

1.1 Design an automated server installation strategy

Microsoft Assessment and Planning Toolkit

The Microsoft Assessment and Planning Toolkit (MAP) is an agentless, automated, multi-product planning and assessment tool for quicker and easier desktop, server and cloud migrations. MAP provides detailed readiness assessment reports with extensive hardware and software information, and actionable recommendations to help organizations accelerate their IT infrastructure planning process, and gather more detail on assets that reside within their current environment.

MAP performs four key functions: discovery and inventory of computers and applications, hardware and software migration readiness assessments, software usage tracking, and capacity planning for virtualization, public and private cloud migration.

1.2 Plan and implement a server deployment infrastructure

Windows Deployment Services (WDS): enables you to deploy Windows operating systems over the network, which means that you do not have to install each operating system directly from a CD or DVD.

Azure:

Download and import publish settings and subscription information (certificate authentication)

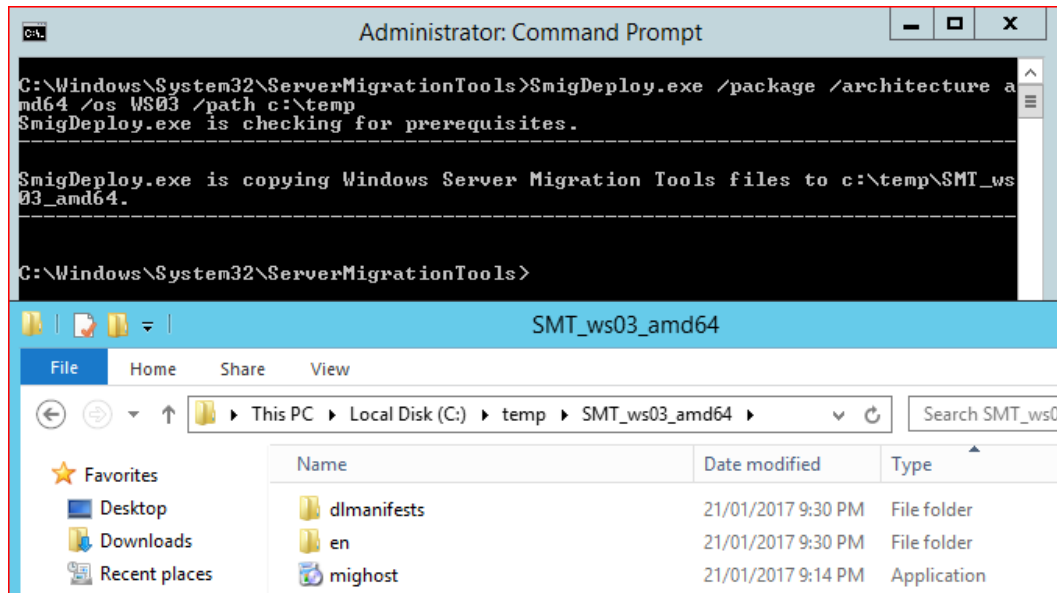
- Installed the Windows Azure PowerShell module by running the Microsoft Web Platform Installer
- At the Windows PowerShell command prompt, type the following command, and then press Enter.
`Get-AzurePublishSettingsFile`
A web browser opens at <https://windows.azure.com/download/publishprofile.aspx> for signing in to Windows Azure.
- Sign in to the Windows Azure Management Portal, and then follow the instructions to download your Windows Azure publishing settings. Save the file as a .publishsettings type file to your computer.
- In the Windows Azure PowerShell window, at the command prompt, type the following command, and then press Enter.
`Import-AzurePublishSettingsFile <mysettings>.publishsettings`

1.3 Plan and implement server upgrade and migration

Windows server migration tools

Windows Server Migration Tools installation and preparation can be divided into the following stages.

1. Installing Windows Server Migration Tools on destination servers that run Windows Server 2012 R2 or Windows Server 2012.
`Install-WindowsFeature Migration –ComputerName DC1`
Or
Use the “Add Roles and Features Wizard” to add the **Windows Server Migration Tools** to your destination machine
2. Creating deployment folders on migration destination servers, for copying to source servers.
`C:\Windows\System32\ServerMigrationTools\smigdeploy.exe`
Windows Server 2008 R2
`SmigDeploy.exe /package /architecture amd64 /os WS08R2 /path <deployment folder path>`
Windows Server 2003 64bit
`SmigDeploy.exe /package /architecture amd64 /os WS03 /path <deployment folder path>`



3. Copying deployment folders from destination servers to source servers.
4. Registering Windows Server Migration Tools on source servers.
 Microsoft .NET Framework 2.0 is installed on computers that are running Windows Server 2003.
 Windows PowerShell 1.0 or a later version is installed on source computers
 1- On our source computer (in our case **W2K8R2-1**) open a command window with elevated privileges,
 2- Change to "**C:\Mig Tools Folder\SMT_ws08R2_amd64**" and type "**SMIGDEPLOY.EXE**"

Migrate print queue

To manage the migration process, use one of the following:

- The Printer Migration Wizard, which you access through Print Management, a snap-in in Microsoft Management Console (MMC).
- The Printbrm.exe command-line tool.

You can perform the migration locally or remotely, and from either a client computer or server.

The Printer Migration Wizard migrates:

- Print queues.
- Shared printer settings.
- Printer drivers in use by the print spooler.
- Any security settings specific to the installed printer.

Printbrm.exe command-line tool

Backup:

Printbrm -s [\\<Server>](#) Computer1> -b -f <Printer1 Settings>.printerExport

Restore:

Printbrm -s [\\<Server>](#) Computer1> -r -f <Printer1 Settings>.printerExport

Migrate DHCP

- Stop DHCP server
- **Export-SmigServerSetting -featureID DHCP -User All -Group -path [\\Canitpro-dc2k12\DHCPShare - Verbose](#) and press enter to export the DHCP data.** In here featureID define the server role. Once enter the command it will ask a password to protect the data.


```

PS C:\WIN2K3MIG\SMT_us03_x86> Export-SmigServerSetting -featureID DHCP -User All
-Group -path \\Canitpro-dc2k12\DHCPShare -Verbose

cmdlet Export-SmigServerSetting at command pipeline position 1
Supply values for the following parameters:
Password: *****

      ItemType ID                Success DetailsList
      -----
WindowsFeature DHCP              True {}
OSSetting Local User             True {}
OSSetting Local Group            True {}

PS C:\WIN2K3MIG\SMT_us03_x86> _

```

- Now to import DHCP data type **Import-SmigServerSetting -featureID DHCP -Force -path C:\DHCPShare -Verbose** and press enter. Here C:\DHCPShare is the folder path where we save the DHCP data from windows server 2003. It will ask the password to enter which we have define during the export DHCP server data process

Migrate File Server

Supported migration scenarios

- File server data and file shares are located in a storage area network (SAN) or other external storage location that preserves data and file share permissions (except data for local users and groups)
- File server data and file shares are located on the server disk (direct-attached storage) that is preserving data and files shares permissions
- DFS Namespaces
- File Server Resource Manager
- iSCSI Software Target
- Network File System (NFS) file shares
- Shadow Copies of Shared Folders

DFS Namespace

FSUtil.exe target remove <[\\SourceServer\Namespace](#)>

Migrate data

Destination server

Receive-SmigServerData

Source server

Send-SmigServerData -ComputerName <DestinationServer> -SourcePath d:\users -DestinationPath d:\shares\users -Recurse -Include All -Force

Migrate local users and groups

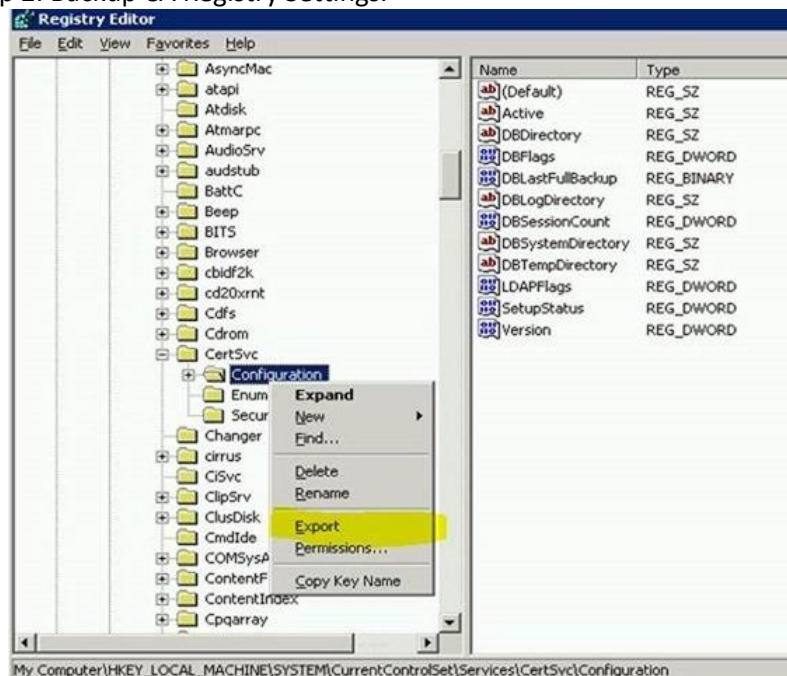
Export-SmigServerSetting -User All -Group -Path <storepath\UsersGroups> -Verbose
 Import-SmigServerSetting -User All -Group -Path <storepath\UsersGroups> -Verbose

Migrate CA

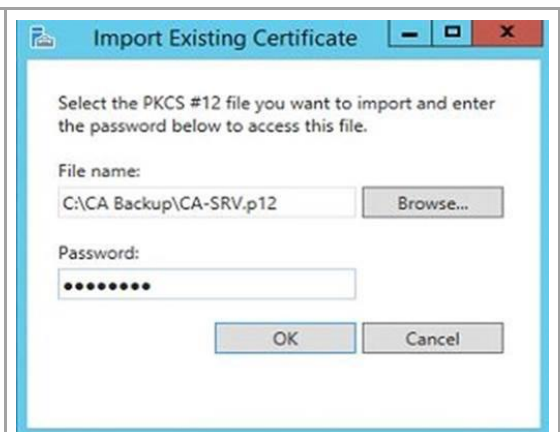
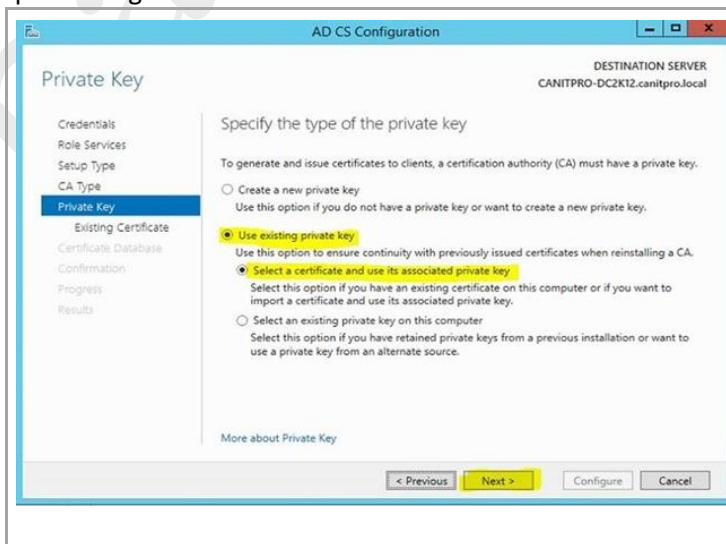
- Step 1: Backup Windows Server 2003 certificate authority database and its configuration.



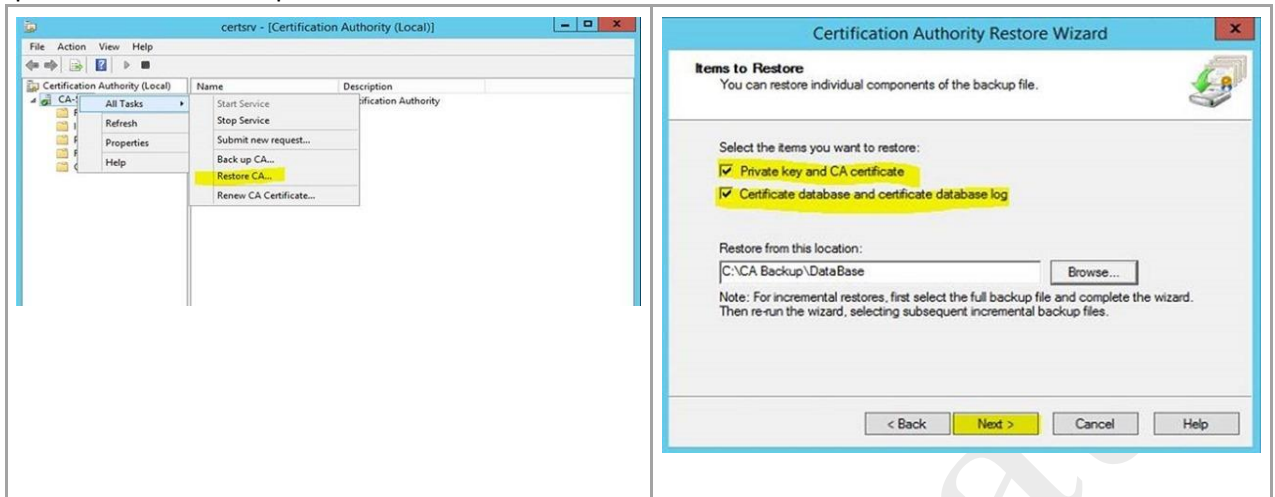
- Step 2: Backup CA Registry Settings.



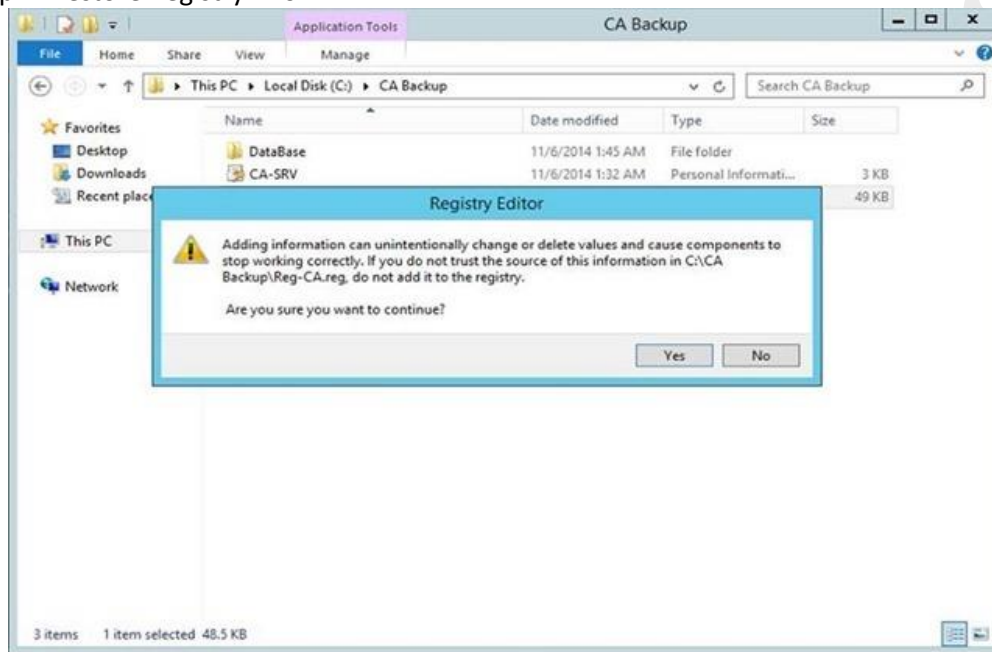
- Step 3: Uninstall CA Service from Windows Server 2003.
- Step 4: Install Windows Server 2012 R2 Certificate Services.
- Step 5: Configure AD CS.



- Step 6: Restore CA Backup.

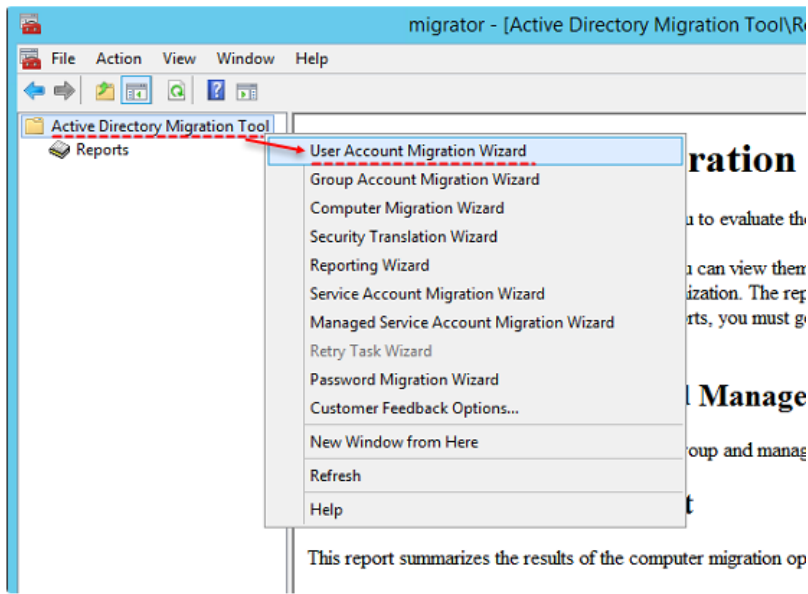


- Step 7: Restore Registry info.



Active Directory Migration Tool

You can use ADMT to migrate objects in Active Directory forests. This tool includes wizards that automate migration tasks, such as migrating **users, groups, service accounts, computers, and trusts** and performing **security translation**.



