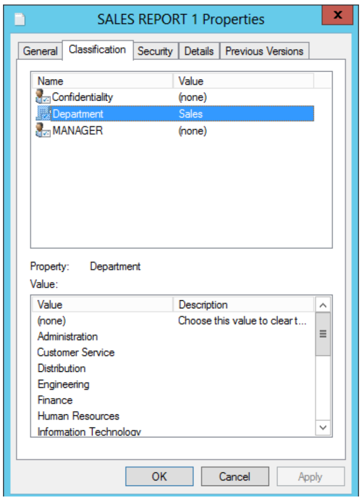
Property

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

General | Classification | Security | Details | Previous Versions

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

Property: Department

Value:

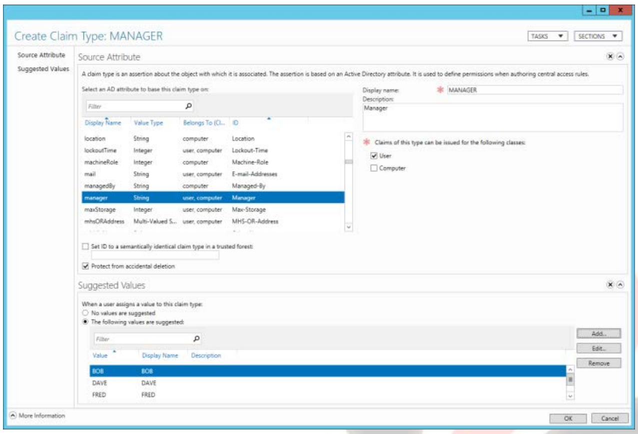
Value	Description
(none)	Choose this value to clear t...
Administration	
Customer Service	
Distribution	
Engineering	
Finance	
Human Resources	
Information Technology	

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.



Create Claim Type: MANAGER

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

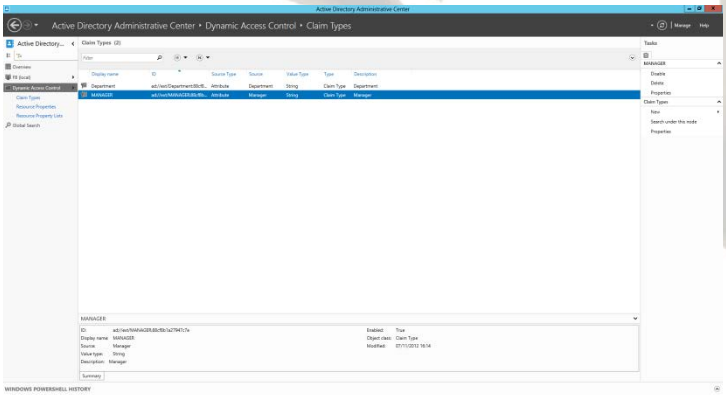
□ Set ID to a semantically identical claim type in a trusted forest:
☑ Protect from accidental deletion

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.



Active Directory Administrative Center

Active Directory Administrative Center • Dynamic Access Control • Claim Types

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

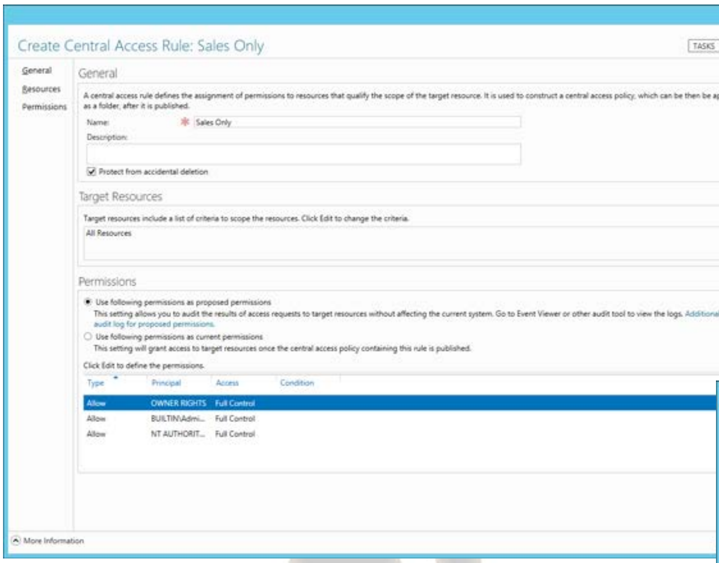
Here you can see our new Claim has been added to the list of claims. Also I have created a second claim called Department

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.

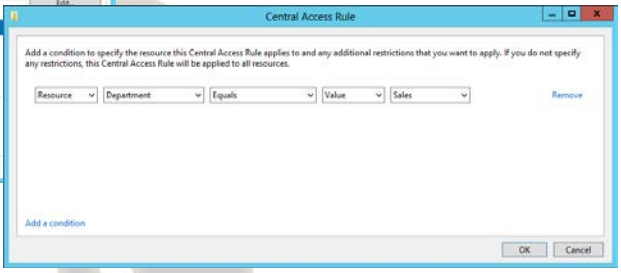
○ Use following permissions as current permissions

