

Microsoft 70-412

Configuring Advanced Windows Server 2012 Services



ABOUT THE EXAM

The Microsoft 70-412 is part three of a series of three exams that test the skills and knowledge necessary to administer a Windows Server 2012 infrastructure in an enterprise environment. Passing this exam validates a candidate's ability to perform the advanced configuring tasks required to deploy, manage, and maintain a Windows Server 2012 infrastructure, such as fault tolerance, certificate services, and identity federation. Passing this exam along with the other two exams confirms that a candidate has the skills and knowledge necessary for implementing, managing, maintaining, and provisioning services and infrastructure in a Windows Server 2012 environment.

Six major topics make up the Microsoft 70-412 Certification. The topics are as follows:

- Configure and manage high availability
- Configure file and storage solutions
- Implement business continuity and disaster recovery
- Configure network services
- Configure the Active Directory infrastructure
- Configure identity and access solutions

This guide will walk you through all the skills measured by the exam, as published by Microsoft.

OBJECTIVES

CHAPTER 1: CONFIGURE AND MANAGE HIGH AVAILABILITY

- 1.1 Configure Network Load Balancing
- 1.2 Configure failover clustering
- 1.3 Manage failover clustering roles
- 1.4 Manage Virtual Machine (VM) movement

CHAPTER 2: CONFIGURE FILE AND STORAGE SOLUTIONS

- 2.1 Configure advanced file services
- 2.2 Implement Dynamic Access Control (DAC)
- 2.3 Configure and optimize storage

CHAPTER 3: IMPLEMENT BUSINESS CONTINUITY AND DISASTER RECOVERY

- 3.1 Configure and manage backups
- 3.2 Recover servers
- 3.3 Configure site-level fault tolerance

CHAPTER 4: CONFIGURE NETWORK SERVICES

- 4.1 Implement an advanced Dynamic Host Configuration Protocol (DHCP) solution
- 4.2 Implement an advanced DNS solution
- 4.3 Deploy and manage IPAM

CHAPTER 5: CONFIGURE THE ACTIVE DIRECTORY INFRASTRUCTURE

- 5.1 Configure a forest or a domain
- 5.2 Configure trusts
- 5.3 Configure sites
- 5.4 Manage Active Directory and SYSVOL replication

CHAPTER 6: CONFIGURE IDENTITY AND ACCESS SOLUTIONS

- 6.1 Implement Active Directory Federation Services 2.1 (AD FSv2.1)
- 6.2 Install and configure Active Directory Certificate Services (AD CS)
- 6.3 Manage certificates
- 6.4 Install and configure Active Directory Rights Management Services (AD RMS)

CHAPTER 1 – CONFIGURE AND MANAGE HIGH AVAILABILITY

1.1 CONFIGURE NETWORK LOAD BALANCING (NLB)

Install NLB nodes

Round Robin Load Balancing is for DNS service. It works by cycling through the IP addresses corresponding to a server group. Hardware load balancers are dedicated for routing TCP/IP packets to various servers within a cluster. Software Load Balancers are usually options that come shipped with expensive server application packages. Software based solutions usually cost less but are often application specific.

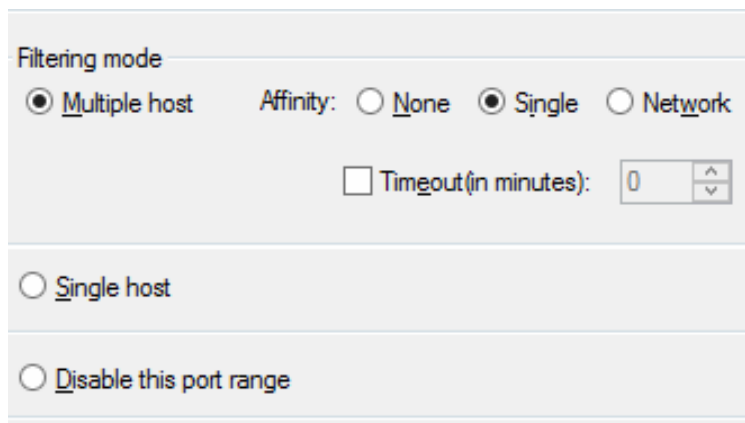
Windows Server 2012 can balance load requests across the cluster - you can have max 32 computers in a cluster. To set up such a cluster, all participating hosts must stay in the same subnet.

Configure NLB prerequisites

NLB doesn't allow multicast and unicast to take place within a cluster. To run in unicast mode, the network adapter must allow the changing of MAC address. Only TCP/IP can be used on the participating adapter, and that the IP addresses of the participating servers must NOT be dynamic.

Configure affinity

Affinity is a parameter for Multiple host filtering mode only. None means multiple connections from the same client can be processed by different cluster hosts. Single means multiple requests from the same client should be directed to only the same cluster host. Class C affinity means multiple requests from the same TCP/IP Class C address range will be directed to the same cluster host. This option is needed if your clients are using multiple proxy servers to access the cluster.



The screenshot shows the 'Filtering mode' section of the Network Load Balancing configuration. It includes three radio buttons for the filtering mode: 'Multiple host' (selected), 'Single host', and 'Disable this port range'. The 'Affinity' section has three radio buttons: 'None', 'Single' (selected), and 'Network'. Below the affinity options is a checkbox for 'Timeout(in minutes):' with a value of '0' and a spin button.

Filtering mode

☒ Multiple host Affinity: ☐ None ☒ Single ☐ Network

☐ Timeout(in minutes): 0

☐ Single host

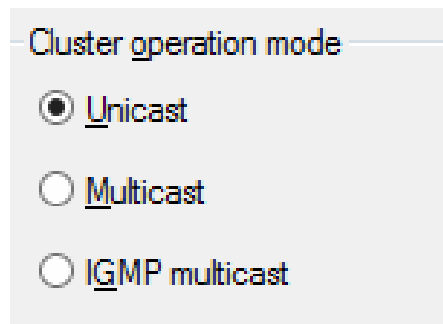
☐ Disable this port range

Configure port rules

You use port rules are for controlling how the cluster network traffic is handled. There are 3 different filtering modes, and you can have max 32 port rules per NLB cluster. Multiple hosts provides scaled performance and fault tolerance. Single host provides port specific fault tolerance. Disable is for blocking all network traffics that are addressed to a specific range of ports.

Configure cluster operation mode

The Cluster Operation Mode is either unicast or multicast (not enabled by default). If multicast is turned on, the cluster MAC address will be converted into a multicast address, and you will be allowed to use IGMP. Internet Group Management Protocol IGMP support useful for limiting switch flooding.



The screenshot shows a configuration window titled "Cluster operation mode". It contains three radio button options: "Unicast" (which is selected), "Multicast", and "IGMP multicast".

Upgrade an NLB cluster

You may upgrade an existing NLB cluster to Windows Server 2012 if you take the entire cluster offline and then upgrade all the hosts. Or you may perform a rolling upgrade which is all about taking individual cluster hosts offline one by one. Before making the upgrade, you need to first verify that the involved applications and roles/features running on the cluster are compatible with Windows Server 2012. The target node's initial host state should be set to Stopped first. When the upgrade is complete on the host, you should first verify that the applications work fine before adding it back to the cluster.