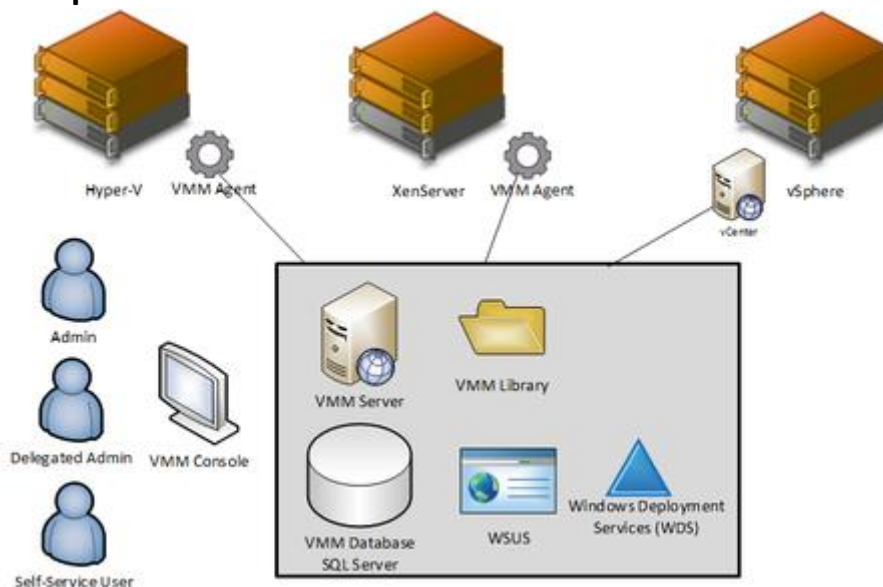
Password Export Server:

The PES service can be installed on any writable domain controller in the source domain that supports 128-bit encryption.

Because ADMT does not check all settings of the target domain password policy, users need to explicitly set their password after migration unless the **Password never expires** or **Smartcard is required for interactive logon** flags are set.

1.4 Plan and deploy Virtual Machine Manager services:

Components of VMM 2012



The VMM Self-Service Portal was deprecated in VMM 2012 and removed from VMM 2012 SP1. There are several alternatives:

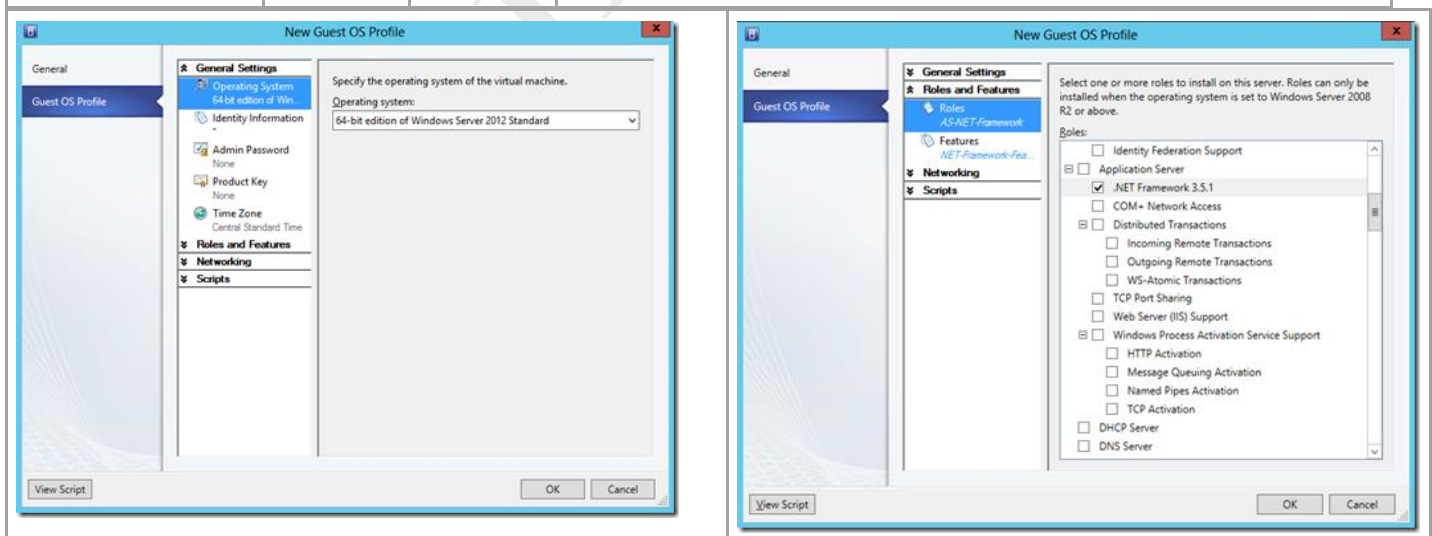
- **App Controller 2012 SP1:** This provides a new portal that also provides access to company-controlled subscriptions to third-party and Microsoft-offered public cloud services.
- **System Center & Orchestrator:** This is the larger private cloud offering for large enterprises, which integrates all of System Center and other parts of IT infrastructure through runbooks.
- **Windows Azure Services for Windows Server:** Originally intended for public clouds, this portal is gathering interest for private cloud implementations.

In Virtual Machine Manager (VMM), a service is a set of virtual machines that are configured and deployed together and are managed as a single entity—for example, a deployment of a multi-tier line-of-business application.

In Virtual Machine Manager (VMM), a profile is a "building block" containing some of the specifications that go into creating a new virtual machine or virtual machine template. You can use profiles to simplify the process of creating templates.

Templates help you to quickly create virtual machines with consistent hardware and operating system settings. Templates can also be used to restrict the virtual machine settings that are available to self-service users who create new virtual machines. A virtual machine template typically consists of a hardware profile, an operating system profile, and a virtual hard disk, which will be used by the virtual machine that is created from the template. The virtual hard disk might be stored in the VMM library, or it might be a disk from an existing virtual machine.

VMM Profile	VM Template	Service Template	Note
Hardware profile	x		Specify CPU, RAM and so on.
Guest OS profile	x		Specify OS details such as domain-join info, computer name, and roles or features to be installed on the destination VMs.
Application profile		x	Contains the instructions for installing and configuring applications on VMs.
SQL Server profile		x	Contains instructions for installing Microsoft SQL Server on VMs.
Physical computer profile			Physical computer profile replaces host profile in SCVMM 2012 R2 and used to provision servers via VMM.
Capability profile	x	x	Capability profile is used via hardware profile and used in cloud deployment scenario.



The **New-SCVirtualMachine** cmdlet creates a virtual machine to be managed by Virtual Machine Manager (VMM). You can create a virtual machine from an existing stopped virtual machine deployed on a host, from an existing virtual machine stored in the VMM library, from a virtual machine template, from an existing virtual hard disk that already contains an operating system, or from a blank virtual hard disk. For example, you can create a new virtual machine from an existing hard disk that contains a third-party operating system, such as Linux.

1.5 Plan and implement file and storage services:

Deduplication requirements:

- Server 2012 <
- Must not be a system or boot volume
- Must be NTFS. NOT FAT, ReFS
- Must be a non-removable drive
- Less than 64TB
- Server 2012 no CSV. 2012 R2 supports CSV

Windows Offloaded Data Transfers

Windows Offloaded Data Transfer (ODX) functionality in Windows maximizes an enterprise's investment in intelligent storage arrays by enabling the arrays to directly transfer data within or between compatible storage devices, bypassing the host computer.

By offloading the file transfer to the storage array, ODX minimizes latencies, maximizes array throughput, and reduces resource usage such as CPU and network consumption on the host computer. Windows offloads file transfers transparently and automatically when you move or copy files, irrespective of whether you drag-and-drop files through File Explorer or use command-line file copy commands.

Some of the applications of ODX include:

- Rapidly import and export Hyper-V virtual machines that are stored on an ODX-capable storage array and accessed via iSCSI, Fibre Channel, or SMB file shares
- Transfer large files such as database files or video files with increased speed and decreased CPU and network resource consumption on the host server

Requirements

- Must be connected by using one of the following protocols:
 - iSCSI
 - Fibre Channel
 - Fibre Channel over Ethernet
 - Serial Attached SCSI (SAS)
 - IDE Not Supported

The computer initiating the data transfer must be running Windows Server 2012 R2, Windows Server 2012, Windows 8.1, or Windows 8.

File system filter drivers such as antivirus and encryption programs need to opt-in to ODX. ODX is not supported by the following file system filter drivers:

- Data Deduplication
- BitLocker Drive Encryption

Files must be on an **unencrypted basic partition**. **Storage Spaces** and **dynamic volumes** are not supported.

Validate file system filter drivers

To use ODX, validate all the file system filter drivers on all servers that are hosting the storage support ODX.

- On each server on which you want to use ODX, list all of the file system filter drivers that are attached to the volume on which you want to enable ODX.

Fltmc instances -v <volume>

- For each filter driver listed, query the registry to determine whether the filter driver has opted-in to ODX support.
`Get-ItemProperty hklm:\system\currentcontrolset\services\<FilterName> -Name "SupportedFeatures"`
 If the **SupportedFeatures** registry value equals **3**, the filter driver supports ODX.

Disable ODX on the server

Check whether ODX is currently enabled (it is by default) by verifying that the **FilterSupportedFeaturesMode** value in the registry equals **0**.

`Get-ItemProperty hklm:\system\currentcontrolset\control\filesystem -Name "FilterSupportedFeaturesMode"`

Disable ODX support.

`Set-ItemProperty hklm:\system\currentcontrolset\control\filesystem -Name "FilterSupportedFeaturesMode" -Value 1`

Mounting an NFS shared resource to a drive letter

`mount [-oOptions] \ComputerName\ShareName {DeviceName | *}`

DeviceName | * The drive letter to assign to the mounted shared resource. The asterisk (*) means to use the next available letter.

-o anon Mounts as anonymous user.

-o nolock Disables locking. This option might improve performance if you only need to read files.

ISCSI:

Microsoft iSCSI Software Target

iSCSI Initiator

iSCSI Software Target

Windows Storage Server

Ethernet switch connecting Gigabit Ethernet

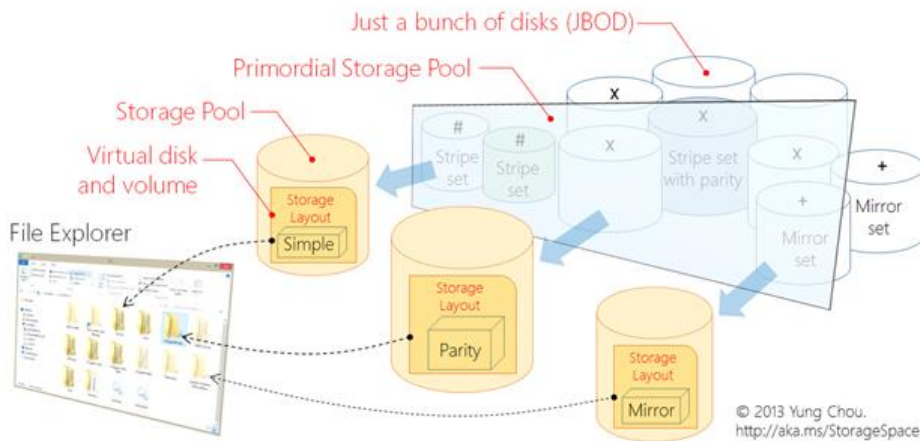
iSCSI: An Internet Protocol (IP) based storage networking standard for linking data storage facilities.

iSCSI Targets are instances of hard disk storage that connect over IP or Ethernet networks. Targets listen to initiator commands and perform the required I/O.

iSCSI Target - (Microsoft iSCSI Software Target)\iSCSI Targ

Virtual Disk Index	Description	Size
Virtual Disk 0	Disk1	1.00 GB
Virtual Disk 1	Disk2	1.00 GB

Windows Server 2012 Storage Virtualization Concept



Powershell:

Set-FileStorageTier

The **Set-FileStorageTier** cmdlet assigns a file to a specified storage tier. Assigning a file to a tier is also called pinning the file to a tier. To pin a file to a storage tier, the file must be on a volume that is hosted by the same tiered storage space. If you pin a file that is already assigned to a different tier, the file changes assignment the next time tier optimization takes place.

Get-FileStorageTier

The **Get-FileStorageTier** cmdlet gets all the files assigned to a Storage tier on a tiered volume stored on a tiered Storage space, and the status of each file. A file that you assign to a Storage tier is called a pinned file. The possible status values are the following:

- Not on tier
- Completely on tier
- Partially on tier

2.1 Design and maintain a Dynamic Host Configuration Protocol (DHCP) solution:

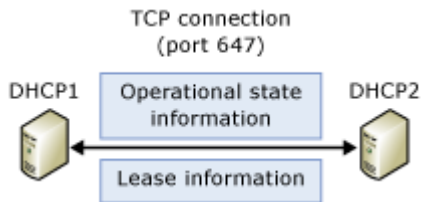
DHCP Failover Modes:

Hot standby mode

In hot standby mode, two servers operate in a failover relationship where an active server is responsible for leasing IP addresses and configuration information to all clients in a scope or subnet. The partner server assumes a standby role, with responsibility to issue leases to DHCP clients only if the active server becomes unavailable. Hot standby mode is ideal for scenarios where the failover partner is only intended to be used temporarily when the active server is unavailable.

Load balance mode

Load balance mode is the default mode of deployment. In this mode, two DHCP servers simultaneously serve IP addresses and options to clients on a given subnet. DHCP client requests are load balanced and shared between the two DHCP servers. The default load balancing ratio between the two servers is 50:50, but this can be customized to any ratio from 0 to 100%.



Setting	Description
Name	Name of the failover relationship. The name of the failover relationship must be unique on the local server.
Partner server	Name or IP address of the server that shares the failover relationship with the local DHCP server.
Mode	The type of DHCP failover mode chosen.
Load balance percentage	The percentage of DHCP client leases that will be evaluated by the local server.
Server role	The role of the local server in hot standby mode, either active or standby .
Reserve percentage	The percentage of IP addresses in a scope that are reserved for the hot standby server.
Maximum client lead time (MCLT)	The maximum amount of time that one server can extend a lease for a DHCP client beyond the time known by the partner server.
State switchover interval	The interval after which a DHCP server automatically transitions its failover partner to a partner down state after loss of communication.
State	The current state of the local server.
Scope IDs	A list of DHCP scope IDs that are associated with the failover relationship.
Automatic state transition	If a state switchover interval is configured, then automatic state transition is enabled. By default, automatic state transition is disabled.
Enable authentication	Whether or not a shared secret is required between failover partners.

To deploy DHCP Failover, you need to have two computers running Windows Server 2012 or higher. If you have any DHCP servers running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003, then you will need to first migrate these to Windows Server 2012.

Configure Failover

Create a new failover relationship

Create a new failover relationship with partner dhcp1.contoso.com

Relationship Name:

Maximum Client Lead Time: hours minutes

Mode:

Load Balance Percentage

Local Server: %

Partner Server: %

☐ State Switchover Interval: minutes

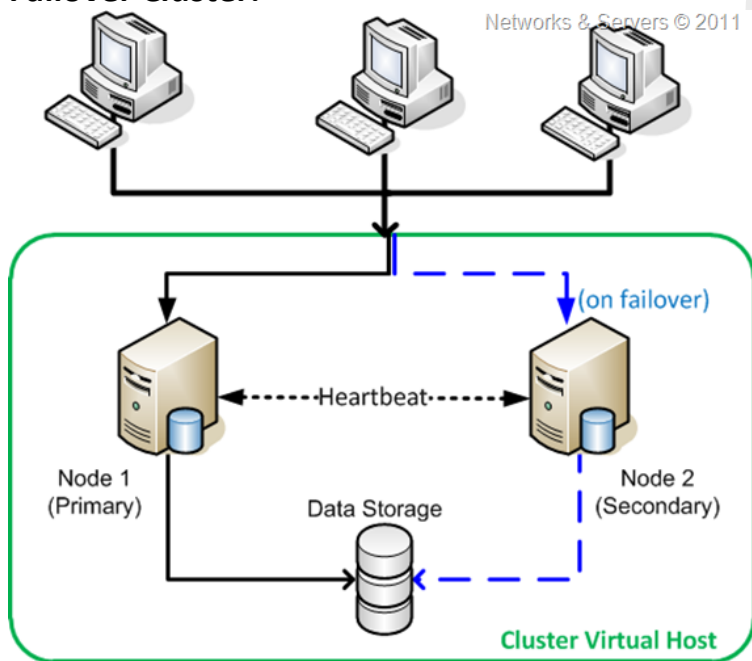
☐ Enable Message Authentication

Shared Secret:

IPv4 Properties

General	DNS	Network Access Protection
<div style="display: flex; justify-content: space-between;"> Filters Failover Advanced </div>		
<p>You can delete, edit and view status of all failover relationships that this server is part of.</p> <div style="display: flex; align-items: flex-start;"> <div style="flex: 1;"> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">dc1.contoso.com-192.168.0.254</div> <div style="border: 1px solid black; padding: 2px;">dhcp1-dc1 load balance</div> </div> <div style="flex: 0.2; text-align: center;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div> </div>		
<p>Failover status</p> <p>State of the server: <input type="text" value="Normal"/></p> <p>Partner Server: <input type="text" value="192.168.0.254"/></p> <p>Mode: <input type="text" value="Hot standby"/></p>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>		

Failover Cluster:





IPv6 - Configurations

- **SLAAC** can be used in a number of ways:
 - Stateless without DHCPv6,
 - Stateless with DHCPv6
 - Stateful with DHCPv6
- **Stateless** -
 - Router/DHCP server does not track ip address,
 - Simply provides network prefix,
 - Node not guaranteed to get same IPv6 address,
 - Node configures host identifier,
- **Stateful** -
 - DHCP server keeps track of addresses handed out (leases),
 - DHCP can assign same IPv6 address to returning node (DUID),

Jumping Bean



Powershell:

Get-DhcpServerv4Lease

The **Get-DhcpServerv4Lease** cmdlet gets one or more lease records from the Dynamic Host Configuration Protocol (DHCP) server service.