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

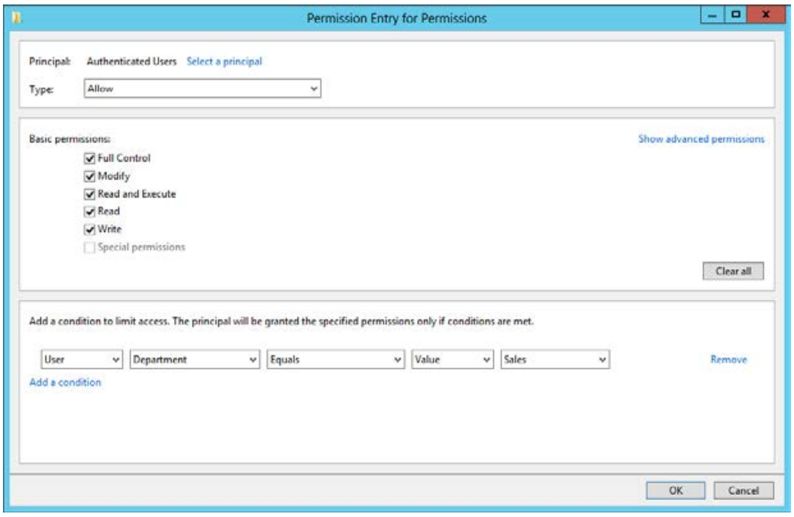


Central Access Rule

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.

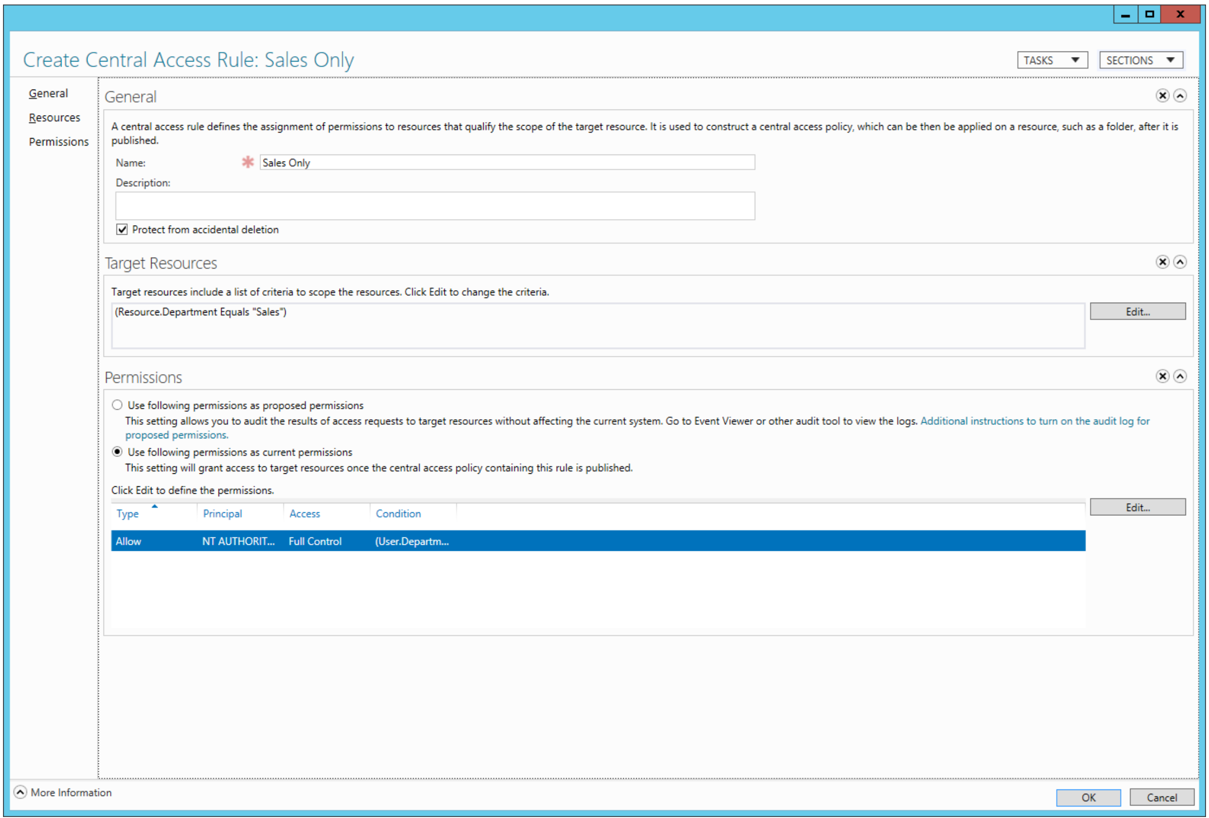
User | Department | Equals | Value | Sales

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



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.