1.2 CONFIGURE FAILOVER CLUSTERING

Configure Quorum

The quorum configuration determines the number of failures a cluster can sustain at the max - it is always determined by the number of voting elements that are part of the active cluster membership of the cluster. A quorum witness can have an additional single quorum vote since one quorum witness can be setup for each cluster (it may be a designated disk resource or a file share resource).

There are several quorum modes. With Node majority (no witness), only nodes can have votes since there is no quorum witness configured. Node majority with witness means both nodes and quorum witness can vote (witness vote allowed). No majority (disk witness only) means only the disk witness and no one else can have vote. It is recommended that the voting elements in the cluster be set to an odd number. The use of a disk witness is recommended as long as all nodes can see the disk. A disk-only configuration, however, is never recommended.

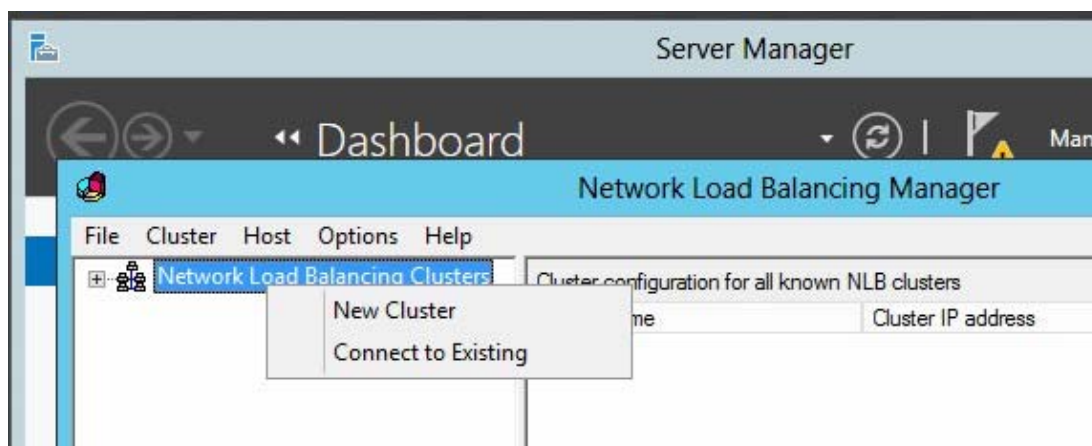
Vote weight allows for flexibility - the weight of each vote can be adjusted – the default is 1.

Cluster configuration can be done via the Failover Cluster Manager GUI. Alternatively, you can use the Set-ClusterQuorum Powershell cmdlet.

In the case of a failover cluster, whenever it goes online the first disk that goes online together becomes the one to be associated with the quorum. The failover cluster executes a disk arbitration algorithm to determine ownership of that disk (and repeat this on all other disks).

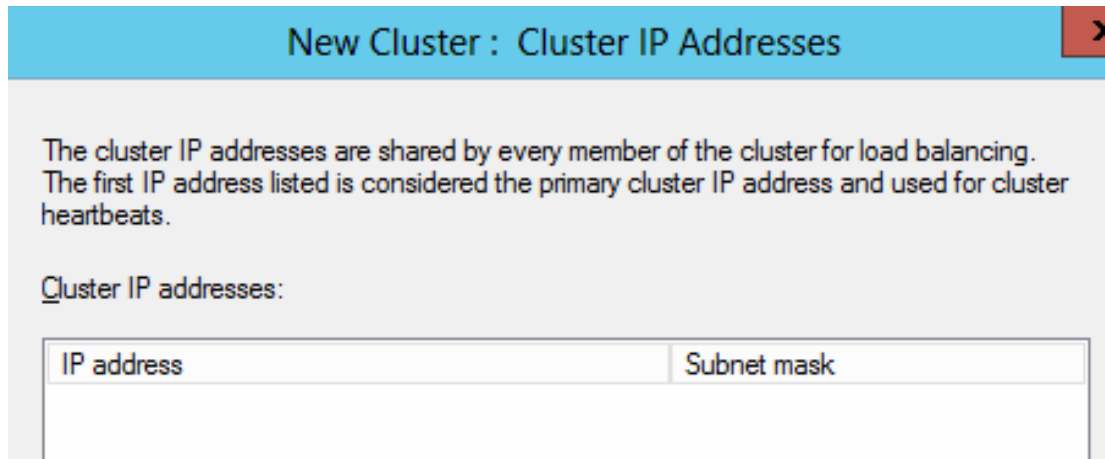
Configure cluster networking

In Windows Server 2012, you use the Server Manager's Network Load Balancing Manager to configure NLB clustering. Through the console you can configure new cluster and also enable logging.



You use the cluster validation wizard to run focused tests on the planned cluster nodes to seek an accurate assessment of how well failover clustering may be implemented on the proposed configuration. To begin adding hardware to a failover cluster, you first connect the hardware to the failover cluster and then run the cluster validation wizard.

Proper IP address configuration is necessary both at the host and cluster levels, which can all be done via the GUI.

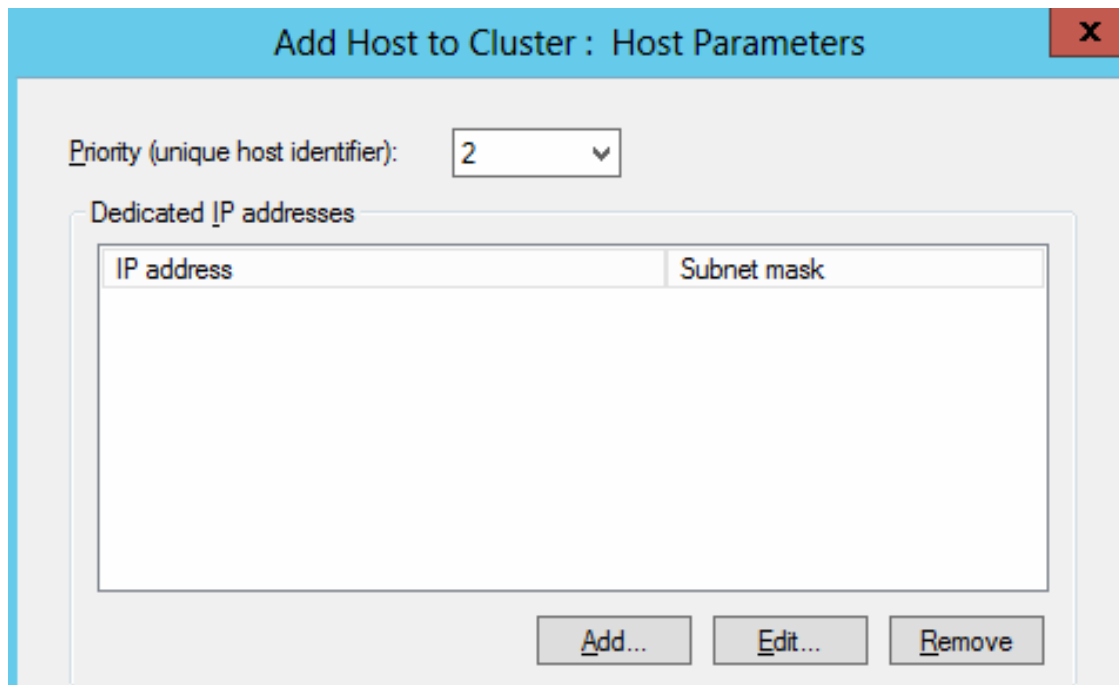


New Cluster : Cluster IP Addresses

The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.