This example gets all the active IPv4 address leases from the DHCPv4 scope 10.10.10.0.

```
Get-DhcpServerv4Lease -ComputerName "dhcpserver.contoso.com" -ScopeId 10.10.10.0
```

Add-DhcpServerv4Lease

The **Add-DhcpServerv4Lease** cmdlet adds a new IPv4 address lease on the Dynamic Host Configuration Protocol (DHCP) server service. This cmdlet is only supported for DHCP server service that runs on Windows Server® 2012.

```
Add-DhcpServerv4Lease -IPAddress 10.10.10.11 -ScopeId 10.10.10.0 -ClientId F0-DE-F1-7A-00-5E -  
LeaseExpiryTime "2012-01-28 01:38:13Z" -HostName "MyComputer.contoso.com"
```

Set-DhcpServerv4DnsSetting

The **Set-DhcpServerv4DnsSetting** cmdlet configures how the Dynamic Host Configuration Protocol (DHCP) server service updates the DNS server by using the client-related information. This cmdlet modifies the effective DNS update setting and sets the setting on the server or the specified scope, policy or reservation.

Example : Set update configuration settings for a server policy

This example sets DNS update configuration settings for the sever policy ForeignDevices to enable DNS registration of clients under the DNS suffix guestdomain.com. The command specifies the computer, named dhcpserver.contoso.com, that runs the DHCP server service.

```
Set-DhcpServerv4DnsSetting -ComputerName "dhcpserver.contoso.com" -DnsSuffix  
"guestdomain.com" -PolicyName "ForeignDevices"
```

Add-DhcpServerv4Policy

The **Add-DhcpServerv4Policy** cmdlet adds a new policy either at the server level or at the scope level. The policy name must be unique at the level, either server or specific scope, where the policy is added and should have at least one condition as specified by the *CircuitId*, *ClientId*, *Fqdn*, *MACAddress*, *RelayAgent*, *Remoteld*, *SubscriberId*, *UserClass*, or *VendorClass* parameter.

Example: Create a server level policy for clients that are not members of a domain

This example creates a server level policy for all foreign clients that are not members of the local domain contoso.com. The policy matches clients that have an FQDN that does not contain the value contoso.com.

```
Add-DhcpServerv4Policy -Name "ForeignDevices" -Condition OR -Fqdn NE, *.contoso.com
```

```
Add-DhcpServerv4Failover -Name dc1-dhcp1 -ScopeId 192.168.10.0 -PartnerServer dhcp1.contoso.com
```

```
Get-DhcpServerv4Failover
```


2.2 Design a name resolution solution strategy:

Zone Types

- **Primary zone**

This DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named *zone_name.dns* and it is located in the %windir%\System32\Dns folder on the server.

- **Secondary zone**

This DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.

- Read-only copy

- **Stub zone**

This DNS server is a source only for information about the authoritative name servers for this zone. The zone at this server must be obtained from another DNS server that hosts the zone. This DNS server must have network access to the remote DNS server to copy the authoritative name server information about the zone.

Pointer to Auth name server: contains SOA, NS, A (Glue record)

- **GlobalNames Zone**

DNS Server role in Windows Server supports a specially named zone, called GlobalNames. By deploying a zone with this name, you can have the static, global records with single-label names, without relying on WINS. These single-label names typically refer to records for important, well-known and widely-used servers—servers that are already assigned static IP addresses and that are currently managed by IT-administrators using WINS.

In order to use this new zone, you have to do the following two steps:

1. Create the GlobalNames Zone (either via GUI or Command line), and
Create primary forward lookup zone named "**GlobalNames**"
2. Enable support for this Zone on the DNS Server

Dnscmd ServerName /config /Enableglobalnamesupport 1

If you want DNS clients in **other forests** to use the GlobalNames zone for resolving names, add **service location (SRV)** resource records to the forest-wide DNS application partition, using the service name **_globalnames._msdcs** and specifying the FQDN of the DNS server that hosts the GlobalNames zone.
Deploying a GlobalNames Zone

Resource Record

- Host (A) resource record for mapping a Domain Name System (DNS) domain name to an IP address that a computer uses.
- Alias (CNAME) resource record for mapping an alias DNS domain name to another primary or canonical name.
- Mail exchanger (MX) resource record for mapping a DNS domain name to the name of a computer that exchanges or forwards mail.
- Pointer (PTR) resource record for mapping a reverse DNS domain name that is based on the IP address of a computer that points to the forward DNS domain name of that computer.
- Service location (SRV) resource record for mapping a DNS domain name to a specified list of DNS host computers that offer a specific type of service, such as Active Directory domain controllers.

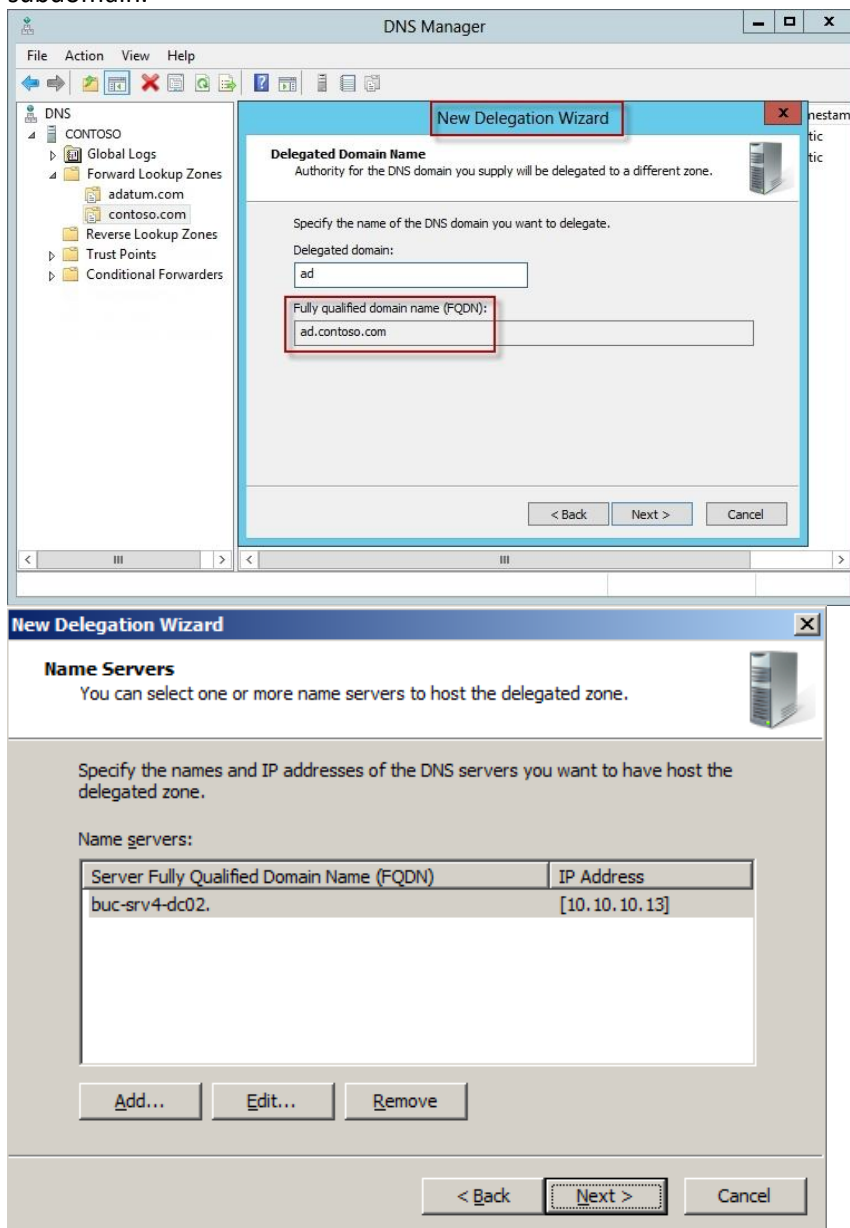
Name	Type	Data
syd-1	Host (A)	10.10.10.100
alias	Alias (CNAME)	Melb-1.Pasan.com.au
mail	Mail Exchanger (MX)	[10] syd-1.Pasan.com.au

Name	Type	Data
_kpasswd	Service Location (SRV)	[0][100][464] syd-1.pasan.com.au.
_ldap	Service Location (SRV)	[0][100][389] melb-1.pasan.com.au.

DNS Zone Delegation

You can divide your Domain Name System (DNS) namespace into one or more zones. You can delegate management of part of your namespace to another location or department in your organization by delegating the management of the corresponding zone.

You could use zone delegation to define the DNS-Server which has to be used when querying an information in a subdomain.



Cache Locking [Helps against cache poisoning]

Cache locking is a new security feature available with Windows Server® 2008 R2 that allows you to control whether or not information in the DNS cache can be overwritten.

Cache locking is configured as a percent value. For example, if the cache locking value is set to 50, then the DNS server will not overwrite a cached entry for half of the duration of the TTL. By default, the cache locking percent value is 100. This means that cached entries will not be overwritten for the entire duration of the TTL.

Set-DnsServerCache –LockingPercent 70

** This changes the cache lock value to 70 percent

DNSSEC

Domain Name System Security Extensions (DNSSEC) is a suite of extensions that add security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks.

Requirements:

Windows Server 2012, or a later operating system

DNS servers can be workgroup computers or domain member computers.

DNS Socket Pool

The DNS socket pool enables a DNS server to use source port randomization when it issues DNS queries. When the DNS service starts, the server chooses a source port from a pool of sockets that are available for issuing queries. Instead of using a predictable source port, the DNS server uses a random port number that it selects from the DNS socket pool.

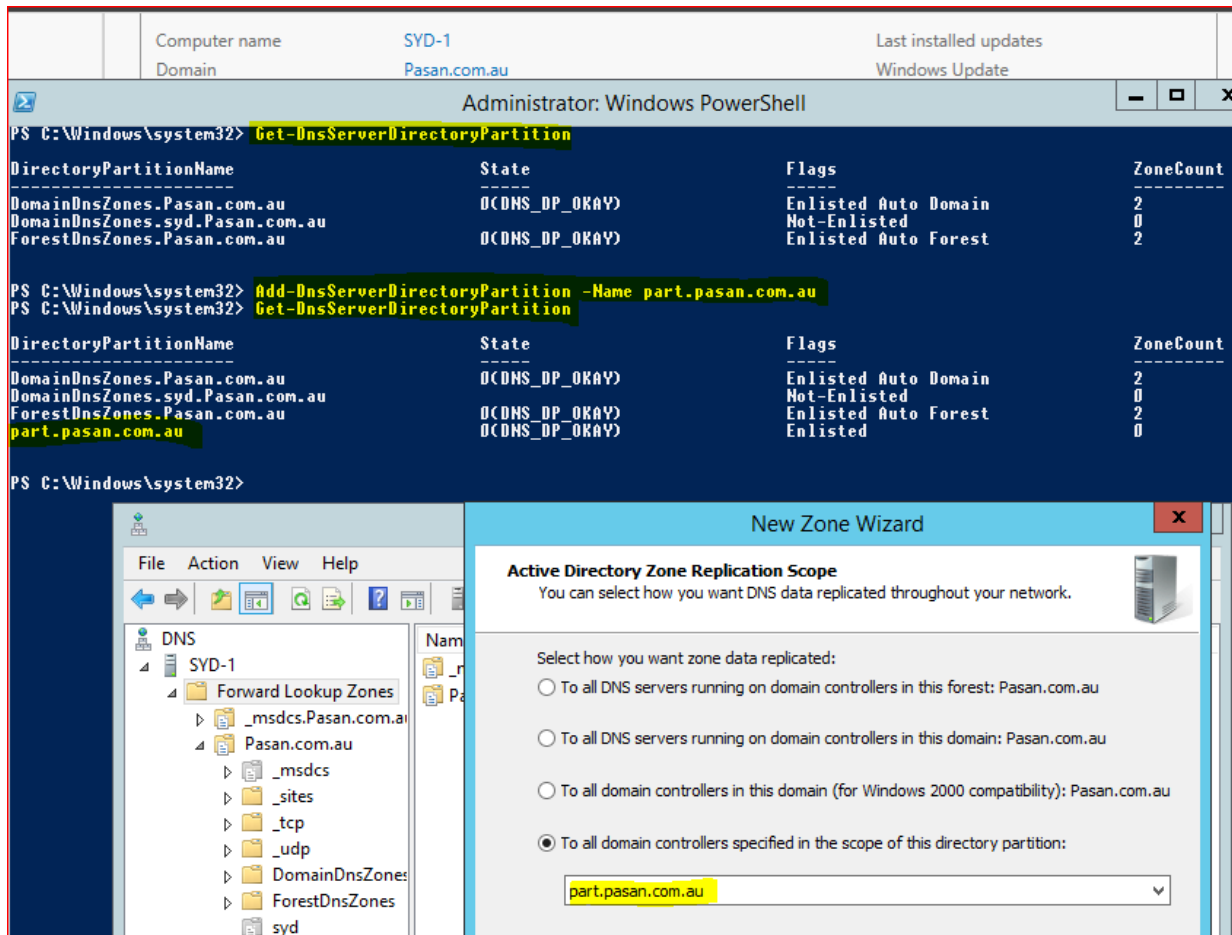
The DNS socket pool is enabled by default in Windows Server 2012 R2.

Global Query Block List

The block list feature that is provided by the DNS server role in Windows Server 2008 helps prevent the takeover of WPAD by ensuring that queries for WPAD servers always fail unless WPAD is excluded from the block list.

Create a DNS Application Directory Partition

You can store Domain Name System (DNS) zones in the domain or application directory partitions of Active Directory Domain Services (AD DS). A partition is a data structure in AD DS that distinguishes data for different replication purposes. When you create an application directory partition for DNS, you can control the scope of replication for the zone that is stored in that partition.



Powershell

The **Add-DnsServerDirectoryPartition** cmdlet creates a Domain Name System (DNS) application directory partition. After you install a DNS server, DNS creates an application directory partition for the service at the forest and domain levels. This cmdlet creates additional DNS application directory partitions.

This command adds a new DNS application directory partition named ADpart to the local computer.

Add-DnsServerDirectoryPartition -Name "ADpart"

dnscmd <ServerName> /CreateDirectoryPartition <FQDN>

The **Register-DnsServerDirectoryPartition** cmdlet registers a Domain Name System (DNS) server in a DNS application directory partition. After you create a Domain Name System (DNS) application directory partition to store a zone, you must register the DNS server that hosts the zone in the application directory partition. After you register a DNS server in a DNS application directory partition, the DNS server adds itself to the replication scope of the DNS application directory partitions.

Register-DnsServerDirectoryPartition -Name "ADpart"

dnscmd <ServerName> /EnlistDirectoryPartition <FQDN>

The **UnRegister-DnsServerDirectoryPartition** cmdlet deregisters a Domain Name System (DNS) server from a specified DNS application directory partition. After you deregister a DNS server from a DNS application directory partition, the DNS server removes itself from the replication scope of the partition.

2.3 Design and manage an IP address management solution:

IP address management (**IPAM**) is a means of planning, tracking, and managing the Internet Protocol address space used in a network. **IPAM** integrates DNS and DHCP so that each is aware of changes in the other (for instance DNS knowing of the IP address taken by a client via DHCP, and updating itself accordingly).

IPAM must be installed on a domain member computer. You cannot install IPAM on a domain controller. If IPAM is installed on the same server with DHCP, then DHCP server discovery will be disabled.

An IPAM server provides support for a single Active Directory forest. Multi-forest topologies are **not** supported. Multiple IPAM servers can support a single domain, or a single IPAM server can support all domains in an Active Directory forest.

You can use IPAM to manage DHCP servers running on Windows Server 2008 R2 and above.

IPAM server itself must run on Windows Server 2012 or Windows Server 2012 R2

IPAM deployment options

An IPAM server is a domain member computer.

Important

You cannot install the IPAM feature on an Active Directory domain controller.

There are three general methods to deploy IPAM servers:

1. Distributed: An IPAM server deployed at every site in an enterprise.
2. Centralized: One IPAM server in an enterprise.
3. Hybrid: A central IPAM server deployed with dedicated IPAM servers at each site.