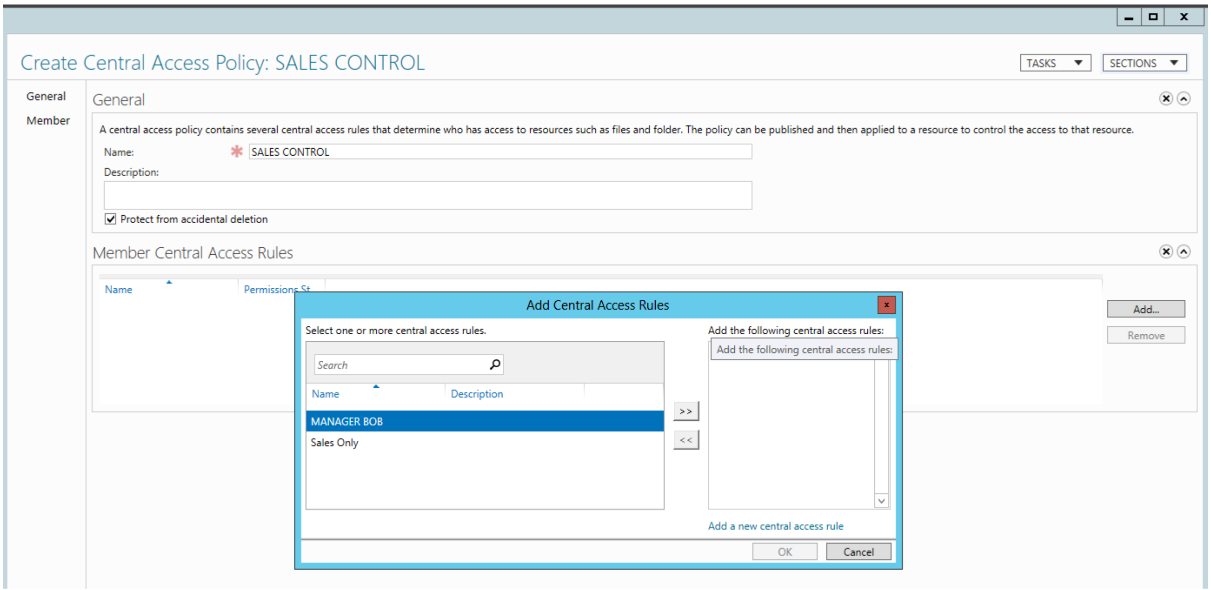
● Use following permissions as current permissions
This setting will grant access to target resources once the central access policy containing this rule is published.

Click Edit to define the permissions.

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

2nd Access rule

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

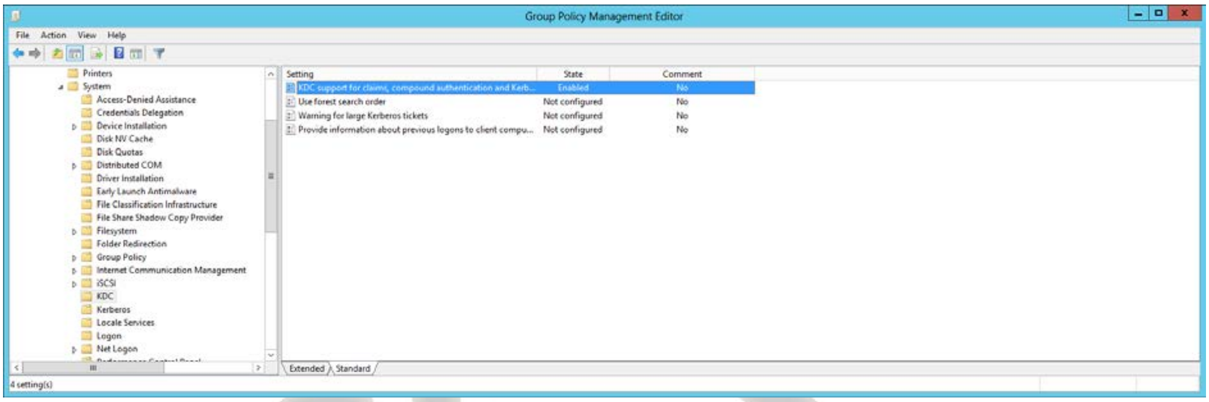
1) We create Claims
2) We Create Access Rules
3) We Create Central Access policies
4) We Create/Edit GPOS
5) We apply Central Access policies to files and folders

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

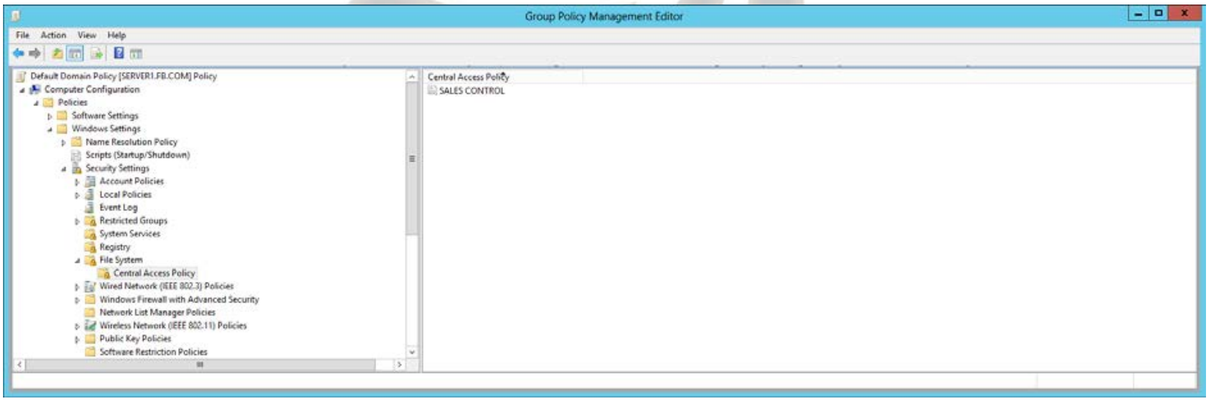
Computer\Administrative Templates\System\KDC