Cluster IP addresses:

IP address	Subnet mask
------------	-------------



Add Host to Cluster : Host Parameters

Priority (unique host identifier):

Dedicated IP addresses

IP address	Subnet mask
------------	-------------

Restore single node or cluster configuration

A cluster without enough quorum votes will not start. However, you can override this by forcing the cluster to start in ForceQuorum mode via the Start-ClusterNode cmdlet.

For a backup to be performed, the cluster must be running with a quorum. Only disks that are Online and owned by the involved cluster node can be backed up or restored. When you restore from a backup, you can choose to restore only the cluster configuration or the disk data or both.

Configure cluster storage

All components of the storage stack in a cluster setup should be identical across all the nodes inside the cluster. It is particularly important for the multipath I/O MPIO software and the Device Specific Module DSM software components to be identical. The host bus adapter HBA, the relevant HBA drivers and the HBA firmware attached to the cluster storage should be identical as well.

Implement Cluster Aware Updating

Cluster-Aware Updating CAU can automate the software updating process on clustered servers. It can put a node into node maintenance mode, then move the clustered roles off the node and then install the updates prior to performing a restart when needed.

CAU can schedule Updating Runs to take place on regular daily, weekly, or monthly intervals. It does not work for Windows Server 2008/R2 though. You may start CAU via Server Manager, Failover Cluster Manager or the ClusterUpdateUI.exe utility.

Upgrade a cluster

You use the Migrate A Cluster Wizard makes it easy to migrate services and applications from an earlier cluster to Windows Server 2012. The wizard has a GUI for migrating the configuration settings for clustered roles. Since it does not migrate settings of the cluster and storage, you must first ensure that the new cluster is properly configured and ready for the migration process.

You want to know that cluster upgrade is kind of similar between Windows Server 2008 and Windows Server 2012.

1.3 MANAGE FAILOVER CLUSTERING ROLES

Configure role-specific settings including continuously available shares

Continuously Available File Shares CAFS involves making use of the Windows file sharing capabilities through a cluster to increase the availability of file shares. You configure this via the High Availability Wizard. For this feature to work, SMB 3.0 is required, which supports features like SMB Scale-Out, SMB Direct, and SMB Multichannel.

The CAFS general use file server implementation can be used to allow a file share to be supported on a failover cluster. On the other hand, the scale-out file server implementation option is for supporting applications such as Hyper-V and Database Server, with the ultimate goal of zero downtime. Do note that the implementation has a limit of max 4 servers. Also, CAFS will not work on the Essentials or Foundation editions.

Select an option for a clustered file server:

☒ File Server for general use

Use this option to provide a central location on your network for users to share files or for server applications that open and close files frequently. This option supports both the Server Message Block (SMB) and Network File System (NFS) protocols. It also supports Data Deduplication, File Server Resource Manager, DFS Replication, and other File Services role services.

☐ Scale-Out File Server for application data

Use this option to provide storage for server applications or virtual machines that leave files open for extended periods of time. Scale-Out File Server client connections are distributed across nodes in the cluster for better throughput. This option supports the SMB protocol. It does not support the NFS protocol, Data Deduplication, DFS Replication, or File Server Resource Manager.

You may then use the New Share Wizard to determine the type of CAFS to create. SMB Share—Quick is general purpose while SMB Share—Applications is for supporting applications.

File share profile:

SMB Share - Quick

SMB Share - Advanced

SMB Share - Applications

NFS Share - Quick

NFS Share - Advanced

Configure VM monitoring

The Failover Cluster Manager allows you to monitor the health of clustered VMs. You can right click the clustered VM and then select Configure Monitoring from the More Actions menu item. You may then select the services to monitor. alternatively you can use Add-ClusterVMMonitoredItem to enable monitoring via the Powershell. VM monitoring does require that you have Windows Server 2012 for both the host and guest OS.

Configure failover and preference settings

Failover-Clustering is the core Failover Clustering feature without any management tools. RSAT-Clustering-Mgmt has the Failover Cluster Manager snap-in and also the Cluster-Aware Updating interface. RSAT-Clustering-PowerShell has the relevant cmdlets plus the Cluster-Aware Updating module for PowerShell. RSAT-Clustering-AutomationServer has the deprecated Component Object Model programmatic interface, while RSAT-Clustering-CmdInterface offers the deprecated cluster.exe command-line tool. They can all be installed via the Server Manager's Add Roles and Features Wizard.

Add features that are required for Failover Clustering?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- ▲ Remote Server Administration Tools
 - ▲ Feature Administration Tools
 - ▲ Failover Clustering Tools
 - [Tools] Failover Cluster Management Tools
 - [Tools] Failover Cluster Module for Windows PowerShell

1.4 MANAGE VIRTUAL MACHINE (VM) MOVEMENT

Perform Live Migration; perform quick migration

With Failover Cluster Manager, cluster migration can be in the form of:

- Live migration
- Quick migration
- Moving VM to another node

You may not use live migration to move multiple VM together at the same time. Only one live migration is allowed to take place at a time. For live and quick migration, the hardware and system settings of the involved nodes should be highly similar if not totally identical.

With Live Migration, Hyper-V connects to the destination host and produces an empty VM. Then it copies the VM's memory to the new VM. The full memory contents are replicated to the destination host through the network. Shared nothing live migration means changes made during migration are logged for applying to the VM on the destination host later.

With Quick Migration, a VM is first placed in the saved state, then its memory information is transmitted to the target host for starting the VM in there - the goal is minimal downtime.

Perform storage migration

To migrate the storage of a running VM you need to perform storage migration. It works assuming that the involved VM is configured to use only virtual hard disks and nothing else for storage. During storage migration the involved VM can still run without downtime.

Import, export, and copy VMs

You can import and export VMs between different Windows Server versions. To import a VM into Windows Server 2012, to avoid troubles it should first be exported with Windows Server 2008 R2 so that the import process can find it. HOWEVER, technically Windows Server 2012 Hyper-V can import a VM that was not previously exported by reading the raw configuration XML file. Note that:

- You use Import-VM to import a VM (you must supply a XML configuration file as an argument).
- You use Export-VM to export a VM (you do not need to supply the configuration file).
- You use Get-VM to retrieve all running VMs.
- To start or stop a VM you use Start-VM and Stop-VM respectively.

Through the Virtual Machine Manager Administrator Console you can choose the Clone action to copy a VM via the New Virtual Machine Wizard. You may either place the virtual machine on a host or store the VM in the library. You cannot change the relevant OS settings though.

Migrate from other platforms (P2V and V2V)

V2V means converting a VM to a VMM Virtual Machine while P2V means converting a Physical Server to a VM. Before performing a V2V operation, you need to first add the necessary VMWare server-based virtual machine files. The .vmx file describes the properties and structure of a VM. The .vmdk file is the VMware virtual hard disk.

You may use the Convert Virtual Machine Wizard to perform V2V conversion. On the other hand, to perform P2V the Virtual Machine Manager will need to install software on the physical computer for gathering the necessary information. This will be removed upon conversion completion.