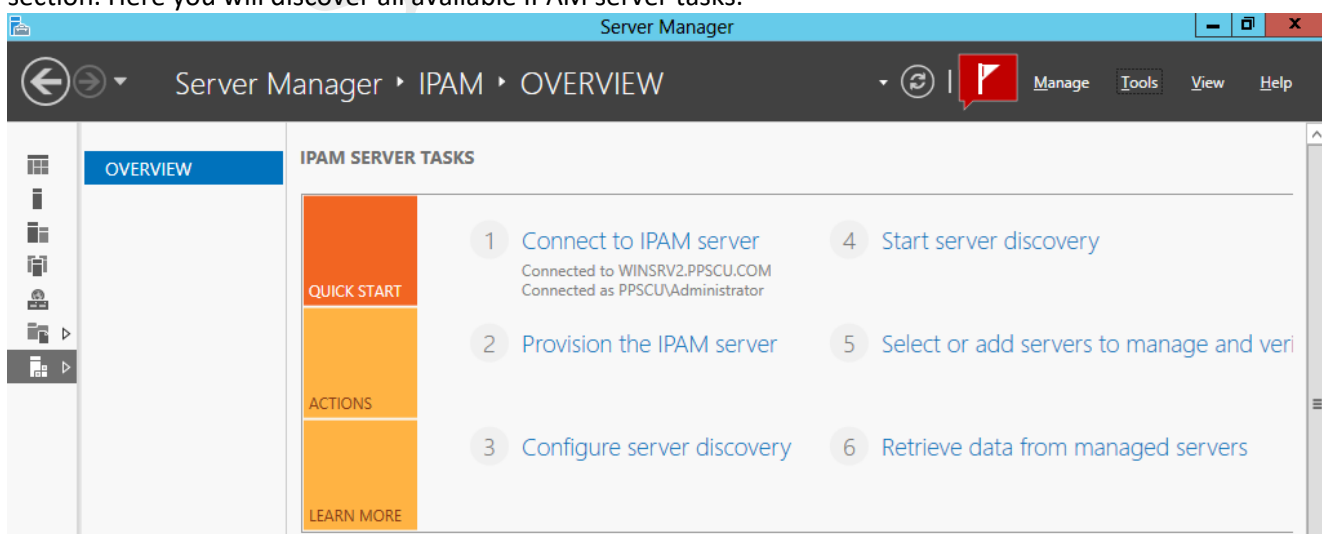
IPAM deployment steps

Step 1 – Installation

IPAM can be installed in two ways: using Windows Powershell or by accessing the Roles and Features section from Server Manager Console:

Step 2 – Provisioning

Once the installation has been successfully completed, open the Server Manager Console and navigate to the IPAM section. Here you will discover all available IPAM server tasks:

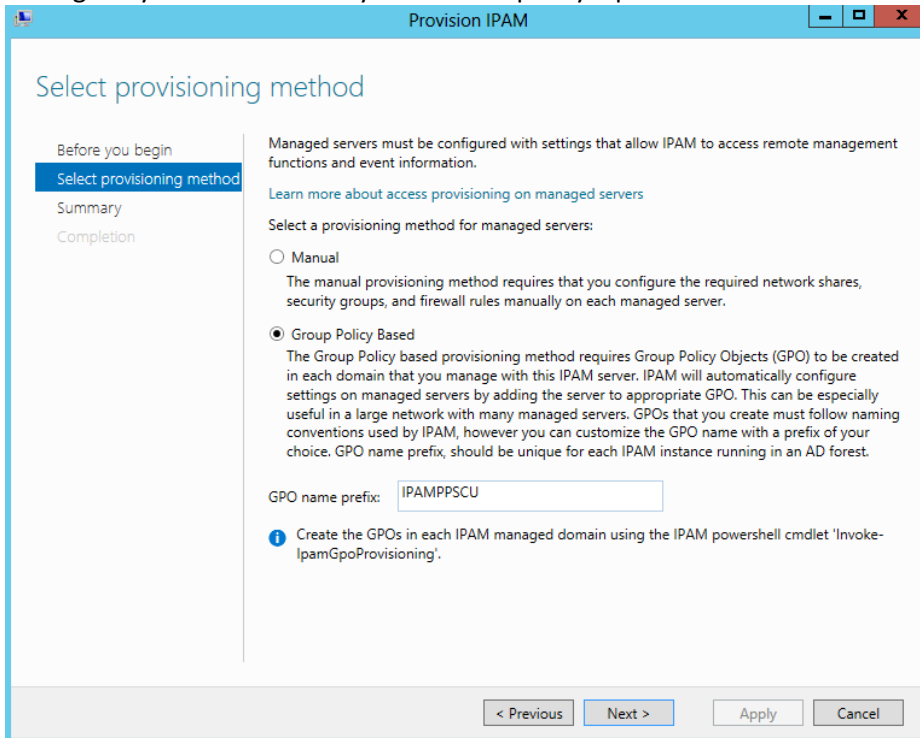


Select the second option, Provision the IPAM, to start the IPAM configuration wizard. In this section is where the IPAM database, security groups, tasks and folders are created.

Step 3 – Provisioning Method

You must configure how the IPAM server interacts with network servers, there are two options available: manually or by using GPOs. Simply put, by selecting the first option, an administrator would have to configure security groups, firewall rules and network shares manually on each machine. This method is really not recommended since it adds a lot of extra configurations and increases the overall complexity of the IPAM deployment.

The second option is much easier to implement since it uses Group Policy Objects to configure all IPAM managed servers. Unless you simply cannot you use the second option, you should always use GPOs to configure servers managed by IPAM. Note that you have to specify a prefix that will be set to the IPAM GPOs:



The screenshot shows the 'Provision IPAM' wizard window. The title bar says 'Provision IPAM'. The main heading is 'Select provisioning method'. On the left, there is a navigation pane with 'Before you begin', 'Select provisioning method' (selected), 'Summary', and 'Completion'. The main content area has the following text: 'Managed servers must be configured with settings that allow IPAM to access remote management functions and event information.' Below this is a link: 'Learn more about access provisioning on managed servers'. Then it says 'Select a provisioning method for managed servers:'. There are two radio buttons: 'Manual' and 'Group Policy Based' (which is selected). Under 'Manual', it says 'The manual provisioning method requires that you configure the required network shares, security groups, and firewall rules manually on each managed server.' Under 'Group Policy Based', it says 'The Group Policy based provisioning method requires Group Policy Objects (GPO) to be created in each domain that you manage with this IPAM server. IPAM will automatically configure settings on managed servers by adding the server to appropriate GPO. This can be especially useful in a large network with many managed servers. GPOs that you create must follow naming conventions used by IPAM, however you can customize the GPO name with a prefix of your choice. GPO name prefix, should be unique for each IPAM instance running in an AD forest.' Below this is a text box labeled 'GPO name prefix:' with the value 'IPAMPPSCU'. At the bottom, there is a note with an information icon: 'Create the GPOs in each IPAM managed domain using the IPAM powershell cmdlet 'Invoke-IpamGpoProvisioning'.'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Apply', and 'Cancel'.

Once the wizard has been successfully completed, three Group Policy Objects will be created: one for DNS servers, one for DHCP servers and one for Domain Controllers.

Step 4 – Configure Server Discovery

Select the third task from the IPAM console to configure server discovery. This is where we specify what servers should be discovered by our IPAM machine. You will need to select and add domains to discover. By default, all three types of servers are selected: DNS, DHCP and Domain Controllers. You can change the discovery options by selecting only desired types of servers:

Configure Server Discovery

Select domains to discover:

Add

Select the server roles to discover:

Domain	Domain controller	DHCP server	DNS server
(root domain) ppscu.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Remove

i For Group Policy based provisioning, create the GPOs for each domain in the list using the Windows PowerShell cmdlet "Invoke-IpamGpoProvisioning" on IPAM server.
[Learn more about group policy based provisioning.](#)

Details of server discovery schedule

Next scheduled run time: 9/28/2015 5:55:21 PM

! Discovery schedule can be changed by editing \Microsoft\Windows\IPAM\ServerDiscovery located in the Task Scheduler on the IPAM server with administrator privileges.

OK Cancel

Step 5 – Start Discovery

Once this section has been covered, select the 4th task to start the server discovery procedure:

Overview Task Details

Overview Task Details and Notifications

All Tasks | 1 total

Filter

Status	Task Name	Stage	Message	Action	Notifications
	IPAM ServerDiscovery task	Comple...	Discovered servers are based on: 9/27/2015 6:0...		0

< >

Status	Notification	Time Stamp
--------	--------------	------------

Step 6 – Verify GPOs

You can now verify the GPOs in the Group Policy Management Console. Connect to the blocked machine and execute gpupdate /force to propagate the newly created GPOs.

For each machine you will have to change its manageability status to managed, you can do so if you right click on the blocked machine and select edit server:

Add or Edit Server

Provide server details and other custom field mapping details:

Field	Value
* Server name (FQDN)	WinSrv1.ppscu.com Verify
* IP address	10.10.1.10
* Server type	<input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> DNS server <input type="checkbox"/> DHCP server <input type="checkbox"/> NPS server
Manageability status	Managed
Owner	
Description	

Custom Configurations

OK Cancel

The machine should change its IPAM Access status to Unblocked.

Step 7 – Import Data

Now that the server has been added to IPAM, you can retrieve and import its data to the IPAM server if you right click on the machine and select Retrieve All Server Data. You can also execute the 6th available task from the IPAM console to retrieve data from managed servers:

Server Manager

◀ IPAM ▶ SERVER INVENTORY ▶ IPv4 ▶

Manage Tools View Help

IPv4
IPv4 | 1 total

Discovered servers are based on: 9/27/2015 9:33:10 PM. Next data collection is on: 9/28/2015 5:55:21 PM. Please re... [More...](#)

Recommended Action	Manageability Status	IPAM Access Status	Server Name	DNS Suffix	Domain Name	Server Status	Server Type
✓ IPAM Access Unblocked	Managed	Unblocked	WinSrv1	ppscu.com	ppscu.com	No change	DC, DNS server

Filter

Tasks: Edit Server..., Retrieve All Server Data, Refresh Server Access Status, Delete

Details View
WinSrv1

Details

Description:

[Learn more about IPAM Access Status](#)

Server Name:	WinSrv1	Data Retrieval Status:	Completed
Domain Name:	ppscu.com	Manageability Status:	Managed
IPv4 Addresses:	10.10.1.10	IPAM Access Status:	Unblocked
IPv6 Addresses:		Recommended Action:	IPAM Access Unblocked
Operating System:	Windows Server 2012 Datacenter	Owner:	
Server Status:	No change	DHCP RPC Access Status:	Not applicable
DNS Suffix:	ppscu.com	DHCP Audit Share Access Status:	Not applicable

Configure IPAM VMM Integration

To enable IPAM and Virtual Machine Manager (VMM) integration, you must first configure a user account for VMM on the IPAM server and then configure the IPAM network service plugin in VMM.

- **Configure IPAM**

VMM must be granted permission to view and modify IP address space in IPAM, and to perform remote management of the IPAM server. VMM uses a “Run As” account to provide these permissions to the IPAM network service plugin. The “Run As” account must be configured with appropriate permission on the IPAM server.

Permissions on IPAM: IPAM ASM administrator, Remote management users

- **Configure VMM**

- In the **Fabric** workspace, expand the **Networking** node and then click **Network Service**.
- Right-click **Network Service**, and click **Add Network Service**.
- In the **Add Network Service Wizard**, on the **Name** page, next to **Name**, type **IPAM** and then click **Next**. The **Description** field is optional.
- On the **Manufacturer and Model** page, next to **Manufacturer**, choose **Microsoft** and next to **Model**, choose **Microsoft Windows Server IP Address Management**, and then click **Next**.
- On the **Credentials** page, next to **Run As account**, click **Browse** and then click **Create Run As Account**.
- On the **Create Run As Account** page, next to **Name** type a name for the account, for example **VMM User**.
- Next to **User name**, **Password** and **Confirm password**, enter the username and password for the account that was created on the IPAM server in the previous procedure, for example **contoso\vmuser**. A description is optional. See the following example. Click **OK** to continue.
- Click **OK** to close the **Select a Run As Account** dialog box.
- Click **Next**, and then on the **Connection String** page, type the fully qualified domain name (FQDN) of the IPAM server, for example **ipam1.contoso.com**. Click **Next** to continue.
- On the **Provider** page, verify that **Microsoft IP Address Management Provider** is selected next to **Configuration provider**, and then click **Test**.
- Verify that **Passed** is displayed next to **Test open connection**, **Test capability discovery**, and **Test system info**. See the following example.

IPAM security groups

The following local IPAM security groups are created when you install IPAM.

- **IPAM Users:** Members of this group can view all information in server discovery, IP address space, and server management. They can view IPAM and DHCP server operational events, but cannot view IP address tracking information.
- **IPAM MSM Administrators:** IPAM multi-server management (MSM) administrators have IPAM Users privileges and can perform IPAM common management tasks and server management tasks.
- **IPAM ASM Administrators:** IPAM address space management (ASM) administrators have IPAM Users privileges and can perform IPAM common management tasks and IP address space tasks.
- **IPAM IP Audit Administrators:** Members of this group have IPAM Users privileges and can perform IPAM common management tasks and can view IP address tracking information.
- **IPAM Administrators:** IPAM Administrators have the privileges to view all IPAM data and perform all IPAM tasks.

Powershell:

Invoke-IpamGpoProvisioning

The **Invoke-IpamGpoProvisioning** cmdlet creates and links three group policies specified in the **Domain** parameter for provisioning required access settings on the server roles managed by the computer running the IP Address Management (IPAM) server.

Example : Provision a GPO by using an FQDN

Invoke-IpamGpoProvisioning -Domain "child.contoso.com" -GpoPrefixName "IPAM2" -IpamServerFqdn "Ipam2.Contoso.com" -Force

3.1 Design a VPN solution:

The **Remote Access server role** is a logical grouping of the following related network access technologies.

- **DirectAccess**
DirectAccess enables remote users to securely access shared resources, Web sites, and applications on an internal network without connecting to a virtual private network (VPN). DirectAccess establishes bi-directional connectivity with an internal network every time a DirectAccess-enabled computer is connected to the Internet. Users never have to think about connecting to the internal network, and IT administrators can manage remote computers outside the office, even when the computers are not connected to the VPN.
- **Routing and Remote Access**
The Routing and Remote Access service (RRAS) supports remote user or site-to-site connectivity by using virtual private network (VPN) or dial-up connections. RRAS provides the following features.
RRAS Multitenant Gateway
Remote Access: By using RRAS, you can deploy VPN connections to provide end users with remote access to your organization's network. You can also create a site-to-site VPN connection
Routing: RRAS is a software router and an open platform for routing and networking.
- **Web Application Proxy**
Web Application Proxy provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access them from outside the corporate network.

VPN Tunneling Protocols

Tunneling enables the encapsulation of a packet from one type of protocol within the datagram of a different protocol. For example, VPN uses Point-to-Point Tunneling Protocol (PPTP) to encapsulate IP packets over a public network, such as the Internet. You can configure a VPN solution based on PPTP, Layer Two Tunneling Protocol (L2TP), Secure Socket Tunneling Protocol (SSTP), or Internet Protocol security (IPsec) using Internet Key Exchange version 2 (IKEv2).

Tunnel	Encryption	Compatibility	Features
PPTP	MS-CHAP v2,EAP-TLS	XP, 2003 <	
L2TP/IPsec	IPsec	XP, 2003 <	
SSTP	HTTPS.SSL	Vista SP1, 2008 <	
IKEv2	Ipsec/ESP	7, 2008R2 <	VPN Reconnect

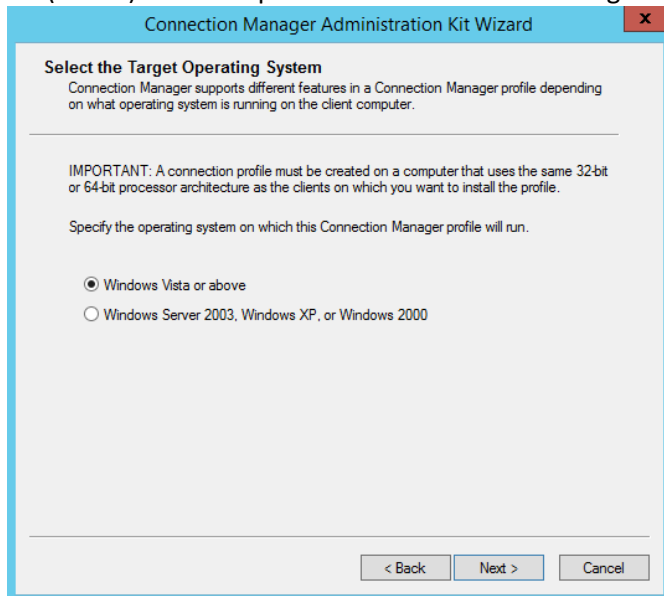
Azure cross-premises connection options

- **Site-to-Site connection**
 - VPN connection over IPsec (IKE v1 and IKE v2). This type of connection requires a VPN device or RRAS.
- **Point-to-Site**
 - VPN connection over SSTP (Secure Socket Tunneling Protocol). This connection does not require a VPN device.

Connection Manager Administration Kit

Connection Manager in Windows is connection management software that simplifies and enhances the management of remote connections. Connection Manager uses *profiles* made of connection settings that allow

connections from the local computer to a remote network. You can use the Connection Manager Administration Kit (CMAC) to create profiles for Connection Manager and distribute them to your users.



3.2 Design a DirectAccess solution:

DirectAccess Split Tunneling and Force Tunneling

When you configure a Windows DA server or UAG DA server-based DirectAccess (DA) solution, the default setting is to enable split tunneling. What split tunneling refers to is the fact that only connections to the corpnet are sent over the DA IPsec tunnels. If the user wants to connect to resources on the Internet, the connection is made over the local link (that is to say, the connection is sent directly to the Internet based on the IP addressing configuration on the DA client computer's NIC).

However, you might not want to enable split tunneling. If that is the case, then all traffic from the DA client to any resource must go over the DA IPsec tunnels. Traffic destined for the intranet goes over the DA IPsec tunnels, and traffic destined to the Internet also goes over the DA IPsec tunnels. Split tunneling is disabled when you enable Force Tunneling for the DA client connections. Force Tunneling is enabled via Group Policy:

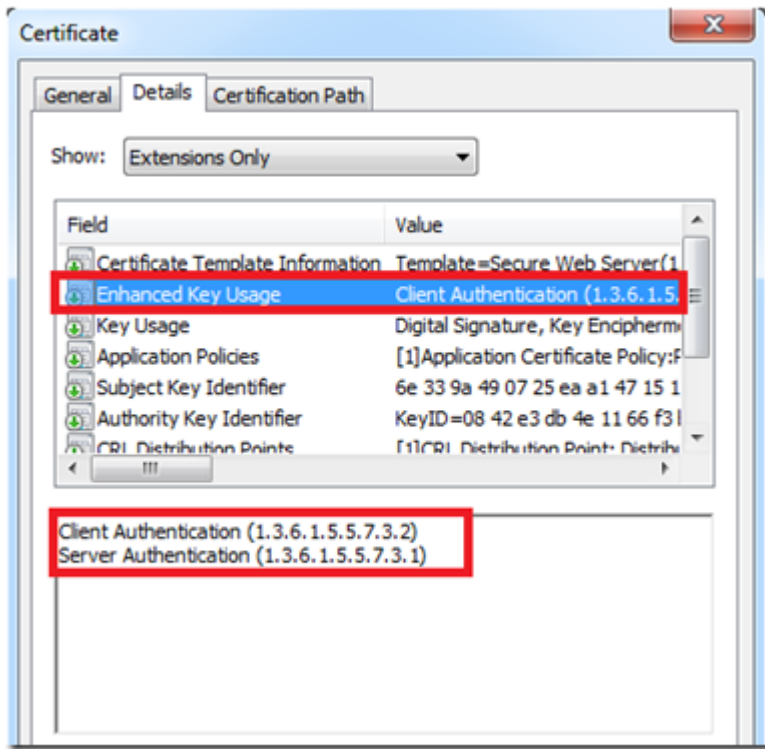
3.3 Design a Web Application Proxy solution:

Web Application Proxy in Windows Server 2012R2 supports two types of preauthentication:

- AD FS preauthentication. AD FS preauthentication uses AD FS for web applications that use claims-based authentication.
- Pass-through preauthentication. Pass-through preauthentication does not use AD FS for authentication, and Web Application Proxy does not preauthenticate the user. Instead, the user connects to the web application through Web Application Proxy.