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

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

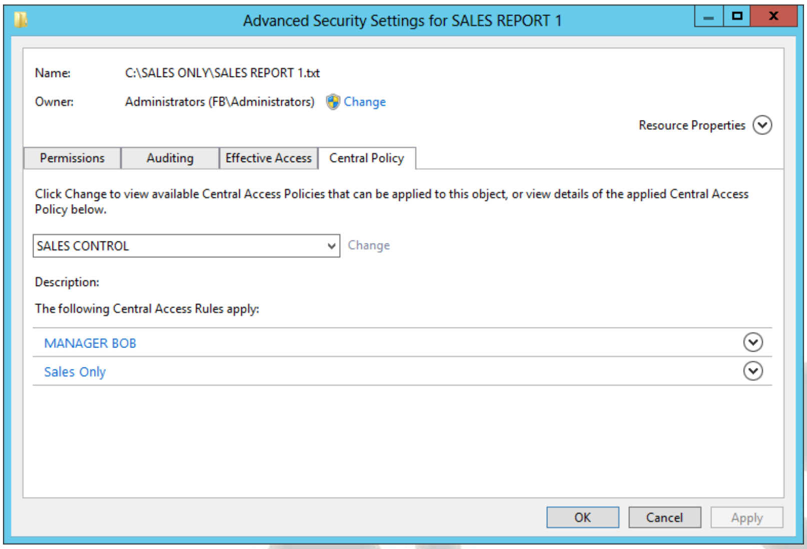
Computer\Windows\Settings\Security\File System


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:

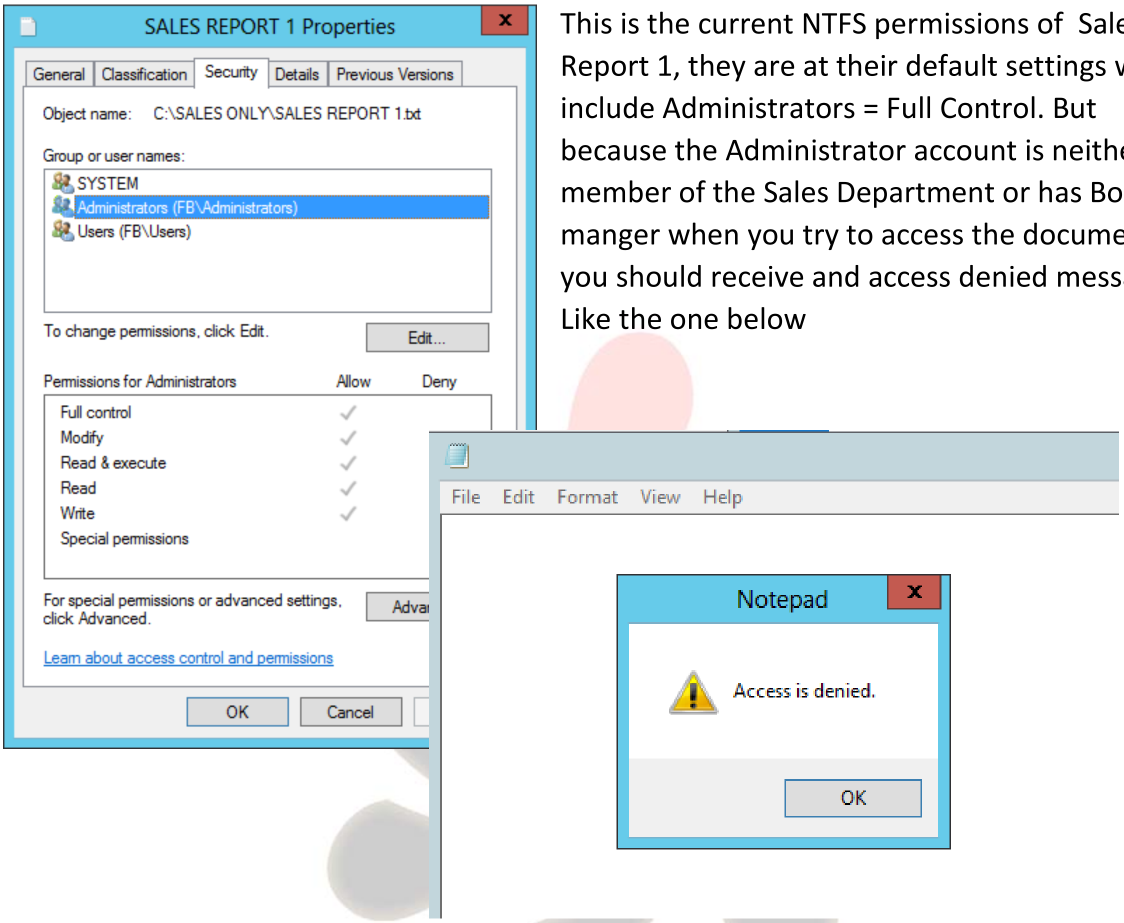
MANAGER BOB

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.