CHAPTER 2 – CONFIGURE FILE AND STORAGE SOLUTIONS

2.1 CONFIGURE ADVANCED FILE SERVICES

Configure NFS data store

Services for **Network File System (NFS)** provides support for file sharing between Windows and UNIX:

- UNIX-based client computers accessing resources on computers running Windows Server 2012 - this is done via Server for NFS
- Windows Server based computers accessing resources on UNIX file servers - this is done via Client for NFS

You use the Services for NFS GUI snap-in to manage each installed component of Services for NFS. To use it, you must be a member of the local admin group. You may also use command line tools to achieve the same:

- mapadmin, for administering the service.
- nfsadmin, for managing Server for NFS and Client for NFS.
- nfsshare, for controlling NFS shared resources.
- nfsstat, for showing and resetting counts of calls made to Server for NFS.

Configure BranchCache

You may have **BranchCache** deployed in a domain-based or non-domain based environment if VPN or DirectAccess connection is available between the content servers and the branch office.

There are different BranchCache modes:

- With BranchCache in distributed cache mode, the content cache at a branch office will be distributed among client computers.
- With BranchCache in hosted cache mode, the content cache at a branch office will be hosted on one or more server computers known as hosted cache servers.
- In any case, only one mode can be used in a branch office.

BranchCache can validate contents using block hashes found in the content information. Also, to restrict cache access to the BranchCache Service the local cache is protected by file system permissions. At the end of the day, data stored in the content cache is not encrypted.

Configure File Classification Infrastructure (FCI) using File Server Resource Manager (FSRM)

With the **File Server Resource Manager (FSRM)** it is possible to configure advanced file share settings such as security, encryption and caching.

File Classification Infrastructure (FCI) is a feature that can automate the data classification processes so that you may classify files and apply policies more effectively. Keep in mind, FCI is exposed only through FSRM and no where else. Properties in FCI require two pieces of information, which are name and type. The possible types supported include:

- Yes/No
- Date
- Number
- Multiple Choice List and Ordered List
- String and Multi-String

Folder Classifier checks files within the scope of a rule. Content Classifier searches contents for certain text or patterns. You may have multiple classification rules being used together.

Configure file access auditing

There are audit policy settings under Security Settings\Advanced Audit Policy Configuration. In particular there are "Object Access" policy settings and audit events that allow you to track attempts to access specific objects or types of objects on a network or computer. Through these settings you may audit attempts to access a file, directory, registry key, or any other object (such as files and folders on a shared folder) assuming you have enabled the appropriate Object Access auditing subcategory for success and/or failure events. The resulting Detailed File Share setting will log an event every time a file or folder is accessed. Detailed File Share audit events cover detailed information on permissions and other relevant criteria used to grant or deny access.

2.2 IMPLEMENT DYNAMIC ACCESS CONTROL (DAC)

Configure user and device claim types

Dynamic Access Control (DAC) implements claims-based access controls and authentication, which rely on a trusted identity provider to authenticate the user. This identity provider issues a token to the user as proof of identity. The AD DS maintains a claims dictionary in each forest to describe how a claim may traverse a trust boundary. All claims are accordingly defined at the forest level. To use user claims, you need to have sufficient Windows Server 2012 domain controllers in place.

You use Open Group Policy Management to support user claims. Device claim is another thing - it may be sourced from the device object attribute in Active Directory that has the value of the claim.

Implement policy changes and staging

DAC allows you to implement central access policy. First you tag your data by marking the relevant folders, then configure a Central Access Rule to specify that only specific security groups may access the tagged data in a specific way, and then you apply a Central Access Policy to the corresponding Windows Server 2012 File Servers. In fact you can create central access policies for files so to centrally deploy and manage authorization policies. Note that a staging policy rule can be set up to monitor the effects of a new policy entry before actually enable it.

Perform access-denied remediation

Access-denied Remediation allows those who encountered an Access Denied error to explain why they should be allowed access. The case is sent to the Admin defined in FSRM for further review. This feature is available only if you implement SMB 3.0. In other words, it may not work with those using an earlier Windows OS.

Configure file classification

You may use the PowerShell classifier to classify a file automatically. You use Enhanced content classifier to specify the minimum and maximum occurrences of a string or regular expression. You use dynamic name space for classification rules - you do this to specify the type of information that a folder can contain and then configure classification rules based on the type of desired information.

2.3 CONFIGURE AND OPTIMIZE STORAGE

Configure iSCSI Target and Initiator

An initiator is a client which could be a software installed on the client operating system, or a hardware + software combo. A target is a host providing the LUN. The target system must support the iSCSI protocol and allow its local storage resources to be assigned to a LUN so that it can be made accessible through the iSCSI protocol. The LUN will never be in use by more than one initiator at any one time unless in the case of a cluster where each node must be able to access a LUN. Microsoft has a full blown Windows based initiator. To use this initiator the iSCSI service must first be running.

Configure Internet Storage Name server (iSNS)

Internet Storage Name Service (iSNS) is a protocol for interaction between iSNS servers and clients. The clients are initiators which attempt to discover storage device targets on the network. Port 3205 is the typical iSNS Server port. Keep in mind, the MS implementation of iSNS Server only supports the discovery of iSCSI devices but not the Fibre Channel devices.

Implement thin provisioning and trim

Thin **provisioning and trim** are features enabled by default for just-in-time allocations of storage space as well as reclaiming storage. Assuming the storage array you use complies with the certification requirements for Windows Server 2012, they would be appropriate if storage consumption is predictable, that the storage volume to use can tolerate brief outage, and that storage monitoring processes are in place to watch and detect the critical thresholds. To use them properly, you should carefully plan for and predict the corresponding capacity requirements.

Manage server free space using Features on Demand

Features on Demand is available only in Windows Server 2012 and Win8. The goal is to be able to remove role and feature files or add roles and features remotely. For this to work there should be a side-by-side feature store available that keeps the feature files.

CHAPTER 3 – IMPLEMENT BUSINESS CONTINUITY AND DISASTER RECOVERY

3.1 CONFIGURE AND MANAGE BACKUPS

Configure Windows Server backups

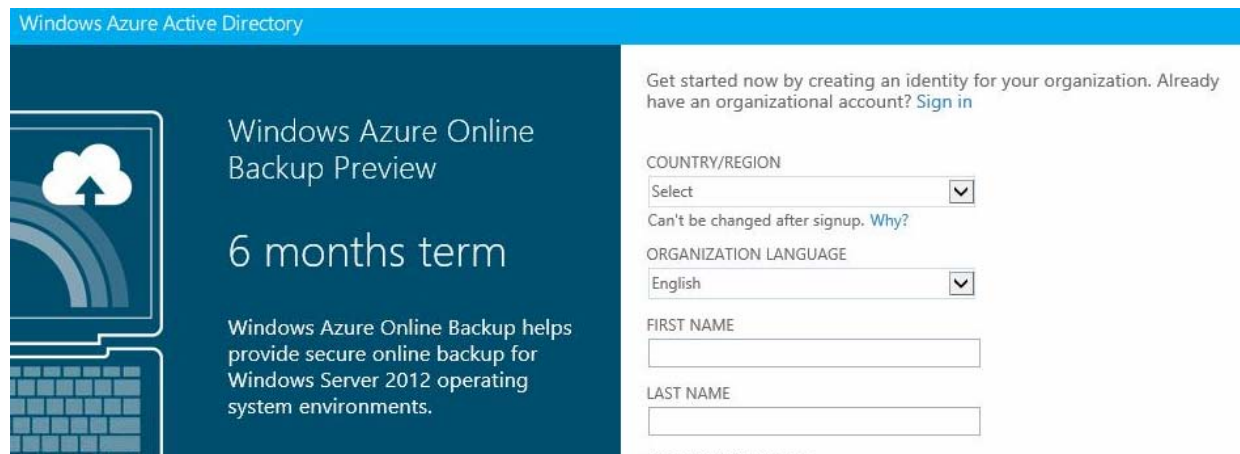
Windows Server Backup is a feature that needs to be added manually. Once added, from Server Manager you can invoke the Server Backup console and its wizard for making backups. You can use it to back up a full server (which means all volumes), selected volumes, or just the system state. In fact you can create and manage backups for the local computer or a remote computer. Do keep in mind this console is not available in a Server Core installation.