Certificate enhanced Key Usage

A certificate enables the subject to perform a specific task. To help control the usage of a certificate outside its intended purpose, restrictions are automatically placed on certificates. These restrictions can be applied by using the key usage extension.



Workplace Join:

Configure Device Registration Service Discovery

Workplace Join client devices will attempt to discover the Device Registration Server by combining the user account name with a well-known Device Registration server name.

You must create a DNS CNAME record that points to the A record associated with your AD FS farm. The CNAME record must use the well-known prefix **EnterpriseRegistration** followed by the UPN suffix used by the user accounts at your organization. If your organization uses multiple UPN suffixes, multiple CNAME records must be created in DNS.

Configure Device Registration Discovery Server SSL certificate

for the Workplace Join client to discover the Device Registration server using a well-known DNS CNAME record, AD FS must be configured with a server SSL certificate that includes the well-known Device Registration server names. You must include one server name for every userPrincipalName (UPN) suffix in use at your company in the format of:

enterpriseregistration.<upnsuffix>

For example, if your company's UPN suffix is @contoso.com, then your AD FS server SSL certificate must contain enterpriseregistration.contoso.com

Example: Using a wildcard certificate

Subject = *.contoso.com

Example: Using subject alternative names

Subject = adfs.contoso.com (This is your AD FS farm name)

Subject Alternative Name (DNS) = adfs.contoso.com

Subject Alternative Name (DNS) = enterpriseregistration.contoso.com

Subject Alternative Name (DNS) = enterpriseregistration.region.contoso.com

3.4 Implement a scalable remote access solution:

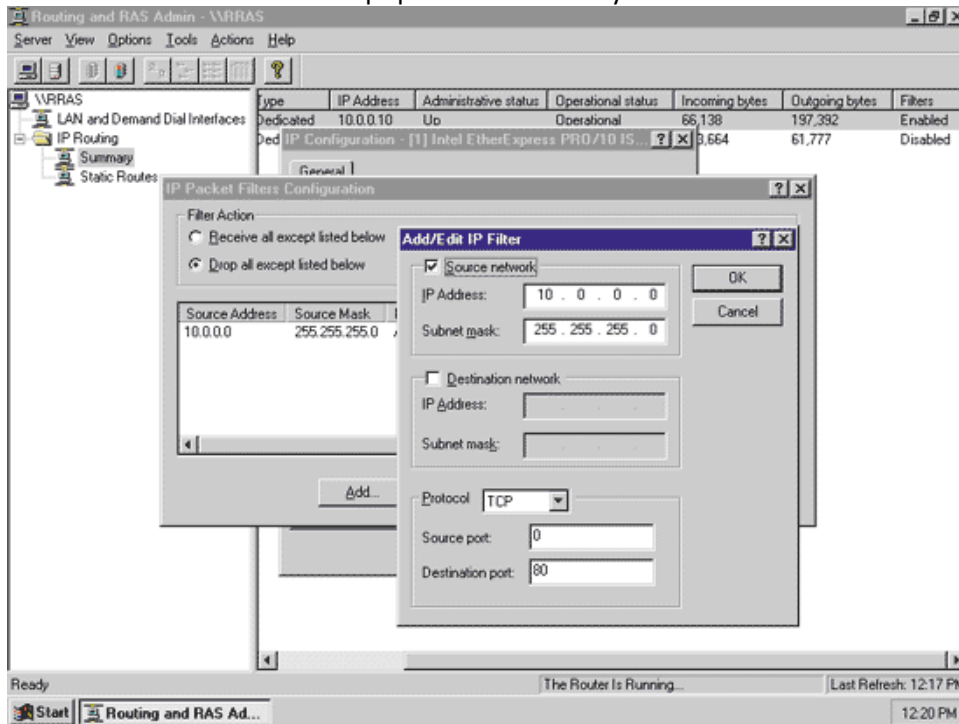
RRAS Routing and Remote Access Service:

Static Packet Filters

RRAS supports IP packet filtering, which specifies which type of traffic is allowed into and out of the RRAS server. The packet filtering feature is based on exceptions.

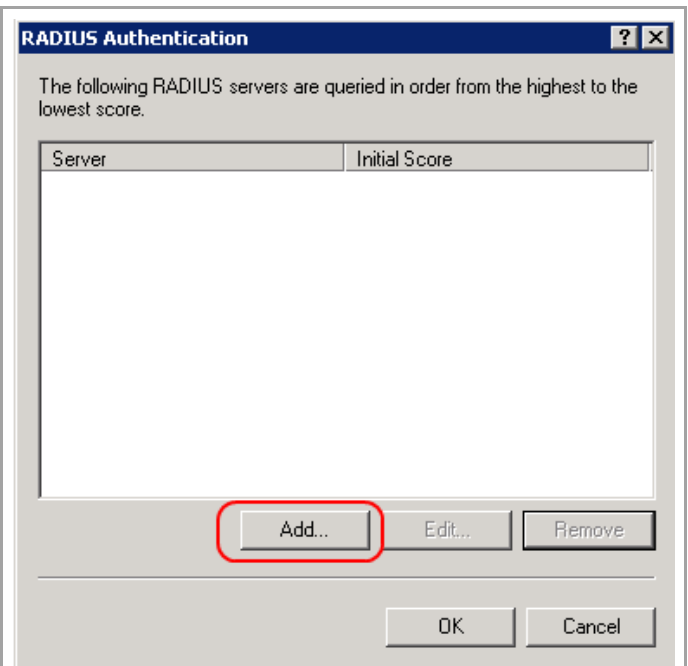
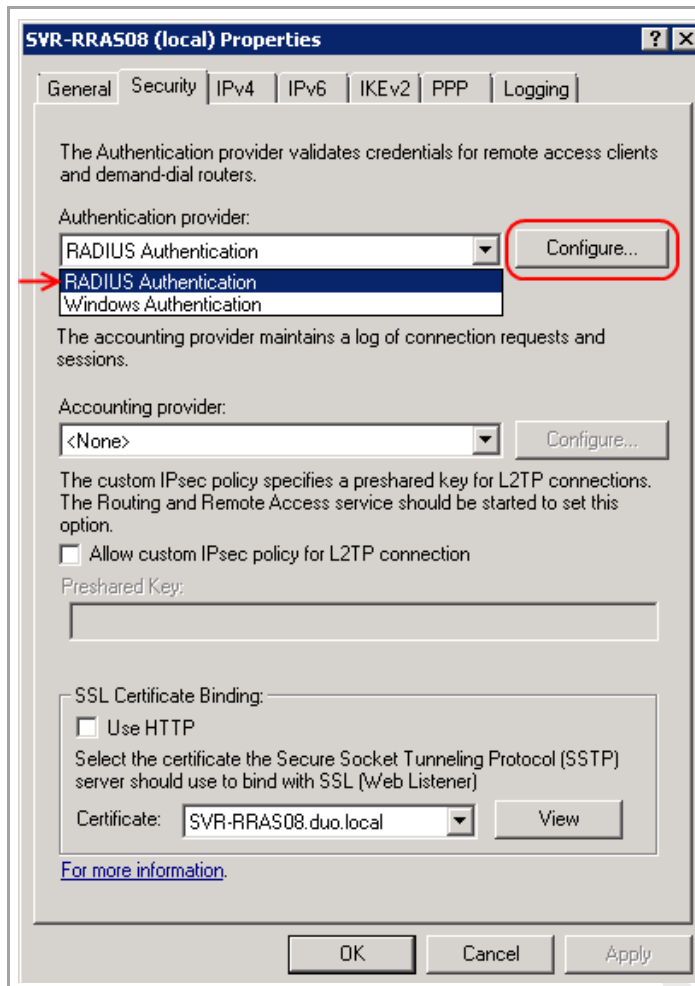
You can set packet filters per interface and configure them to do one of the following:

- Pass through all traffic except packets prohibited by filters.
- Discard all traffic except packets allowed by filters.

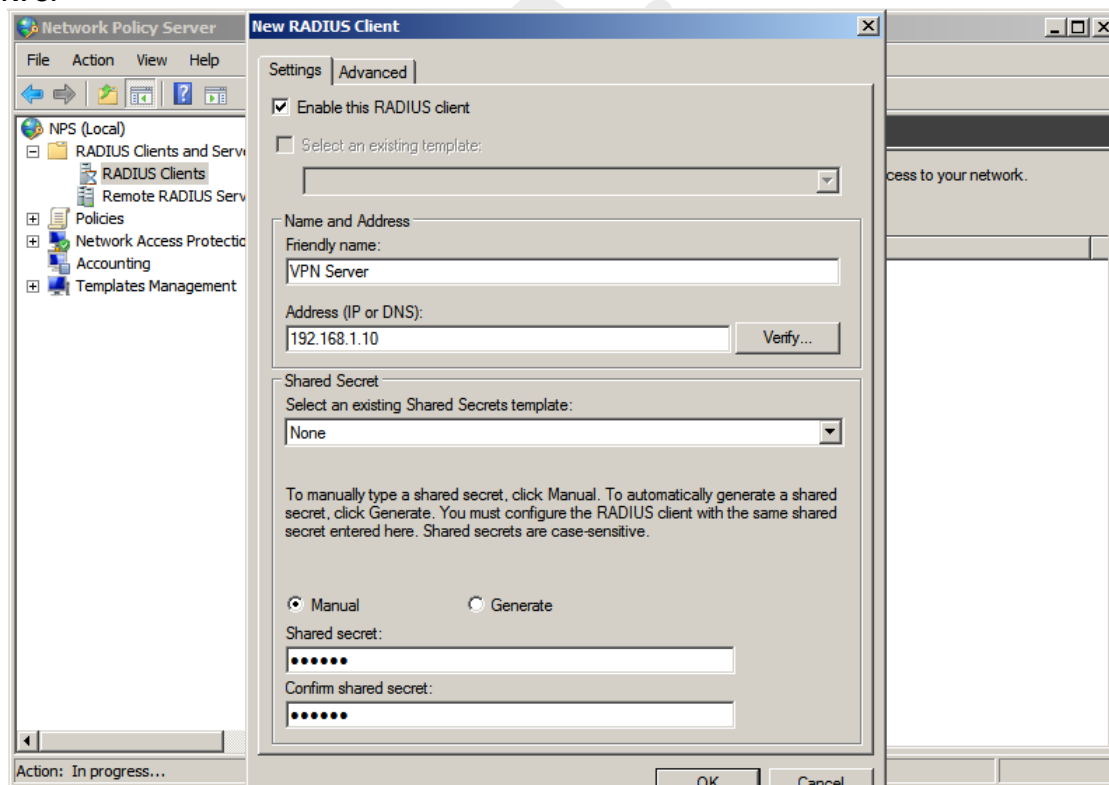


RRAS VPN Authentication:

Authentication Provider -> NPS RADIUS Client



NPS:



3.5 Design a network protection solution

Network Policy 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.

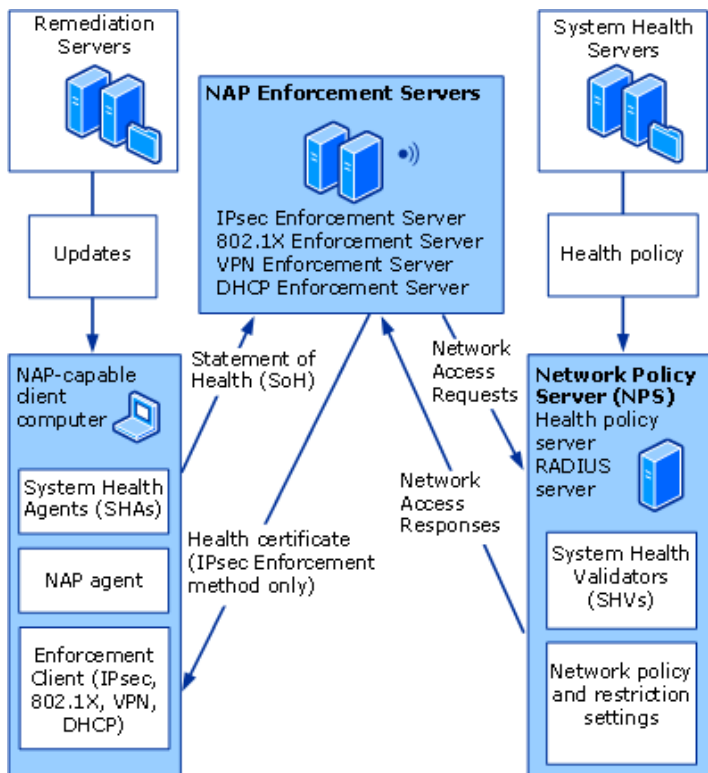
NPS allows you to centrally configure and manage network access authentication, authorization, and client health policies with the following three features:

- **RADIUS server** . NPS performs centralized authentication, authorization, and accounting for wireless, authenticating switch, remote access dial-up and virtual private network (VPN) connections.
- **RADIUS proxy** . When you use NPS as a RADIUS proxy, you configure connection request policies that tell the NPS server which connection requests to forward to other RADIUS servers and to which RADIUS servers you want to forward connection requests.
- **Network Access Protection (NAP) policy server** . When you configure NPS as a NAP policy server, NPS evaluates statements of health (SoH) sent by NAP-capable client computers that want to connect to the network.

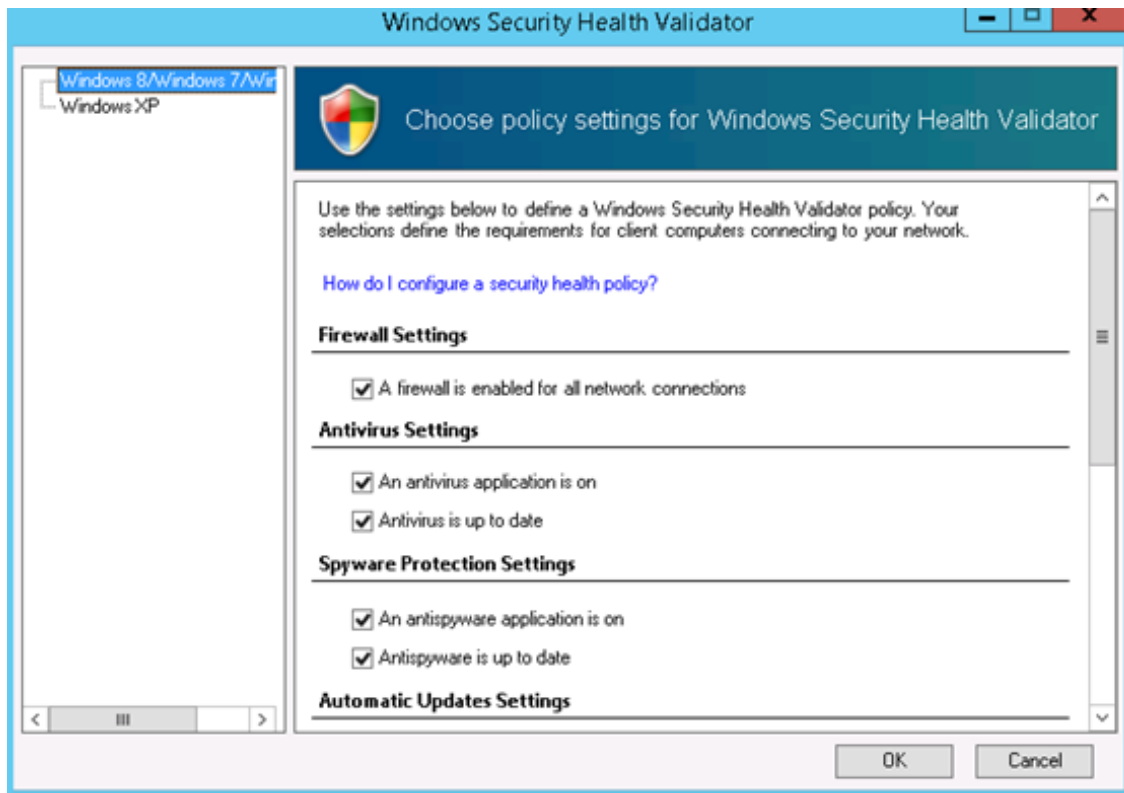
NAP enforcement methods:

Network Policy Server (NPS) enforces Network Access Protection (NAP) health policies for the following network technologies:

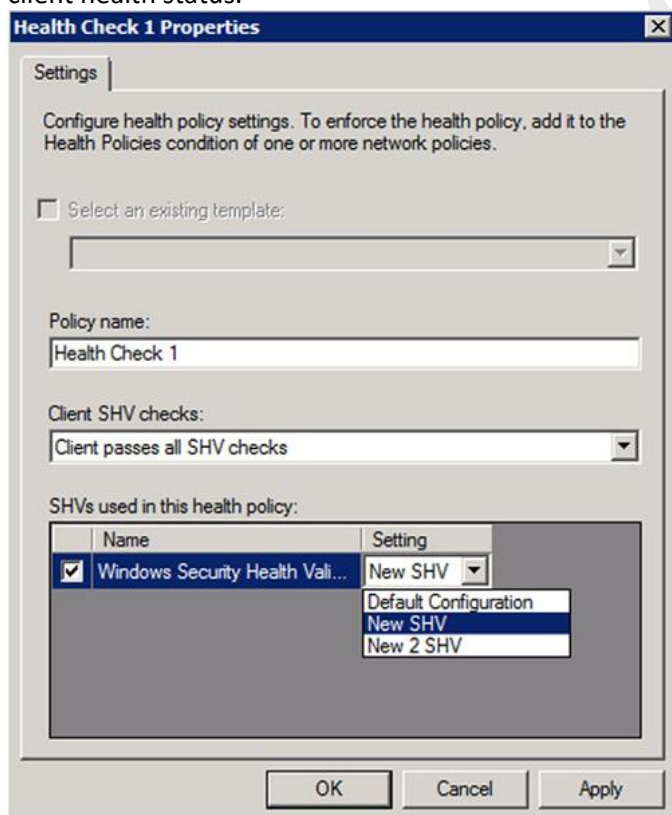
- Internet Protocol security (IPsec) policies for Windows Firewall on client computers. For NAP IPsec enforcement, the IPsec enforcement client must be installed on client computers.
- 802.1X port-based wired and wireless network access control. VLANs, ACLS
- Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address lease and renewal.
- Terminal Server Gateway (TS Gateway) connections with Terminal Services.
- Virtual private networks (VPN) with Routing and Remote Access.