TESTING

This 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



SALES REPORT 1 Properties

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

Group or user names:

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

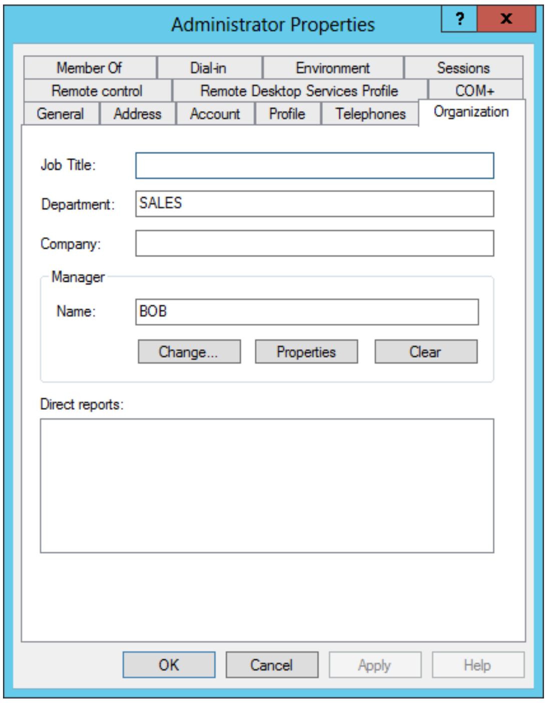
To change permissions, click Edit.

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

For special permissions or advanced settings, click Advanced.

Notepad

Access is denied.



Administrator Properties

Job Title:

Department: SALES

Company:

Manager

Name: BOB

Direct reports:

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)

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?

Windows Server 2012 Hyper-V High Availability and Migration Features

Options

Virtual Machine and Storage Migration

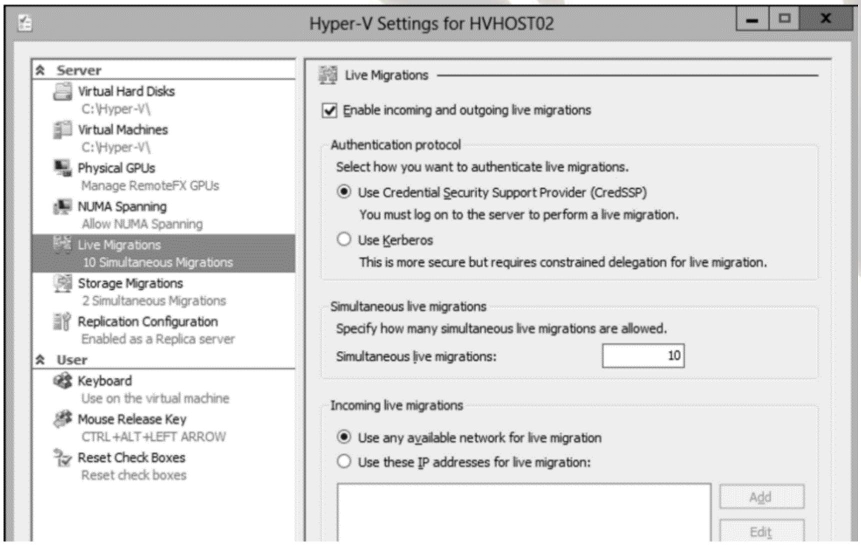
With Windows Server 2012 Microsoft has introduce a new feature that allows you to migrate a running virtual machine and its storage to a new location without first needing to Cluster the Hyper-V host servers. This type of migration is sometimes called shared nothing migration. To enable this type of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

<u>Step 1</u>

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

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

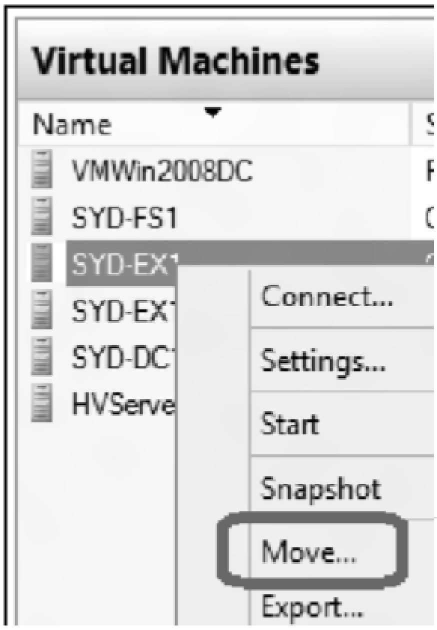
● Use any available network for live migration

○ Use these IP addresses for live migration:

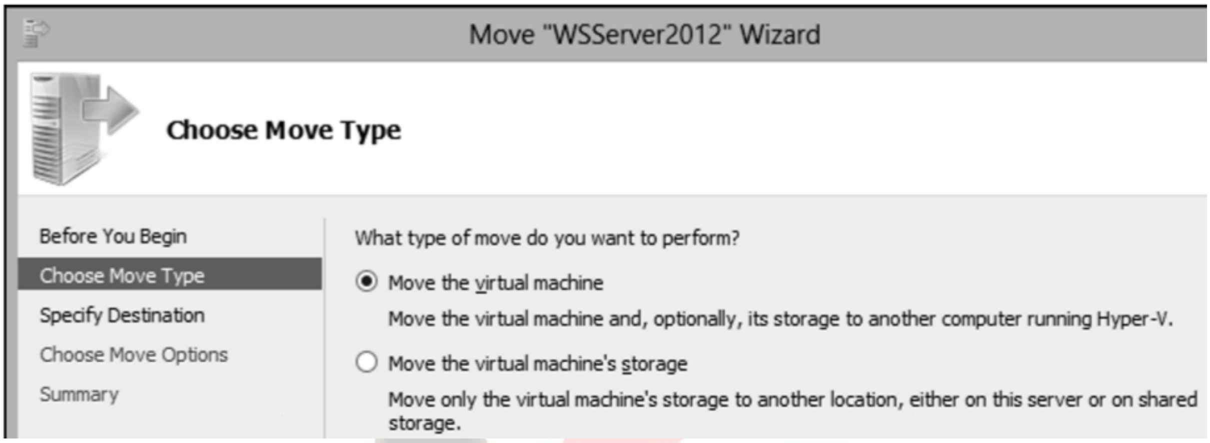
<u>Step 2</u>

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?