Keep in mind that the Windows Server Backup application is for restoring files and folders only. For a complete system recovery, you may want to boot up from the Windows setup disk and then choose System Image Recovery in the Advanced options screen. If your backup media has been attached properly, it should be automatically discovered.

Configure Windows Online backups

Online Backup is for storing backups in Windows Azure. For this to work, in addition to adding the Windows Server Backup feature you must sign up for the service. And you must have a fast and reliable connection for this solution to be practical.



The screenshot shows the 'Windows Azure Active Directory' sign-up page for 'Windows Azure Online Backup Preview'. The page has a blue header and a dark blue sidebar on the left with a cloud and arrow icon. The main content area is white. On the left, it says '6 months term' and 'Windows Azure Online Backup helps provide secure online backup for Windows Server 2012 operating system environments.' On the right, there's a sign-up form with the following fields: 'COUNTRY/REGION' (a dropdown menu with 'Select' and a 'v' icon), 'ORGANIZATION LANGUAGE' (a dropdown menu with 'English' and a 'v' icon), 'FIRST NAME' (a text input field), and 'LAST NAME' (a text input field). Above the form, it says 'Get started now by creating an identity for your organization. Already have an organizational account? [Sign in](#)'. Below the form, there's a partially visible 'ACCOUNT TYPE' dropdown menu.

Configure role-specific backups

Features on Demand allows you to add or remove files that are associated with specific roles and features (they are called payload files). When files are removed, they must be added back since the removal was not temporary.

To use the feature via DISM for feature removal, this command can be used:

`DISM.exe /Online /Disable-Feature /Featurename:`

To use the feature via the DISM PowerShell Cmdlet, do this:

`Disable-WindowsOptionalFeature -Online -FeatureName -Remove`

If you use the Server Manager PowerShell Cmdlet, follow this:

`Remove-WindowsFeature -Remove`

Manage VSS settings using VSSAdmin

VSS has three major components in addition to the service itself, which are writer, requester and provider. VSS creates shadow copy for the entire volume, NOT for an individual file. You use `vssadmin add shadowstorage` to add a volume shadow copy storage association. You use `vssadmin create shadow` to create a new volume shadow copy. You use `vssadmin delete shadows` to delete volume shadow copies. And you use `vssadmin delete shadowstorage` to delete volume shadow copy storage associations. You use `vssadmin list shadows` to list the existing volume shadow copies. And you use `vssadmin list shadowstorage` to list all the shadow copy storage associations on the system.

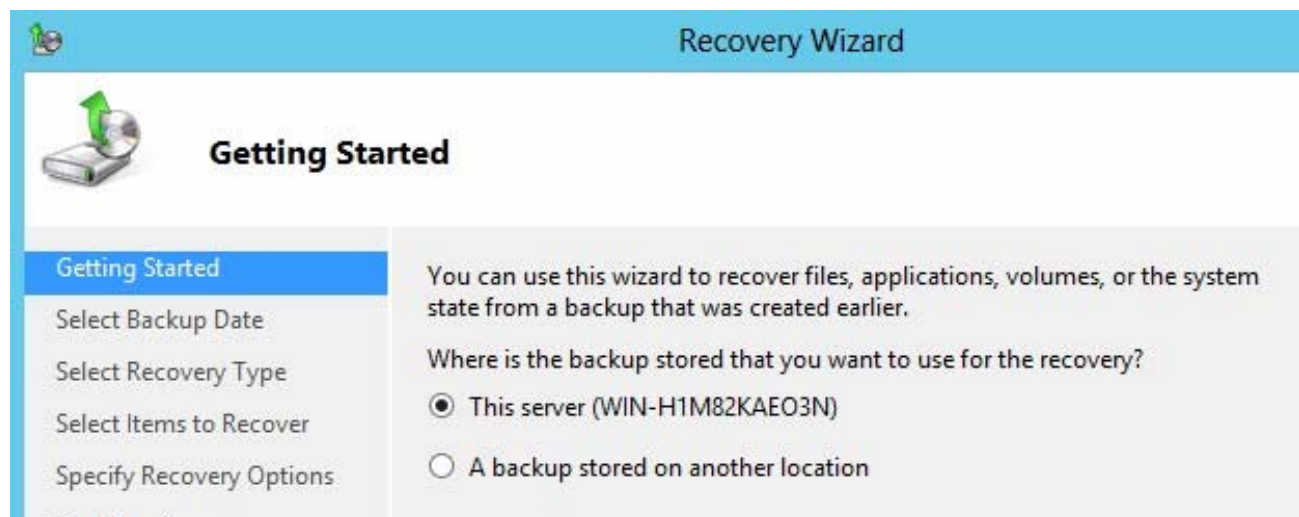
Create System Restore snapshots

VSS operates at the block level of the NTFS file system. System Restore snapshots are automatically created on a periodic basis with a Task Scheduler job or when triggered by certain events. The snapshots created allow the production of consistent backups of a volume and avoid potential file locking since they are read-only. The actual data copy process can be handled by the Windows file system.

3.2 RECOVER SERVERS

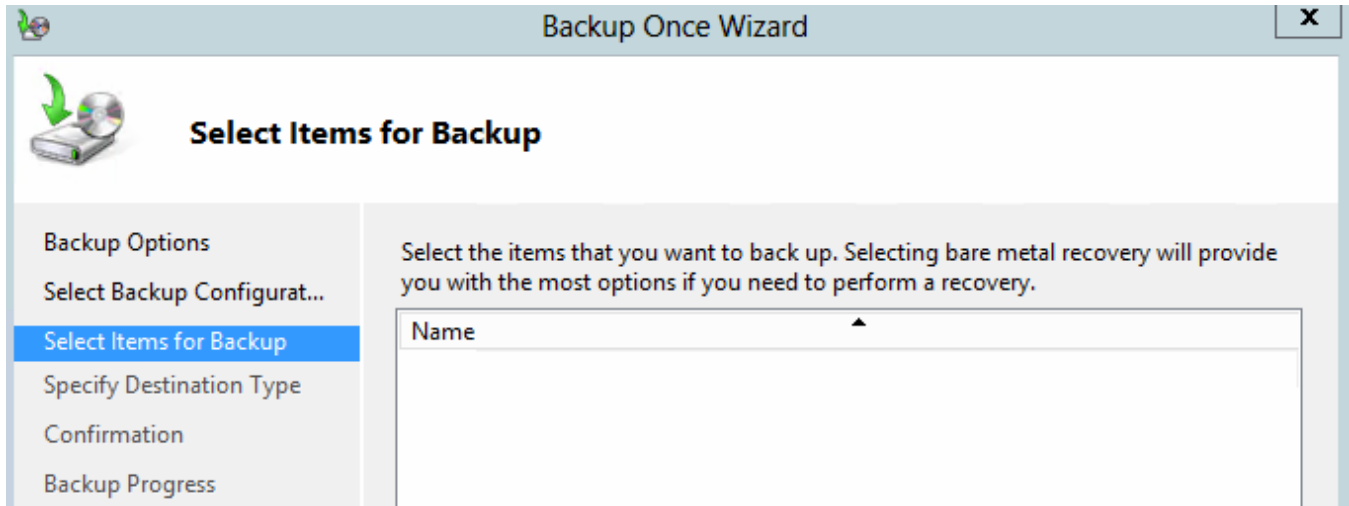
Restore from backups

You can restore from a backup using the Recovery Wizard. It can restore from backups stored locally or in a remote folder.