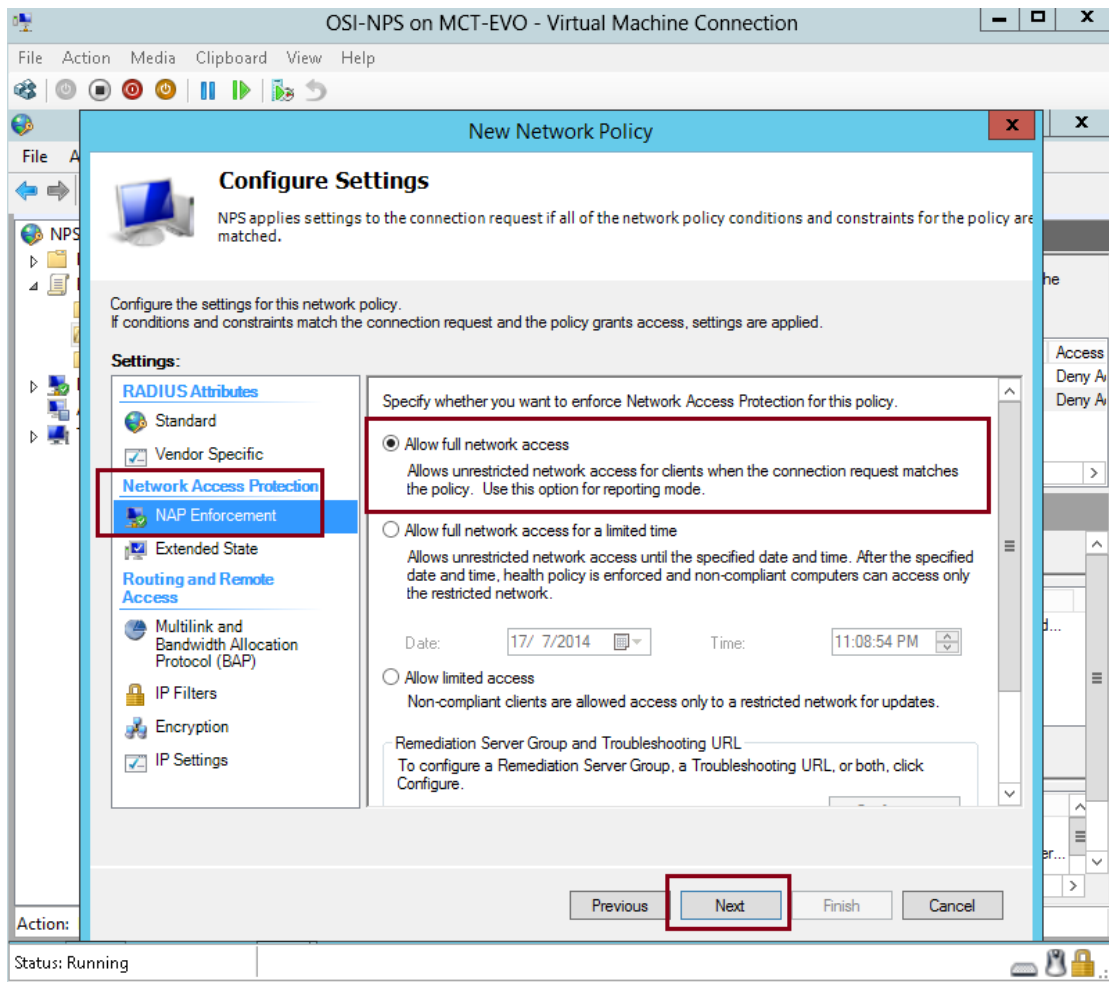
System health validators (SHVs) define configuration requirements for computers that attempt to connect to your network.



Health policies define which SHVs are evaluated and how they are used in validating the configuration of computers that attempt to connect to your network. Based on the results of SHV checks, health policies classify client health status.



Network policies use conditions, settings, and constraints in order to determine who can connect to the network. There must be a network policy that is applied to computers that are compliant with the health requirements and a network policy that is applied to computers that are noncompliant.



4.1 Design a forest and domain infrastructure

AD functional levels:

Level	Domain	Forest
2000		
2003		RODC
2008	Fine-grained password policies	
2008 R2	Authentication mechanism assurance: Claims	Active Directory Recycle Bin
2012		
2012 R2		

You cannot set the domain functional level to a value that is lower than the forest functional level, but you can set it to a value that is equal to or higher than the forest functional level.

Domain Trust:

Selective Authentication

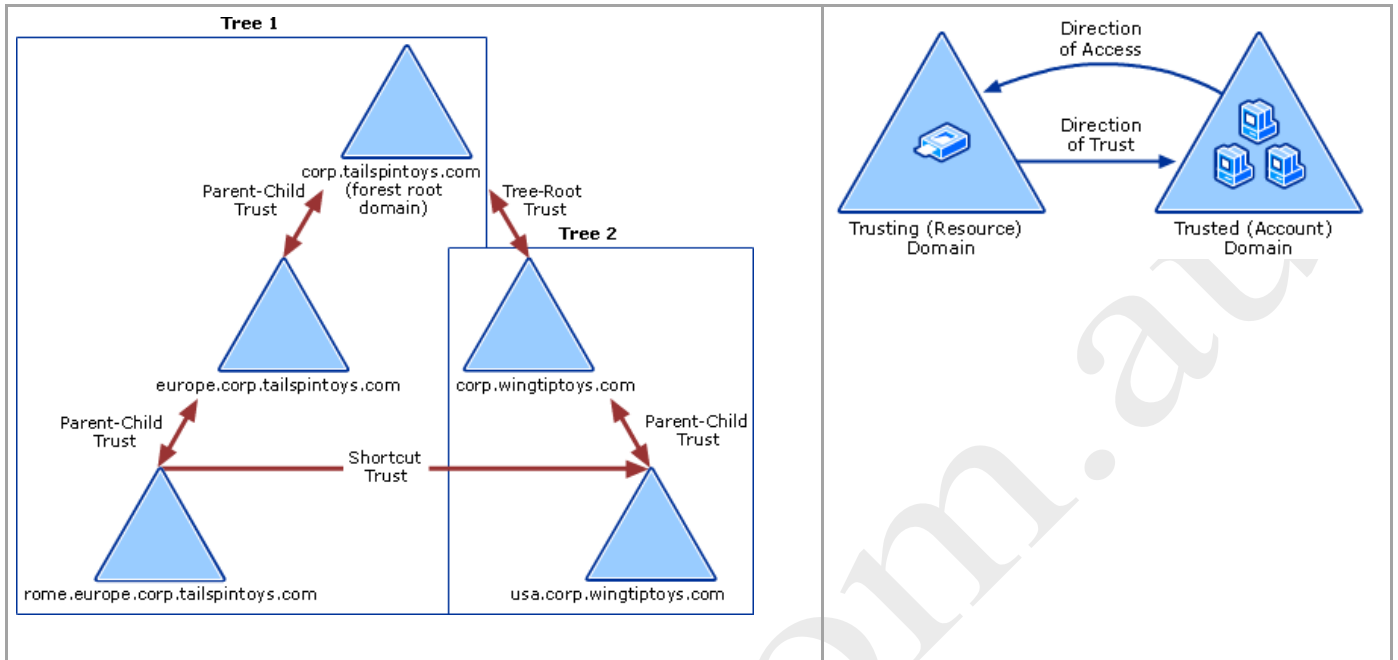
When you enable the selective authentication feature of a forest trust relationship, users accessing cross-forest resources from one forest cannot authenticate to a domain controller or resource server (e.g., file server, print server) in the other forest unless they are explicitly allowed to do so.

Not in authenticated users group for the domain

Shortcut trust. A transitive trust between domains in the same domain tree or forest that is used to shorten the trust path in a large and complex domain tree or forest.

Forest trust. A transitive trust between one forest root domain and another forest root domain.

Realm trust. A transitive trust between an Active Directory domain and a Kerberos V5 realm.



Parent-child trust

A parent-child trust relationship is established whenever a new domain is created in a tree. The Active Directory installation process automatically creates a trust relationship between the new domain and the domain that immediately precedes it in the namespace hierarchy (for example, corp.tailspintoys.com is created as the child of tailspintoys.com). The parent-child trust relationship has the following characteristics:

- It can exist only between two domains in the same tree and namespace.
- The parent domain is always trusted by the child domain.
- It must be transitive and two-way. The bidirectional nature of transitive trust relationships allows the global directory information in Active Directory to replicate throughout the hierarchy.

NetDOM

- Establishes, verifies, or resets a trust relationship between domains.
- Netdom **cannot** be used to create a forest trust between two AD DS forests.
- `netdom trust /d:marketing.contoso.com engineering.contoso.com /add /twoway /Uo:admin@engineering.contoso.com /Ud:admin@marketing.contoso.com`

Downgrading A Windows Server Domain and Forest Functional Level

Once upon a time, it was not possible to downgrade Windows Server forest and domain functional levels once upgraded. Enter Windows Server 2012 R2 and its Active Directory enhancements, as detailed by the video below, backed by PowerShell automation capabilities. This enablement makes the forest and domain functional level downgrade even easier. Do keep in mind however that the lowest functional level that can be utilized is Windows Server 2008 R2.

4.2 Implement a forest and domain infrastructure

Rename domain

- create a report which explains the current forest setup. To do that type **rendom /list** and press enter.
- This will create an xml file with name **Domainlist.xml** in the path above command is executed. In my demo its **C:\Users\Administrator.CONTOSO**

- To proceed it need to be edited to match with the new domain name. Make sure you save the file after edits.
- Then type **rendom /upload** command from same folder path.
- To check the domain readiness before the rename process type **rendom /prepare**
- Once its pass with no errors, execute **rendom /execute** to proceed with rename. It will reboot all domain controllers automatically.
- The next thing we need to fix is the group policies. It's still uses the old domain name.
To fix this type and enter **gpfixup /olddns:contoso.com /newdns:canitpro.local**
Then run **gpfixup /oldnb:CONTOSO /newnb:canitpro**
- The only thing we need to run is **random /end** to stop the rename process and unfreeze the DC activity.

In Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 and future versions of Windows Server, Rendom is built into domain controllers promoted to "Active Directory Domain Services" role, or as part of Remote Server Administration Tools (RSAT). Rendom can be found at %windir%\System32\rendom.exe.

4.3 Design a Group Policy strategy

Advanced Group Policy Management

Microsoft Advanced Group Policy Management (AGPM) extends the capabilities of the Group Policy Management Console (GPMC) to provide comprehensive change control and improved management for Group Policy Objects (GPOs). AGPM is available as part of the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance.

WMI Filtering:

ProductType="1" -> Client operating systems

ProductType="2" -> Domain controllers

ProductType="3" -> Servers that are not domain controllers

Version like "10.%" -> 2016,10

Version like "6.2%" -> 2012,8

Version like "6.1%" -> 2008R2,7

Version like "6.0%" -> 2008,Vista

Version like "5.2%" -> 2003,XP

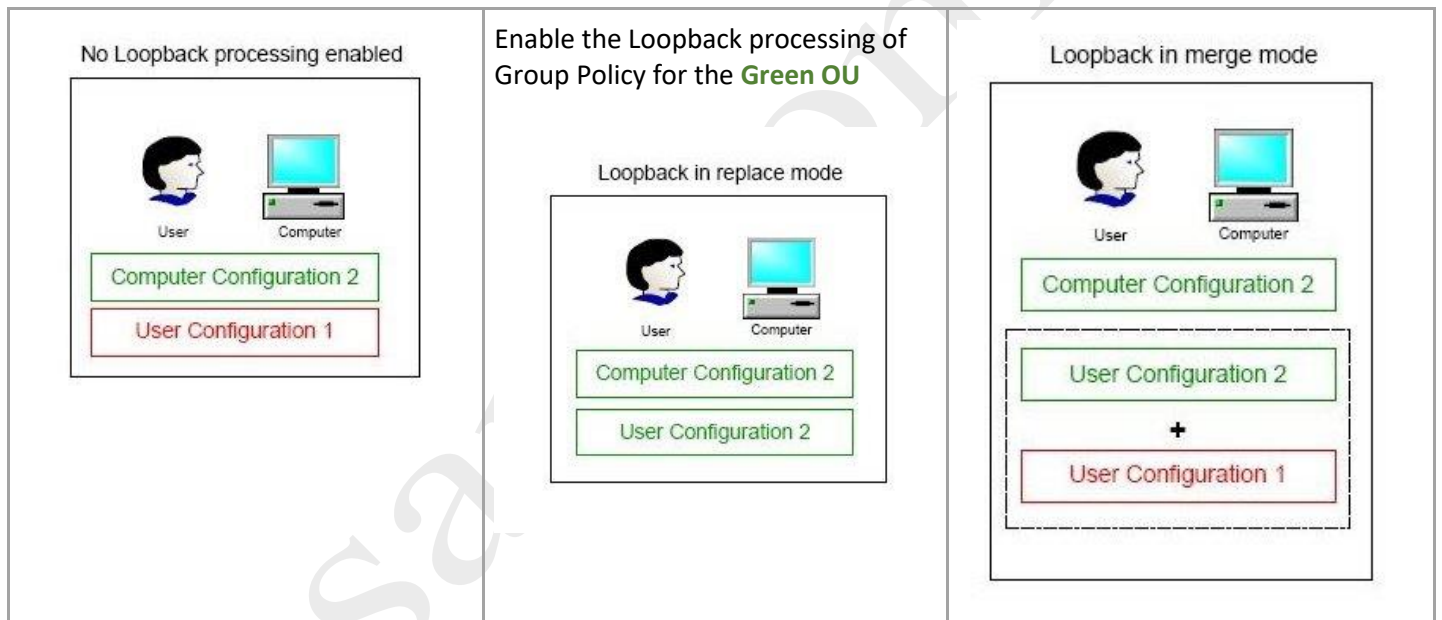
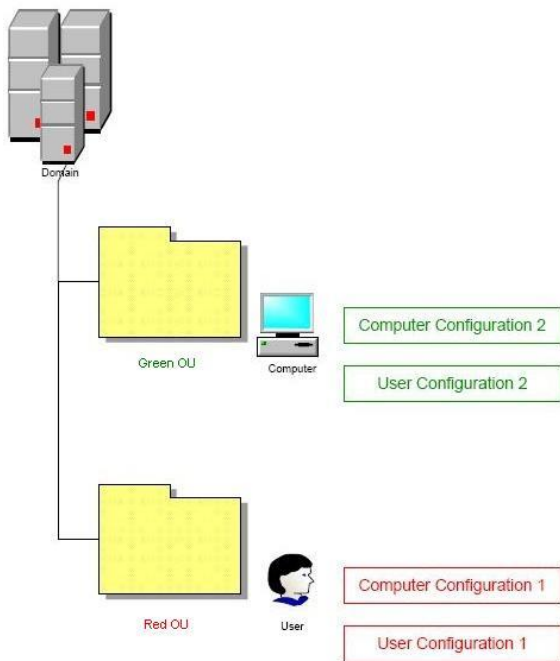
OSArchitecture -> "64-bit"

Order of execution:

- Policies in hierarchy are located. (L-S-D-OU)
- WMI Filters are checked
- Security settings are checked
- Only then after everything has passed is the policy applied

Loopback processing:

1. It is a computer configuration setting.
2. When enabled, user settings from GPOs applied to the computer apply to the logged on user.
3. Loopback processing changes the list of applicable GPOs and the order in which they apply to a user.