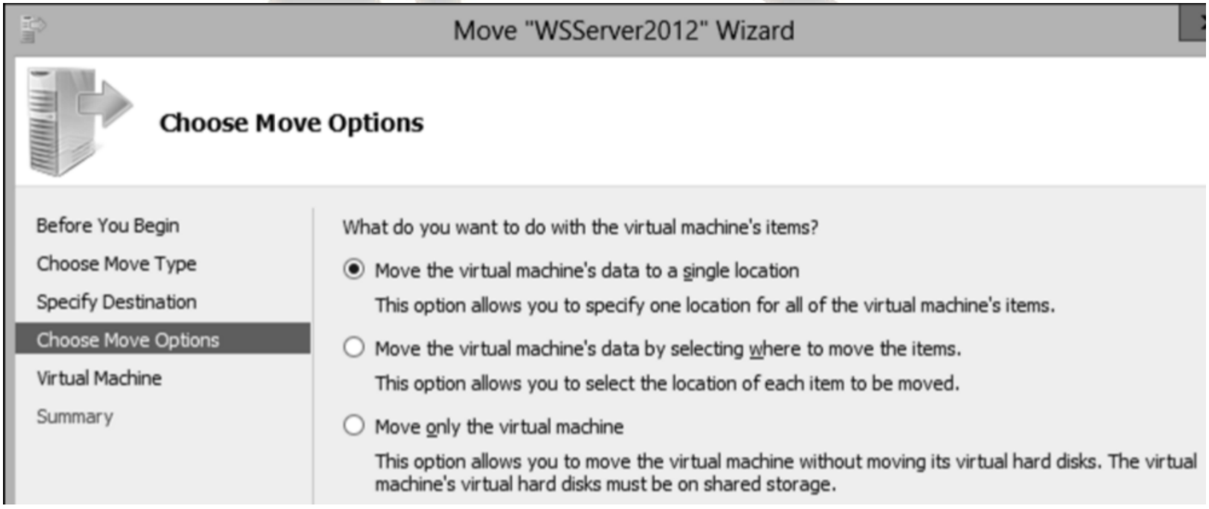
● Move the virtual machine

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

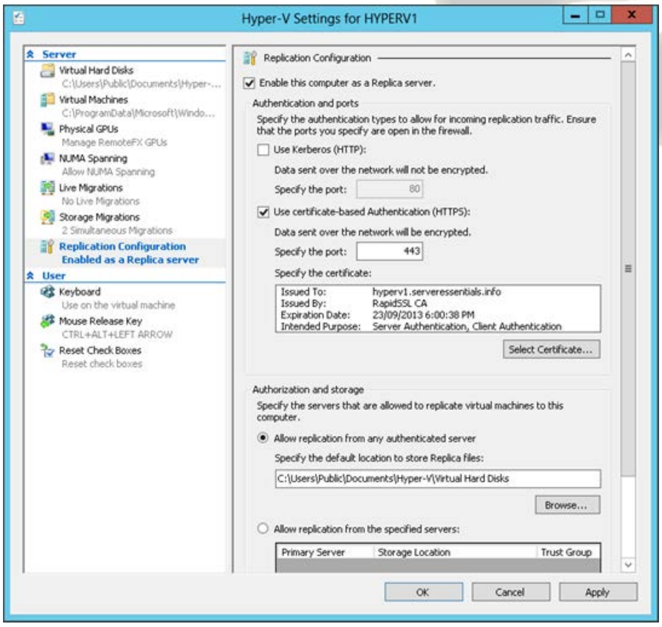
Hyper-V Replica provides asynchronous replication of Hyper-V virtual machines between two hosting servers. It is simple to configure and does not require either shared storage or any particular storage hardware. Any server workload that can be virtualized in Hyper-V can be replicated. Replication works 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.



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

Authorization and storage

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

● Allow replication from any authenticated server

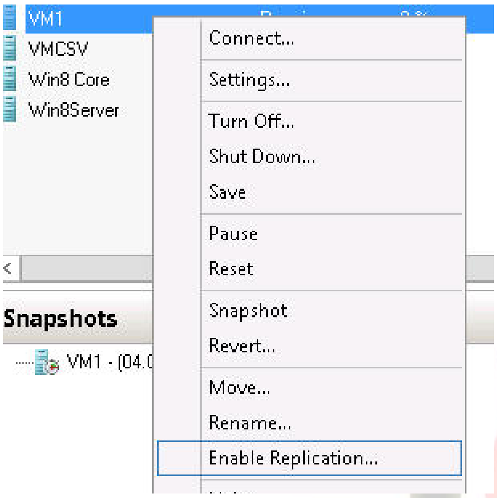
Specify the default location to store Replica files:

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

○ Allow replication from the specified servers:

Primary Server	Storage Location	Trust Group

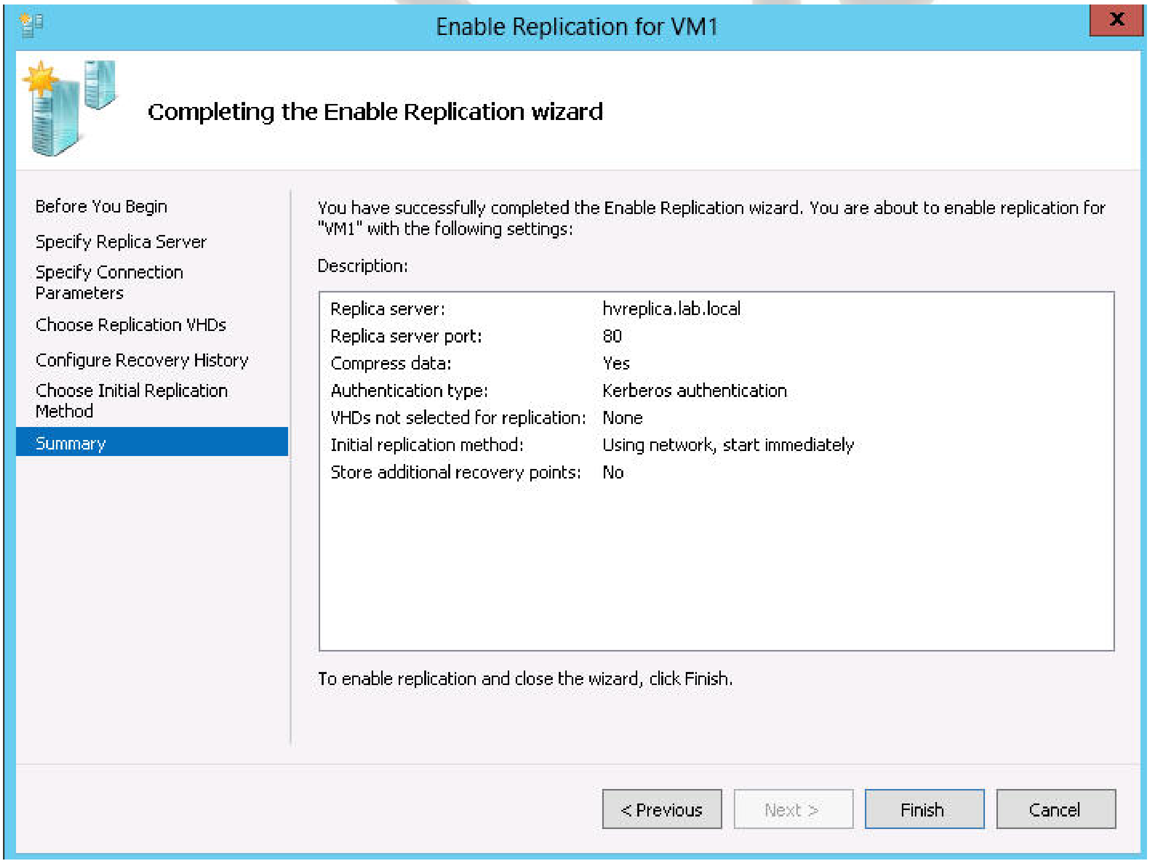
Enabling Hyper-V Replica requires first of all enabling Replication Configuration on the Hyper-V server you wish to replicate to. Here we can see Hyper-V Settings and the Replication Configuration section. Here we can enable this computer as a Replica Server, we can specify the type of authentication 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
Before You Begin
Specify Replica Server
Specify Connection Parameters
Choose Replication VHDs
Configure Recovery History
Choose Initial Replication Method
Summary
< Previous
Next >
Finish
Cancel

Completing the Enable Replication wizard

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.

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.

PowerShell Web Access Gateway

Windows PowerShell® Web Access, first introduced in Windows Server® 2012, acts as a Windows PowerShell gateway, providing a web-based Windows PowerShell console that is targeted at a remote computer. It enables IT Pros to run Windows PowerShell commands and scripts from a Windows PowerShell console in a web browser, with no Windows PowerShell, remote management software, or browser plug-in installation necessary on the client device. All that is required to run the web-based Windows PowerShell console is a properly-configured Windows PowerShell Web Access gateway, and a client device browser that supports JavaScript® and accepts cookies.

After successful gateway setup and configuration, users can access a Windows PowerShell console by using a web browser. When users open the secured Windows PowerShell Web Access website, they can run a web-based Windows PowerShell console after successful authentication.

Windows PowerShell Web Access setup and configuration is a three-step process:

1. Installing Windows PowerShell Web Access

   Install-WindowsFeature –Name WindowsPowerShellWebAccess -ComputerName <computer_name> -IncludeManagementTools -Restart

2. Configuring the gateway

   Install-PswaWebApplication

3. Configuring authorization rules that allow users access to the web-based Windows PowerShell console

   Add-PswaAuthorizationRule

Additional Server 2012 PowerShell CMDLETS

GPO CMDLETS

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	Links a GPO to a site, domain, or OU.
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

DISM CMDLETS

The Deployment Image Servicing and Management (DISM) platform is used to mount and service Windows® images before deployment. A subset of DISM commands can be used on online Windows images. You can use DISM tools to mount, and get information about, Windows image (.wim) files or virtual hard disks (.vhd or .vhdx). You can also use it to install, uninstall, configure, and update Windows features, packages, and drivers in a Windows image or to change the edition of a Windows image.