Perform a Bare Metal Restore (BMR)

Bare-metal restore (BMR) involves taking a physical machine that has crashed and have it brought up on another physical machine - you are actually restoring to blank disk drives. The problem with this kind of restore is that if the hardware involved is not identical you may encounter problems. Through the Windows Server Backup GUI, when you choose to Backup Once you can pick the Bare Metal Recovery option.



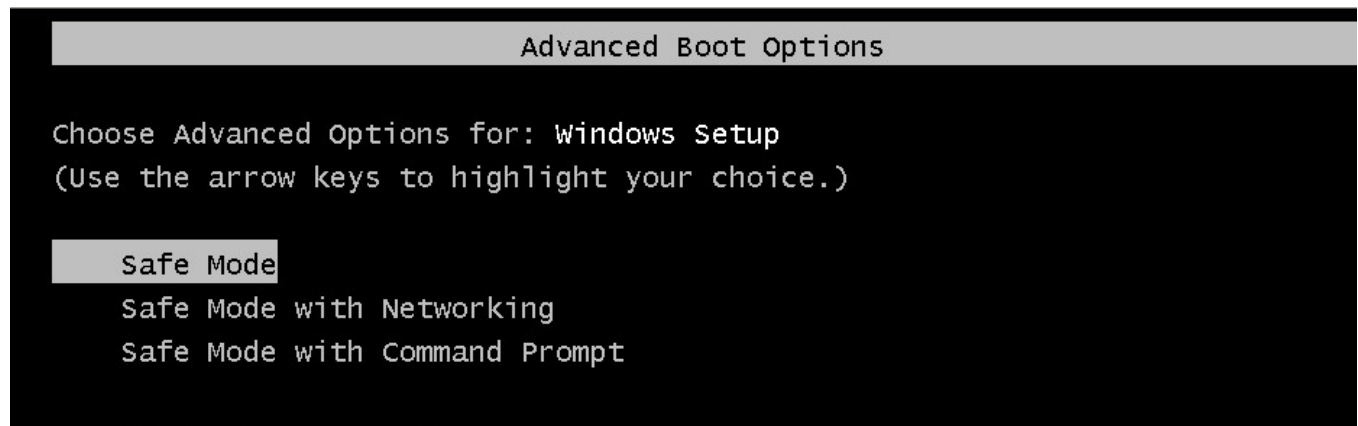
Recover servers using Windows Recovery Environment (Win RE) and safe mode

The default **Windows RE** image is known as Winre.wim. All the required Windows RE configurations are automatically set after OOBE. In order to manually enter Windows RE you need to boot using a Windows setup disc or restart the server system and choose Repair Your Computer.

Windows RE gives you the System Image Recovery option, allowing you to restore from a backup created by Windows Server Backup.



At bootup if you keep pressing F8 you can reach a menu which allows you to boot into Safe Mode, which gives you access to basic files and drivers. On the other hand, Safe Mode with Networking loads all these drivers plus the essential services and drivers to enable networking. Simply put, Safe Mode aims to help you diagnose problems.



Apply System Restore snapshots

System restore point is a system snapshot that can be configured to take place automatically. In Powershell you can enable the feature via `Enable-ComputerRestore`. To disable it you use `Disable-ComputerRestore`. To find out about the available restore points you use `Get-ComputerRestorePoint`. To add a new one you use `Checkpoint-Computer`. To go ahead with a restore you use `Restore-Computer` with the `-RestorePoint` option.

Configure the Boot Configuration Data (BCD) store

You use **BCDboot** to set up a system partition or repair the boot environment. On the other hand, you use `BCDEdit` to manage BCD stores. Boot Configuration Data Store BCD Store is firmware-independent - it is simply a namespace container for boot configuration objects and elements that hold the information required to load Windows. At the physical level it is a binary file following the registry hive format. In fact it is the Windows Deployment Services PXE Provider that creates the BCD store for an image.

3.3 CONFIGURE SITE-LEVEL FAULT TOLERANCE

Configure Hyper-V Replica including Hyper-V Replica Broker and VMs

Hyper-V Replica is a software based asynchronous replication mechanism – you use it for replicating VMs. It involves replicating VMs to other locations, through intercepting writes to VHDs. Once Replica is enabled, a source host will maintain a Hyper-V Replica Log file HRL for the VHDs. A write by the VM means a write to the VHD and also a write to the HRL. With the log file replayed to the replica VHD, replication can take place every 5 minutes. There is no need to enable Hyper-V Replica on the source host. However, you will need to enable it on all the replica hosts. The first initial copy may be made using offline media or other means. Do keep in mind all hosts involved must use the same processor type.

Very importantly, Hyper-V Replica will require the Failover Clustering role known as Hyper-V Replica Broker if either the primary or the replica Hyper-V server is part of a Windows Server cluster.

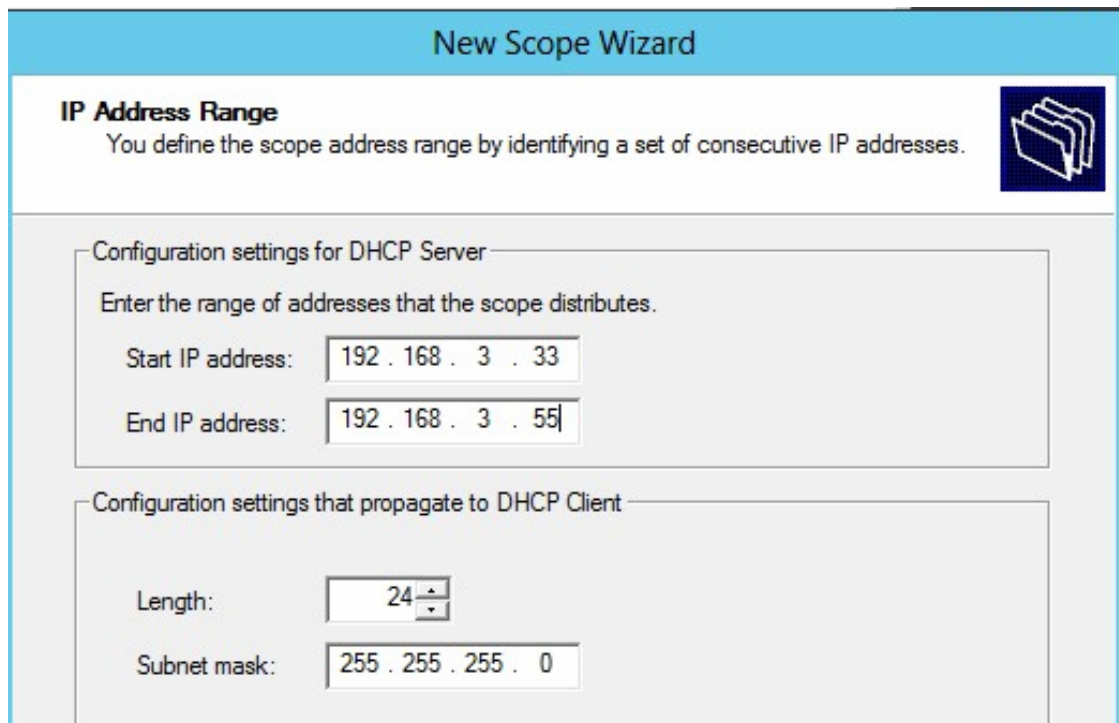
Configure multi-site clustering including network settings, Quorum, and failover settings