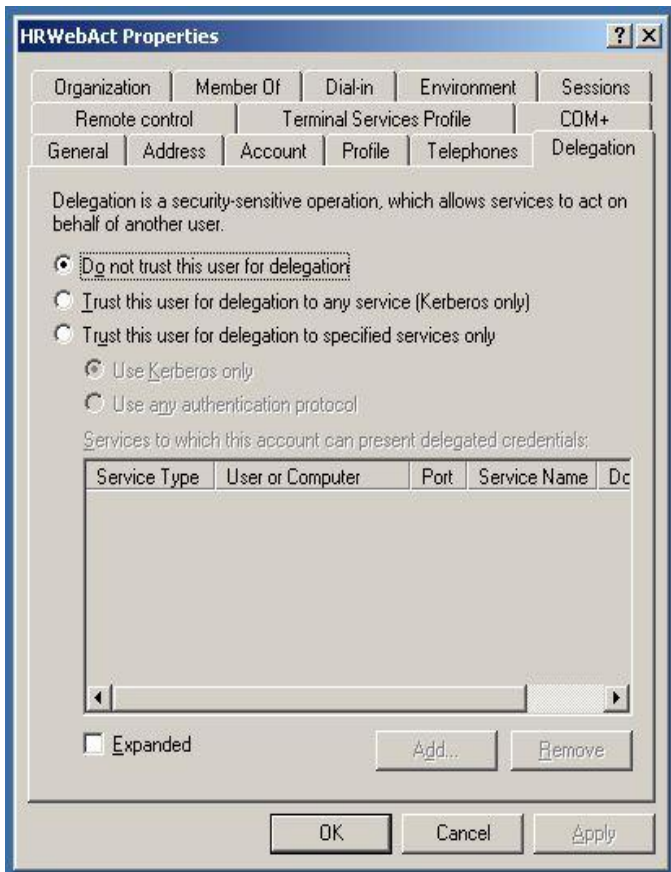
4.4 Design an Active Directory permission model:

Kerberos Delegation

Kerberos Delegation is a feature that allows an application to reuse the end-user credentials to access resources hosted on a different server. You should only allow that if you really trust the application server, otherwise the application may use your credentials to purposes that you didn't think of, like sending e-mails on your behalf or changing data in a mission critical application pretending that you made that change.

The Kerberos Delegation is configured as a property for the domain account that is used by the application as a service account. For an IIS application that is the application pool account configured for that particular application. That is the also the same domain account that you used when you configured the SPN.

If you have raised the Domain Functional level to Windows Server 2003, the Delegation property is moved for both computer accounts and user accounts to a dedicated tab page "Delegation" and you are also giving more options to control the scope of the delegation.

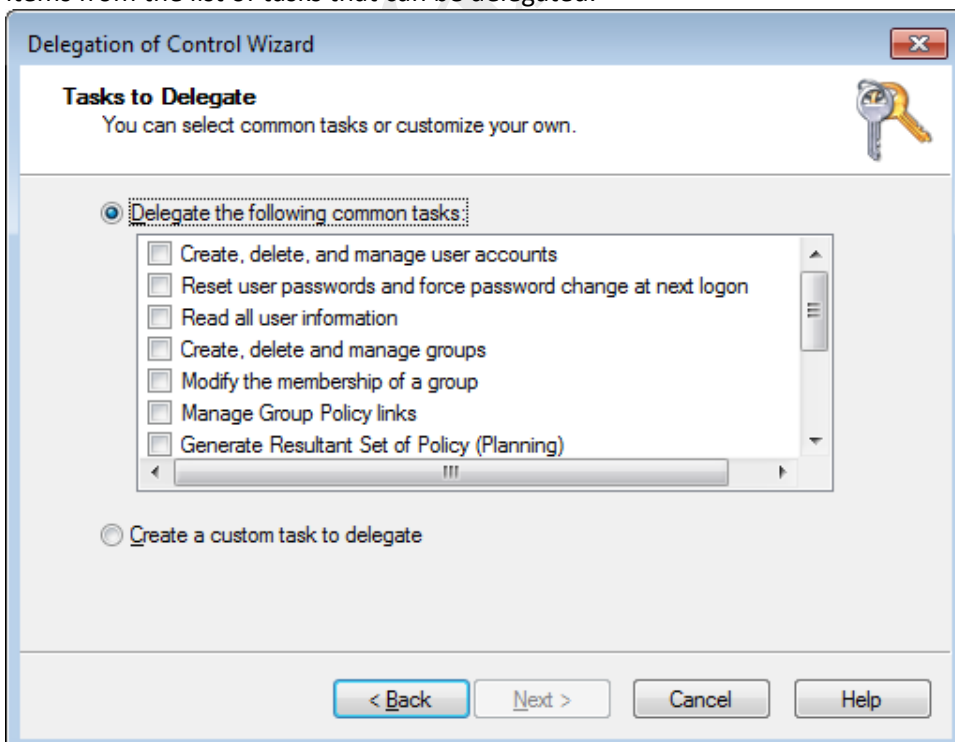


The delegation tab is only visible on the user account when you have created a SPN for that account.

Active Directory Delegation Wizard File

The Delegation of Control Wizard allows you to delegate administrative tasks to users or groups within a specific administrative scope and is primarily used to delegate data administration. This tool is driven by a customizable text file (**Delegwiz.inf**) and ships with a base set of common administrative tasks.

The list of tasks that can be delegated through the Delegation Wizard is maintained in the Delegwiz.inf file, which is created in the %windir%\System32\delegwiz.inf folder. Administrators can modify this file to add or delete items from the list of tasks that can be delegated.



5.1 Design an Active Directory sites topology:

Replication Transports

- Uniform high-speed, synchronous **RPC over IP** within a site.
- Point-to-point, synchronous, low-speed **RPC over IP** between sites.
- Low-speed, asynchronous **SMTP** between sites.

Site Link Bridge Design

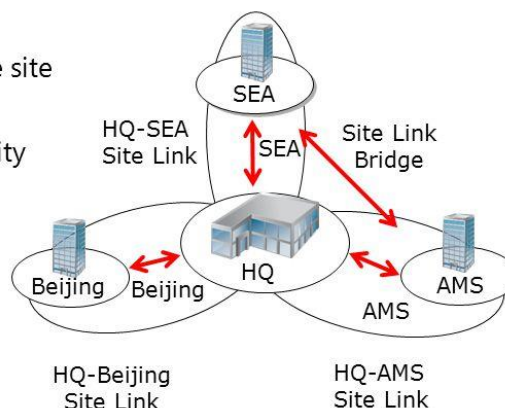
A site link bridge connects two or more site links and enables transitivity between site links. Each site link in a bridge must have a site in common with another site link in the bridge. The Knowledge Consistency Checker (KCC) uses the information on each site link to compute the cost of replication between sites in one site link and sites in the other site links of the bridge. Without the presence of a common site between site links, the KCC also cannot establish direct connections between domain controllers in the sites that are connected by the same site link bridge.

By default, all site links are transitive. We recommend that you keep transitivity enabled by not changing the default value of **Bridge all site links** (enabled by default). However, you will need to disable **Bridge all site links** and complete a site link bridge design if:

- Your IP network is not fully routed. When you disable **Bridge all site links**, all site links are considered nontransitive, and you can create and configure site link bridge objects to model the actual routing behaviour of your network.
- You need to control the replication flow of the changes made in Active Directory Domain Services (AD DS). By disabling **Bridge all site links** for the site link IP transport and configuring a site link bridge, the site link bridge becomes the equivalent of a disjointed network. All site links within the site link bridge can route transitively, but they do not route outside of the site link bridge.

What Is Site Link Bridging?

- By default, automatic site link bridging:
 - Enables ISTG to create connection objects between site links
 - Allows disabling of transitivity in the properties of the IP transport
- Site link bridges:
 - Enable you to create transitive site links manually
 - Are useful only when transitivity is disabled



Automatic Site Coverage

1. Build a list of target sites — sites that have no domain controllers for this domain (the domain of the current domain controller).
2. Build a list of candidate sites — sites that have domain controllers for this domain.
3. For every target site, follow these steps:
 - a. Build a list of candidate sites of which this domain is a member. (If none, do nothing.)

- b. Of these, build a list of sites that have the lowest site link cost to the target site. (If none, do nothing.)
- c. If more than one, break ties (reduce this list to one candidate site) by choosing the site with the largest number of domain controllers.
- d. If more than one, break ties by choosing the site that is first alphabetically.
- e. Register target-site-specific SRV records for the domain controllers for this domain in the selected site.

Powershell:

Sync-ADObject

The Sync-ADObject cmdlet replicates a single object between any two domain controllers that have partitions in common. The two domain controllers do not need to be direct replication partners. You can also use this cmdlet to populate passwords in a read-only domain controller (RODC) cache.

Example 1: Replicate an object to another location

This command replicates an object with the distinguished name

CN=AccountManagers,OU=AccountDeptOU,DC=corp,DC=contoso,DC=com from corp-DC01 to corp-DC02.

PS C:\> Sync-ADObject -Object "CN=AccountManagers,OU=AccountDeptOU,DC=corp,DC=contoso,DC=com" -Source "corp-DC01" -Destination "corp-DC02"

Example 2: Pre-cache a password to a domain controller

This command pre-caches the password of Patti Fuller to the read-only domain controller corp-RODC01 using the SAM account name of the user.

PS C:\> Get-ADUser -Identity pattifuller | Sync-ADObject -Destination "corp-RODC01" -PasswordOnly

Get-ADDomainController

Gets one or more Active Directory domain controllers based on discoverable services criteria, search parameters or by providing a domain controller identifier, such as the NetBIOS name.

Get all ROGCs in the child domain to which the client is connected.

Get-ADDomainController -Server "research.fabrikam.com" -Filter { isGlobalCatalog -eq \$true -and isReadOnly -eq \$true }

Get a global catalog in the current forest using Discovery.

Get-ADDomainController -Discover -Service "GlobalCatalog"

Get-ADReplicationUpToDatenessVectorTable

The **Get-ADReplicationUpToDatenessVectorTable** cmdlet displays the highest Update Sequence Number (USN) for the specified domain controller(s). This information shows how up-to-date a replica is with its replication partners. During replication, each object that is replicated has USN and if the object is modified, the USN is incremented. The value of the USN for a given object is local to each domain controller where it has replicated are number is different on each domain controller.

Repadmin /showrepl

The **repadmin /showrepl** command helps you understand the replication topology and replication failures. It reports status for each source domain controller from which the destination has an inbound connection object. The status report is categorized by directory partition.

Repadmin /syncall

Synchronizes a specified domain controller with all of its replication partners.

5.2 Design a domain controller strategy

RODC:

Read-only domain controllers (RODCs) are a new feature of Active Directory Domain Services (AD DS) in Windows Server 2008. RODCs are additional domain controllers for a domain that host complete, read-only copies of the partitions of the Active Directory database and a read-only copy of the SYSVOL folder contents. By selectively caching credentials, RODCs address some of the challenges that enterprises can encounter in branch offices and perimeter networks

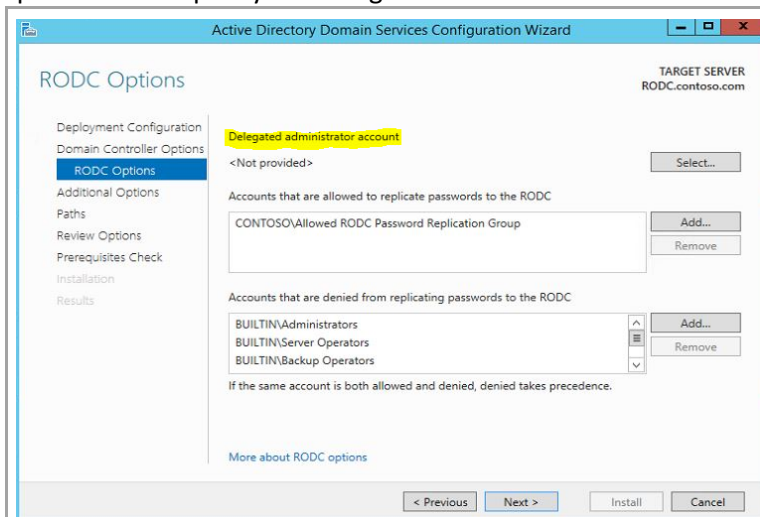
Prerequisites

- **Ensure that the forest functional level is Windows Server 2003 or higher**
- **Deploy at least one writable domain controller** running Windows Server 2008 or Windows Server 2008 R2< in the same domain as the RODC and ensure that the writable domain controller is also a DNS server

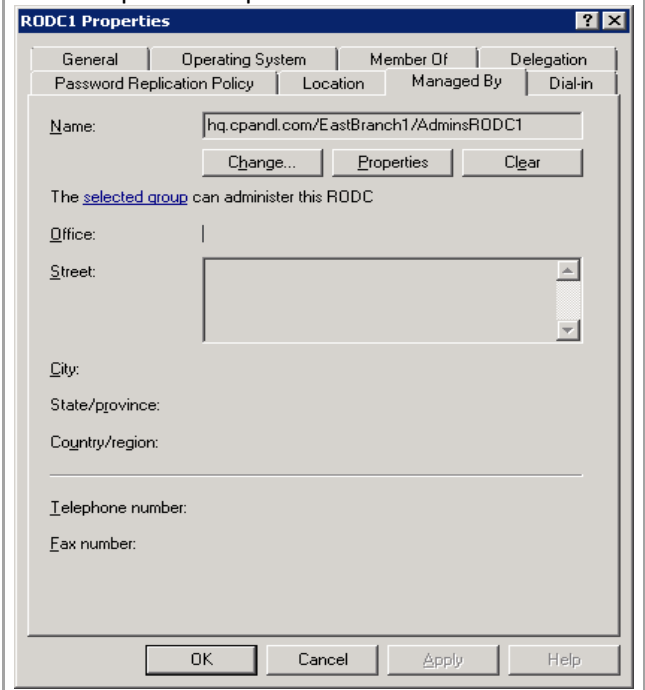
Administrator Role Separation:

With the introduction of RODCs, domain administrators can delegate both the installation and the administration of RODCs to any domain user, without granting them any additional rights in the domain. The ability to perform this delegation is called ARS.

If you are installing an RODC at the command line or by using an answer file, add the **/DelegatedAdmin** parameter to specify the delegated RODC administrator.

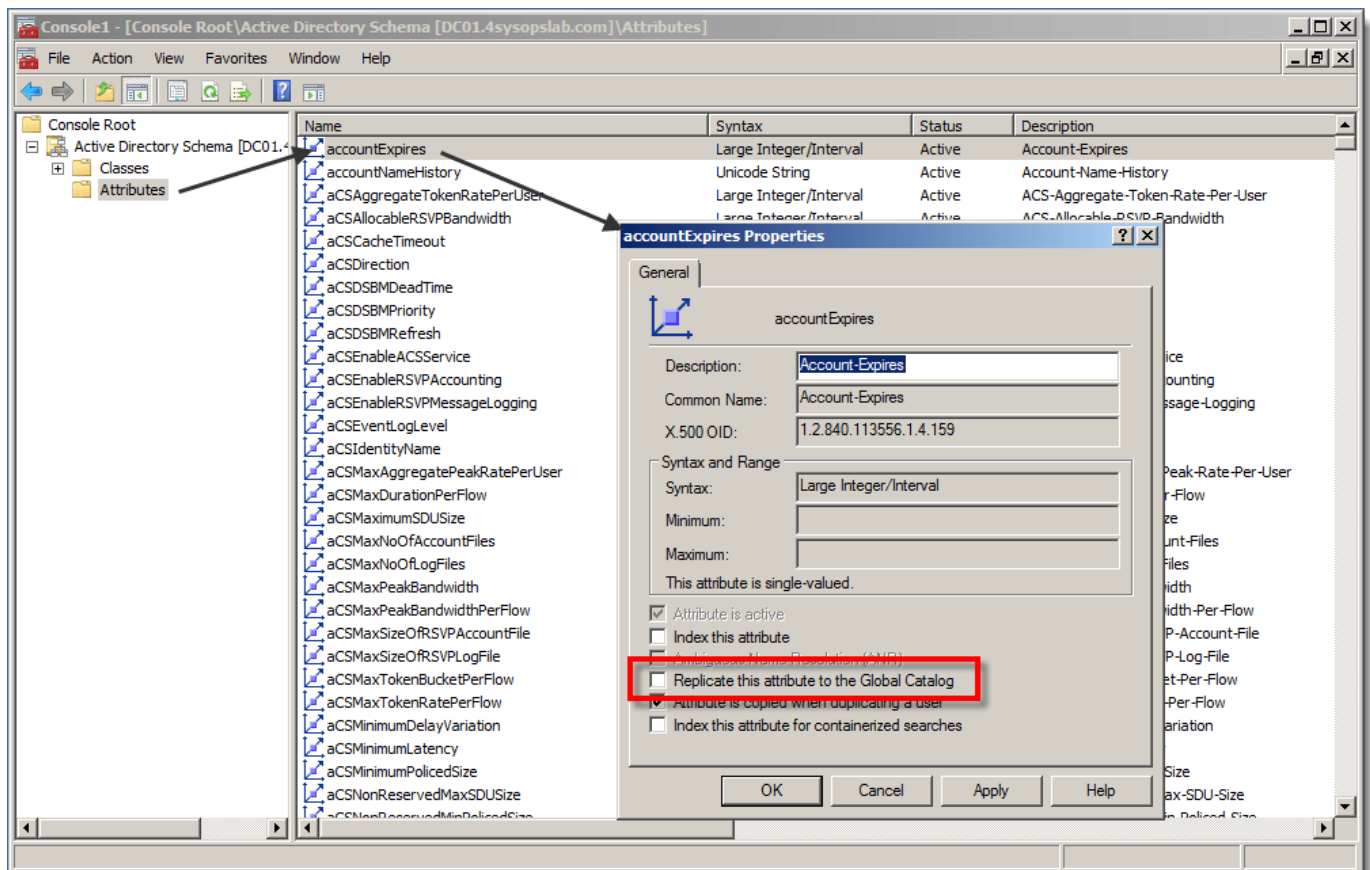


To specify the delegated RODC administrator after installation, you can use either of the following options: Modify the **Managed By** tab of the RODC account properties in the Active Directory Users and Computers snap-in



Global Catalogue Partial Attribute Set

The Partial Attribute Set (PAS) is the subset of attributes in the Active Directory Schema that are replicated to the Global Catalog (GC). Each Domain Controller (DC) has a complete writable replica of the domain the DC resides in. If it is also a Global Catalog server, then it also has a partial read-only replica of all other naming contexts in the forest. The partial replicas include all objects, but only selected attributes for those objects. The selected attributes are those in the Partial Attribute Set.



Filtered attribute set:

The RODC FAS is a dynamic set of attributes that is not replicated to any RODCs in the forest. These attributes are not replicated to RODCs because they contain sensitive data.