CMDLET	Description
Add-AppxProvisionedPackage	Adds an app package (.appx) that will install for each new user to a Windows image.
Add-WindowsDriver	Adds a driver to an offline Windows image
Enable-WindowsOptionalFeature	Enables a feature in a Windows image.
Mount-WIM	Mounts a Windows image in a WIM or VHD file to a directory on the local computer.
Set-WindowsProductKey	Sets the product key for a Windows image

AD CS Administration Cmdlets

The CA administration cmdlets can only be run on a computer that has the CA role service installed.

CMDLET	Description
Add-CATemplate	Adds a certificate template to the CA
Add-CACrlDistributionPoint	Adds a certificate revocation list (CRL) distribution point uniform resource indicator (URI) where the CA publishes certification revocations.
Add-CAAuthorityInformationAccess	Configures Authority Information Access (AIA) or Online Certificate Status Protocol (OCSP) URI on a CA.

Active Directory Domain Services Cmdlets

You can use the Active Directory module cmdlets to perform various administrative, configuration, and diagnostic tasks in your AD DS and AD LDS environments.

CMDLET	Description
Enable-ADOptionalFeature	Enables an Active Directory Optional Feature
New-ADServiceAccount	Creates a new Active Directory managed service account or group managed service account object
Install-ADServiceAccount	Installs an Active Directory managed service account on a computer or caches a group managed service account on a computer
Add-ADComputerServiceAccount	Adds one or more service accounts to an Active Directory computer
New-AdFineGrainedPasswordPolicy	Creates a new Active Directory fine grained password policy
Set-ADFineGrainedPasswordPolicy	Modifies an Active Directory fine grained password policy.
Set-ADUser	Modifies an Active Directory user
New-Aduser	Creates a new Active Directory user.

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

Note.

The above are examples of CMDLETS, hopefully they give you an idea of the range of CMDLETS available for you to use. For a more complete list of all the CMDLETS available for Windows Server 2012 go to the following site:

http://technet.microsoft.com/en-gb/library/hh801904.aspx

Glossary of Additional Command Line tools

TOOL NAME	Description
Auditpol	Displays information about and performs functions to manipulate audit policies.
BCDBoot	Enables you to quickly set up a system partition, or to repair the boot environment located on the system partition.
BCDEdit	BCDEdit is a command-line tool for managing BCD stores. It can be used for a variety of purposes, including creating new stores, modifying existing stores, adding boot menu parameters, and so on.
Cacls	Displays or modifies discretionary access control lists (DACL) on specified files.
Certreq	Certreq can be used to request certificates from a certification authority (CA), to retrieve a response to a previous request from a CA, to create a new request from an .inf file, to accept and install a response to a request, to construct a cross-certification or qualified subordination request from an existing CA certificate or request, and to sign a cross-certification or qualified subordination request.
Certutil	Certutil.exe is a command-line program that is installed as part of Certificate Services. You can use Certutil.exe to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.
Cipher	Displays or alters the encryption of directories and files on NTFS volumes. If used without parameters, **cipher** displays the encryption state of the current directory and any files it contains.
DCGPOfix	Recreates the default Group Policy Objects (GPOs) for a domain
DFSRMIG	The `dfsrmig` command migrates SYSVOL replication from File Replication Service (FRS) to Distributed File System (DFS) Replication, provides information about the progress of the migration, and modifies Active Directory Domain Services (AD DS) objects to support the migration.
Gpfixup	Fix domain name dependencies in Group Policy Objects and Group Policy links after a domain rename operation
GpResult	Displays the Resultant Set of Policy (RSoP) information for a remote user and computer.
NETDOM	Enables administrators to manage Active

	Directory domains and trust relationships from the command prompt.
NsLookup	Displays information that you can use to diagnose Domain Name System (DNS) infrastructure.
Redircmp	Redirects the default container for newly created computers to a specified, target organizational unit (OU) so that newly created computer objects are created in the specific target OU instead of in CN=Computers.
Redirusr	Redirects the default container for newly created users to a specified, target organizational unit (OU) so that newly created user objects are created in the specific target OU instead of in CN=Users.
Rendom	Rendom.exe is a command-line tool that is used to rename Active Directory domains
Repadmin	Repadmin.exe helps administrators diagnose Active Directory replication problems between domain controllers running Microsoft Windows operating systems.
ROUTE	Displays and modifies the entries in the local IP routing table
Secedit	Configures and analyzes system security by comparing your current configuration to specified security templates.
SetSPN	Reads, modifies, and deletes the Service Principal Names (SPN) directory property for an Active Directory service account. You use SPNs to locate a target principal name for running a service. You can use **setspn** to view the current SPNs, reset the account's default SPNs, and add or delete supplemental SPNs.
Wecutil	Enables you to create and manage subscriptions to events that are forwarded from remote computers, which support WS-Management protocol.
Wevtutil	Enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs.
Winrs	Windows Remote Management allows you to manage and execute programs remotely.

NOTE: This is not a complete list of Windows Server tools, for more information about these tools including examples and a complete list of tools follow this link:

http://technet.microsoft.com/en-us/library/cc754340.aspx