A **failover cluster** has multiple independent computers working together to improve availability. The clustered server nodes are connected physically via cables and can function in different roles such as file server, print server, mail server, and database server. If one fails, another is supposed to "pick up". All the participating servers in a cluster must be in the same domain. Also, they should have the same domain role (in fact the role of member server is preferred). There is also a common storage unit physically connected to all the participating servers. Normally you should use identical hardware for all the clustered servers. If you are using Serial Attached SCSI or Fibre Channel, all components of the storage stack should be identical in all servers.

CHAPTER 4 – CONFIGURE NETWORK SERVICES

4.1 IMPLEMENT AN ADVANCED DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SOLUTION

Create and configure superscopes and multicast scopes



The screenshot shows the 'New Scope Wizard' window in DHCP Manager. The title bar is blue with the text 'New Scope Wizard'. Below the title bar, there is a section titled 'IP Address Range' with a subtitle 'You define the scope address range by identifying a set of consecutive IP addresses.' and a folder icon. The main area is divided into two sections: 'Configuration settings for DHCP Server' and 'Configuration settings that propagate to DHCP Client'. The first section contains the text 'Enter the range of addresses that the scope distributes.' and two input fields: 'Start IP address:' with the value '192 . 168 . 3 . 33' and 'End IP address:' with the value '192 . 168 . 3 . 55'. The second section contains two input fields: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'.

A DHCP scope refers to an administrative grouping of IP addresses. An administrator can first create a scope for each physical subnet, then uses the scope to further define the parameters to be used by the clients. Each subnet can only have one single DHCP scope with a single continuous range of IP addresses. If you want to use multiple address ranges within a single scope then you will have to carefully configure the required exclusion ranges.

With a superscope, you are trying to provide leases from more than one scope to your clients that reside in a single physical network. To create a superscope you must use DHCP Manager to define the scopes that are to be included in the superscope (they are known as member scopes). You will find this useful if you have multiple logical IP networks in a physical network, or that you have clients that are about to be migrated to a new scope. If you have DHCP clients on the other side of a BOOTP relay agent with multiple logical subnets in a physical network, this superscope configuration will also work.

Multicast scope may be used through the Multicast Address Dynamic Client Allocation Protocol MADCAP. This protocol allows a MADCAP server to dynamically provide IP addresses to the MADCAP clients. You want your MADCAP server to also act as a multicast server MCS. This MCS is assigned an address. Your multicast clients need to register membership with the MCS in order to receive streams sent to this MCS address. Windows Server has the New Multicast Scope Wizard UI for creating a multicast scope.

Implement DHCPv6

DHCPv6 stateless mode clients may use DHCPv6 to obtain network configuration parameters separately from address configuration. IPv6 clients may configure an IPv6 address via a non-DHCPv6 based mechanism (such as IPv6 address auto-configuration and static configuration).

In contrast, DHCPv6 stateful mode allows clients to acquire both the IPv6 address and the network configuration parameters through DHCPv6 together.

Configure high availability for DHCP including DHCP failover and split scopes

Know the 80/20 rule for scopes. This means you should divide scope addresses between two DHCP servers - one with approximately 80% of the addresses and another with approximately 20% of the addresses. Employing multiple DHCP servers for fault tolerance and redundancy is called split-scope configuration. There is in fact a DHCP Split-Scope Configuration Wizard you can use for IPv4 scopes.

DHCP failover is a feature in Windows Server 2012 that can support the use of 2 DHCP servers in a failover relationship when dealing with IPv4 scopes and subnets. Failover partners can operate in either hot standby or load sharing mode. With the former there is one active primary server and one secondary server, although only one can stay active at a time. With load sharing (the default), you have two servers working simultaneously. Such a setup is most ideal when both servers are in the same physical site.

Configure DHCP Name Protection

DHCP Name protection is a feature against name squatting, which is said to take place when a non-Windows computer is registering itself in DNS with a name already registered to a Windows-based computer (server name squatted by a client/server name squatted by a server/client name squatted by a client/client name squatted by a server). The feature works using Dynamic Host Configuration Identifier DHCID in the DHCP server. For it to work the DHCID RR resource record must be supported in DNS for mapping names and preventing duplicate registration.

4.2 IMPLEMENT AN ADVANCED DNS SOLUTION

Configure security for DNS including DNSSEC, DNS Socket Pool, and cache locking

DNSSEC refers to the group of extensions for hardening the DNS infrastructure as specified in IETF RFC 4033, 4034 and 4035. It has several new types of record, including DNSKEY, RRSIG, DS, and NSEC/NSEC3. Dynamic DNS updates can be deployed for DNSSEC-signed zones with active directory, and that the scavenging stale record option can be used for purging old DNSSEC records. You can enable DNSSEC via the Zone Signing Wizard.

A **DNS server with socket pool** is capable of deploying source port randomization – this is for protecting against DNS cache poisoning attacks. It simply allows the server to randomly pick a source port when the service starts so there is no longer a predictable source port when issuing queries. The default size of this socket pool is 2500.

Cache locking means the DNS server is disallowing the cached records to be overwritten for the duration of the TTL value. This is done to protect against possible cache poisoning attacks. By default it has a value of 100%, meaning the cached entries will not be overwritten at all.

Configure DNS logging

The **DNS server log** can be viewed by the DNS Manager or the Event Viewer. From the Properties of the DNS Server, inside the Debug Logging tab there is a checkbox named Log Packets for Debugging. You may also use file-based logs as an advanced tactic. However, this should be treated as a temporary measure only. Keep in mind, the more you log, the more overheads are to be involved.

Configure delegated administration

You may use the New Delegation Wizard to add a new delegated domain. Zone delegation works like "dividing" your DNS namespace. You want to do this if you find the need to distribute traffic loads among multiple servers and improve DNS name resolution performance/resiliency, or that you prefer to extend the namespace to accommodate the opening of a new remote branch.

Configure recursion

You may have your DNS server designated as a forwarder when the other DNS servers are configured to forward the queries that can't be resolved locally. You can use the DNS Manager or the dnscmd command with the /ResetForwarders option to configure such feature.