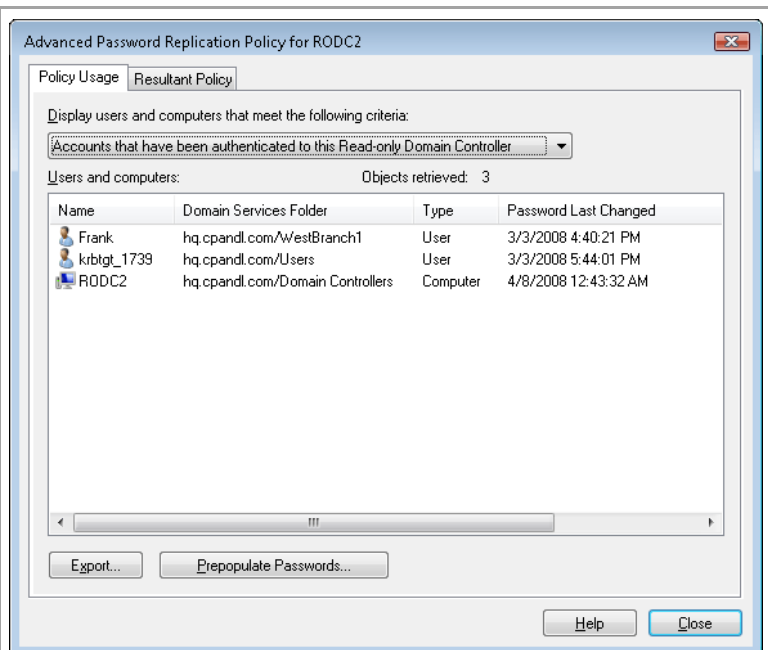
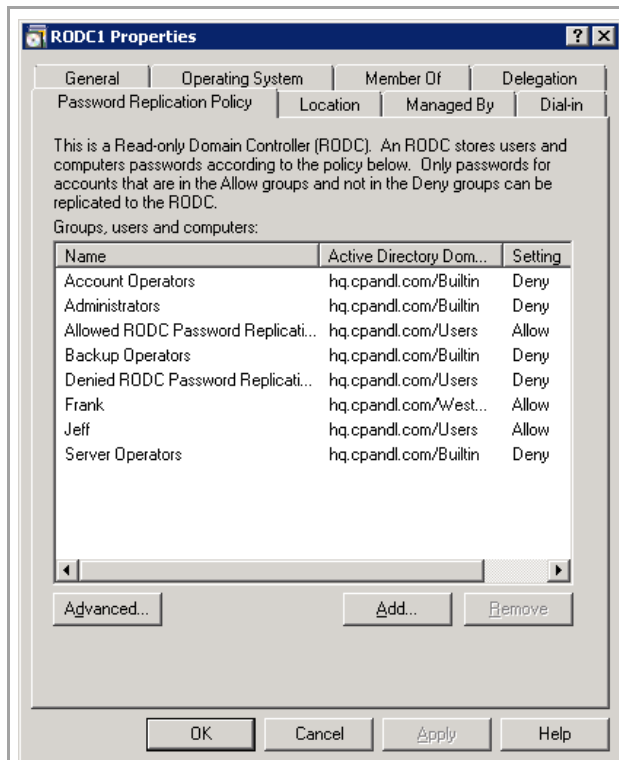
Password replication policy:

The PRP acts as an access control list (ACL). It determines whether an RODC is permitted to cache credentials for an account.

A default PRP is defined that applies to any newly installed RODC. The default PRP specifies that no account passwords can be cached on any RODC, and certain accounts are explicitly denied from being cached on any RODC.

You can cache passwords in advance by using the Active Directory Users and Computers snap-in or by using the **repadmin /rodcpwdrepl** command

Active Directory Users and Computers -> Domain Controllers -> RODC account object -> Properties



Adding Attributes to the RODC Filtered Attribute Set:

To add an attribute to an RODC FAS, you must first determine the current **searchFlags** value of the attribute that you want to add, and then set the following values for **searchflags**:

To add the attribute to the RODC FAS, set the 10th bit to **0x200**.

To mark the attribute as confidential, set the 7th bit to **0x080 (128)**.

Domain controller cloning:

Requirements:

- Source virtual DC must be running Windows Server 2012.
- PDC emulator role holder must be online and available to the cloned DC *and* must be running Windows Server 2012
- Hypervisor must support VM-GenerationID
 - VM-GenerationID is supported by the following hypervisors:
 - All versions of Hyper-V that are Windows Server 2012/Windows 8 and later
 - VMware vSphere 5.0 with Update 2
 - VMware vSphere 5.1 and later
 - XenServer 6.2.0-70446 and later

Steps

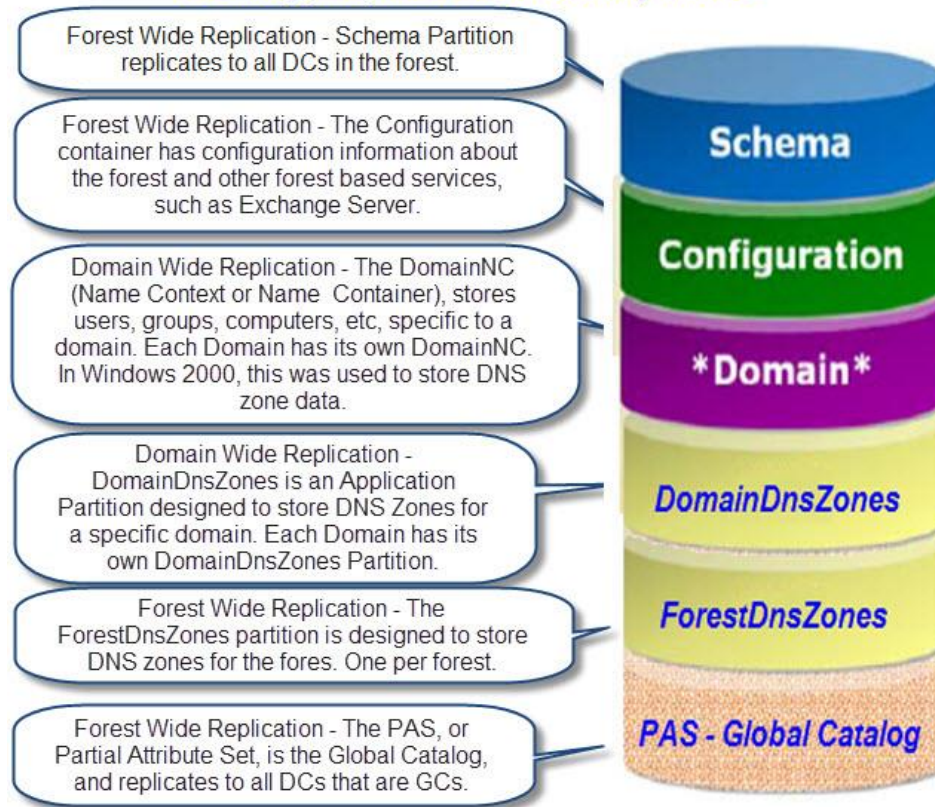
- Add the source DC to the Cloneable Domain Controllers group
- Check for unsupported apps *Get-ADDCCloneExcludedApplicationList*
- Generating the allow list *Get-ADDCCloneExcludedApplicationList -GenerateXML*
Saved in c:\windows\ntds\CustomDCCloneAllowList.xml
- Generate clone config file
`New-ADDCCloneConfigFile -IPv4Address 10.2.1.10 -IPv4DefaultGateway 10.2.1.1 -IPv4SubnetMask 255.255.255.0 -IPv4DNSResolver 10.1.1.10,10.1.1.11 -Static -SiteName CORPDR`
c:\windows\ntds\DCCloneConfig.XML
- Export the VM
- Import the VM and Boot up

Directory Partitions:

To scale to tens of millions of objects, a forest is partitioned into domains. Each Active Directory domain controller can be a member of one domain, and domain controllers within the same domain contain the same information. Domain controllers from different domains share the same configuration and schema data, but they do not share the same domain data. The means to distributing storage in this manner is the *directory partition*, which is also called a "naming context."

Active Directory Data Store Logical Partitions

Ace Fekay, MCT, Microsoft MVP Directory Services



FSMO Roles

Domain controllers that perform operations master roles, also known as Flexible Single Master Operations (FSMO) roles, manage critical aspects of Active Directory. Three operations roles and two forest-wide operations master roles exist in each domain.

Role	Scope	Description
Schema master	Forest	Maintains the structure of the Active Directory schema, in particular the list of object types and the attributes they contain
Domain naming master	Forest	Contains the domain and forest structure; handles creation and removal of domains in the forest
Primary domain controller (PDC) emulator master	Domain	Performs password changes for the domain and begins replicating the changes to other domain controllers
Relative ID (RID) master	Domain	Manages ID numbers for the domain, issuing pools to domain controllers to assign to objects as they are created
Infrastructure operations master	Domain	Tracks membership of user principals from other domains for groups within the domain

When an operations master becomes unavailable, different symptoms occur, depending on the role. When the schema master is unavailable, any attempted modifications to the schema fail. Addition and removal of domains

from the forest fail if the domain-naming master is offline. Problems with the RID master result in domain controllers being unable to create new objects after their RID pool is exhausted. Problems with users updating their passwords can be attributed to problems with the PDC emulator master. If the infrastructure master becomes unavailable, problems related to interdomain group membership can occur. Remember that problems related to a missing or unavailable operations master might not be noticed for an extended period of time.

Adprep.exe:

Adprep.exe commands run automatically as needed as part of the AD DS installation process on servers that run Windows Server 2012 or later. The commands need to run in the following cases:

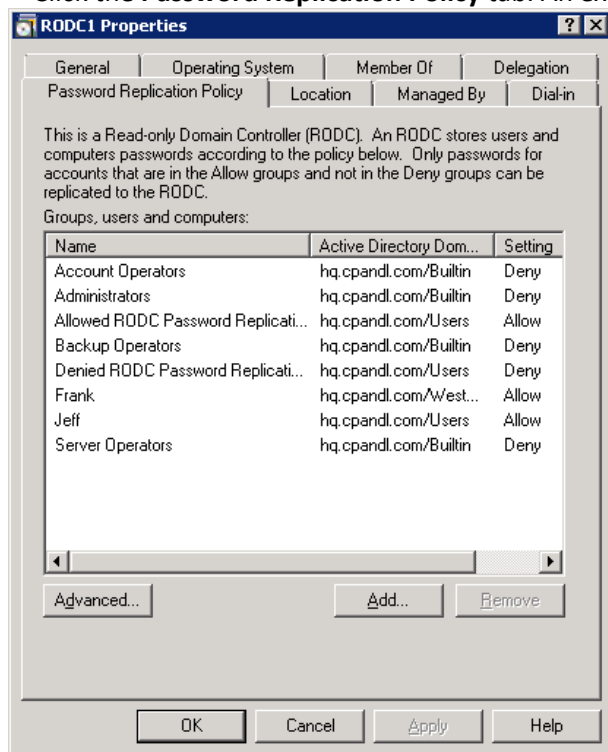
- Before you add the first domain controller that runs a version of Windows Server that is later than the latest version that is running in your existing domain.
- Before you upgrade an existing domain controller to a later version of Windows Server, if that domain controller will be the first domain controller in the domain or forest to run that version of Windows Server.

Command	Domain controller	Number of times to run the command
adprep /forestprep	Must be run on the schema operations master for the forest.	Once for the entire forest
adprep /domainprep	Must be run on the infrastructure operations master for the domain.	Once in each domain where you plan to install an additional domain controller that runs a later version of Windows Server than the latest version that is running in the domain. <div>Note Domains where you will not add a new domain controller will be affected by adprep /forestprep, but they do not require you to run adprep /domainprep.</div>
adprep /domainprep /gpprep	Must be run on the infrastructure operations master for the domain. If you already ran the /gpprep parameter for Windows Server 2003, you do not have to run it again for later versions of Windows Server.	Once in each domain within the forest
adprep /rodcprep <div>Note This command is optional. Run it only if you want to install a read-only domain controller (RODC).</div>	Can be run from any computer. This command performs operations remotely. For the operations to complete successfully, the domain naming operations master for the forest and the infrastructure operations master for each application directory partition and each domain partition must be accessible. If you already ran this command for Windows Server 2008, you do not have to run it again for later versions of Windows Server.	Once for the entire forest

5.3 Design and implement a branch office infrastructure

View the PRP using Active Directory Users and Computers

1. Open Active Directory Users and Computers.
2. Ensure that you are connected to the correct domain. To connect to the appropriate domain, in the details pane, right-click the Active Directory Users and Computers object, and then click **Change Domain**.
3. Expand **Domain Controllers**, right-click the RODC account object for which you want to modify the PRP, and then click **Properties**.
4. Click the **Password Replication Policy** tab. An example is shown in the following illustration.

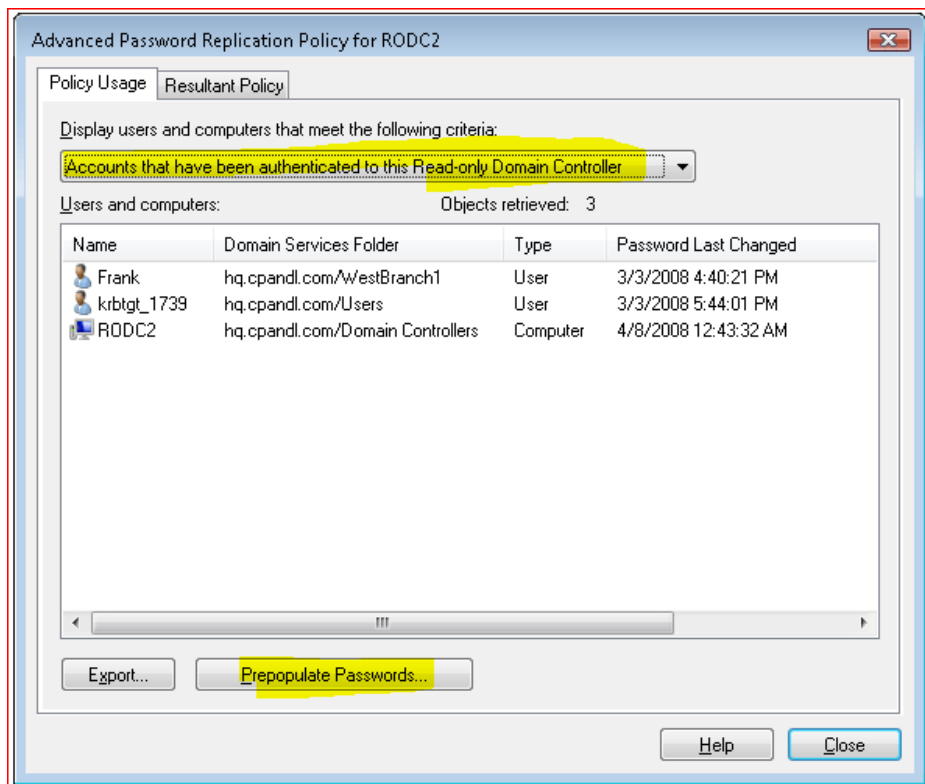


repadmin /prp view rod2.pasan.com.au allow

View the authenticated accounts:

Click **Advanced**.

In the drop-down list, click **Accounts that have been authenticated to this Read-only Domain Controller**, as shown in the following illustration.



repadmin /prp view rodc2.hq.cpandl.com auth2

BranchCache:

is designed to reduce WAN link utilization and improve application responsiveness for branch office workers who access content from servers in remote locations. Branch office client computers use a locally maintained cache of data to reduce traffic over a WAN link. The cache can be distributed across client computers (Distributed Cache mode) or can be housed on a server in the branch (Hosted Cache mode).

Distributed Cache mode

If client computers are configured to use Distributed Cache mode, the cached content is distributed among client computers on the branch office network. No infrastructure or services are required in the branch office beyond client computers running Windows 7<.

Hosted Cache mode

In hosted cache mode, cached content is maintained on a computer running Windows Server 2008 R2 on the branch office network.

Powershell:

Cmdlet	Description
Add-BCDataCacheExtension	Increases the amount of cache storage space that is available on a hosted cache server by adding a new cache file.
Clear-BCCache	Deletes all data in all data and hash files.
Disable-BC	Disables the BranchCache service.
Enable-BCDistributed	Enables BranchCache and configures a computer to operate in distributed cache mode.
Enable-BCHostedClient	Configures BranchCache to operate in hosted cache client mode.

Enable-BCHostedServer	Configures BranchCache to operate in hosted cache server mode.
Get-BCClientConfiguration	Retrieves the current BranchCache client computer settings.
Get-BCContentServerConfiguration	Retrieves the current BranchCache content server settings.
Get-BCDataCache	Retrieves the BranchCache data cache.
Get-BCHostedCacheServerConfiguration	Retrieves the current BranchCache hosted cache server settings.
Get-BCStatus	Retrieves a set of objects that provide BranchCache status and configuration information.
Publish-BCFileContent	Generates hashes for files in shared folders.
Remove-BCDataCacheExtension	Deletes a data cache file.
Reset-BC	Resets BranchCache to the default configuration.
Set-BCCache	Modifies the cache file configuration.
Set-BCDataCacheEntryMaxAge	Modifies the maximum amount of time that data can remain in the cache.
Set-BCMinSMBLatency	Sets the minimum latency that must exist between client and server before transparent caching functions are utilized.

This example moves the cache file from C:\datacache to D:\datacache.

```
PS C:\> Set-BCCache -Path C:\datacache -MoveTo D:\datacache
```

This example increases data cache files from 10% to 20%.

```
PS C:\> Get-BCDataCacheExtension | Where-Object -FilterScript
{$_.MaxCacheSizeAsPercentageOfDiskVolume -Eq 10} | Set-BCCache -Percentage 20
```

This command adds a data cache extension in the C:\datacache directory reserving ten percent of C:

```
PS C:\> Add-BCDataCacheExtension -Path "C:\datacache" -Percentage 10
```