The screenshot shows the 'New Conditional Forwarder' dialog box. It has a title bar with a close button (X). The main area contains the following fields and controls:

- DNS Domain:** A text input field.
- IP addresses of the master servers:** A table with three columns: 'IP Address', 'Server FQDN', and 'Validated'. The first row contains the text '<Click here to add a...'. To the right of the table are three buttons: 'Delete', 'Up', and 'Down'.
- ☐ **Store this conditional forwarder in Active Directory, and replicate it as follows:** A checkbox followed by a dropdown menu currently showing 'All DNS servers in this forest'.
- Number of seconds before forward queries time out:** A text input field containing the value '5'.
- A note at the bottom: 'The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.'

You can specify that the DNS server only uses forwarders and make no further recursion even if the forwarders fail. If you disable recursion for the DNS server, it will never perform recursion on any query.

Configure netmask ordering

Netmask ordering is a feature you can use to return addresses for type A DNS queries. You do this to prioritize local resources to your DNS clients (you want your clients to receive query results that are most relevant to their location). You will find this feature particularly useful if you have many type A records for the same DNS name, that each of these type A records has a different address. You may use `Dnscmd /Config /LocalNetPriorityNetMask` to achieve this.

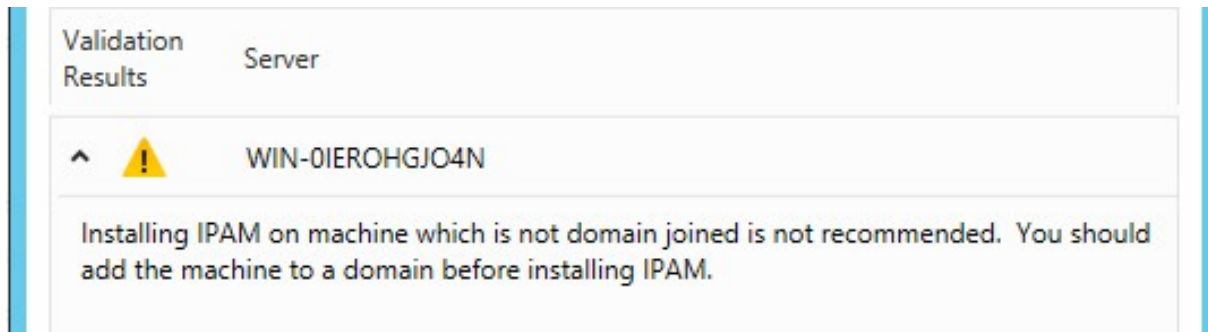
Configure a GlobalNames zone

A special zone named **GlobalNames (GNZ)** can be used to provide resolution of single-label names. GlobalNames zone can be created via the DNS Manager UI or the `dnscmd` command. Do note that GNZ is for aiding the retirement of WINS only. Also note that single-label name resolution of records is NOT supposed to use dynamic registration.

4.3 DEPLOY AND MANAGE IPAM

Configure IPAM manually or by using Group Policy

You may have an **IPAM** server deployed at every site. If your network is reasonably small, you may want to have one IPAM server deployed for the entire network. You should install IPAM on a server that has joined a domain, or you will receive a warning.



FYI, an IPAM server should be set up as a single-purpose server. Do not collocate other network infrastructure roles on the same server! Each IPAM server can support max 150 DHCP servers and 500 DNS servers. External databases and non-MS implementations are not supported.

Provisioning is the process that you must go through for the infrastructure servers to be managed. You choose a provisioning method through the IPAM console overview (this is how you launch the Provision IPAM wizard). The manual provisioning method is usually not preferred due to concern on complexity. The Group Policy based method is less prone to errors since GPOs are automatically applied to the infrastructure servers once they are assigned a status of managed via the IPAM console.

Configure server discovery

Server discovery involves defining the scope of discovery prior to actually discovering the servers. IPAM uses AD to define the scope of servers that are to be managed. To begin discovering servers you first set a scope by invoking Configure server discovery from within the IPAM client console. You need to choose a domain to discover (this is the scope). To actually discover server roles, you click Start server discovery to call up the IPAM ServerDiscovery task.

Create and manage IP blocks and ranges

You need to know the basic concepts here. **IP address blocks** refer to the large chunks of IP addresses for organizing address space at a higher level. IP address ranges are smaller chunks of addresses that correspond to DHCP scopes. Individual IP addresses are the smallest units - they map to a single IP address range. The goal of all these is to allow a more structural way of managing the overall address space and visualization.

IP addresses detailed tracking and utilization data is available, that IPv4 and IPv6 address spaces are organized into IP address blocks, IP address ranges, and individual IP addresses. You may further organize IP address space into hierarchical, logical groups.

Monitor utilization of IP address space

A single IPAM server can support max 6000 DHCP scopes and 150 DNS zones. Do remember, IP address utilization trends are IPv4 only. In fact, IPAM can automatically collect the dynamic address scopes together with their utilization statistics from the DHCP servers being managed. Through IPAM you can even create, duplicate, edit, or delete DHCP scopes directly without going through the DHCP console.

Migrate to IPAM

To be managed and monitored by IPAM, the security settings and firewall ports on a Windows server must be configured to allow the IPAM server to access it. This can be done manually or via GPOs.

Delegate IPAM administration

The IPAM setup creates several local security groups to isolate and restrict the relevant permissions. IPAM Users can view information in server discovery, address space configuration, and server management. They can also view IPAM and DHCP server operational events but not the address tracking information. IPAM MSM Administrators can also perform common management tasks and server management tasks. IPAM ASM Administrators can additionally perform IP address space tasks. IPAM IP Audit Administrators can in particular view and track the important IP address tracking information. IPAM Administrators can do everything IPAM.

Manage IPAM collections

IPAM has a number of scheduled data collection tasks. They are self explanatory:

- AddressExpiry
- AddressUtilization
- Audit
- ServerAvailability
- ServerConfiguration
- ServerDiscovery
- ServiceMonitoring

Keep in mind, the information kept in the IPAM database is regularly updated with inputs from these data collection tasks, although the database can be manually modified by you the administrator.

CHAPTER 5 – CONFIGURE THE ACTIVE DIRECTORY INFRASTRUCTURE

5.1 CONFIGURE A FOREST OR A DOMAIN

Implement multi-domain and multi-forest Active Directory environments including interoperability with previous versions of Active Directory

When the first Windows Server 2012–based Domain Controller is introduced, the forest will operate by default at the lowest functional level that is possible, which is Windows 2003, so that you may take advantage of the default Active Directory features while accommodating older versions of Windows Server.

Windows Server 2012 requires at the least a Windows Server 2003 forest functional level. Before you can add domain controllers that run Windows Server 2012 to the forest, the existing forest functional level must be at least Windows Server 2003.

Upgrade existing domains and forests including environment preparation and functional levels

You need to install the Active Directory Domain Services (AD-DS) role on a server so to allow it to act as a Domain Controller. After this you need to promote the server to a domain controller. You do NOT use the `dcpromo` command anymore.

When you raise the forest functional level, newer advanced features can become available at the expense of compatibility. After you raise the domain functional level, domain controllers running earlier operating systems will not be able to participate in the domain anymore. Keep in mind, rollback or lowering of level is highly difficult! Also, you cannot set the domain functional level to a value lower than the forest functional level.

Configure multiple user principal name (UPN) suffixes

You can use the AD Domains and Trusts UI to add new **user principal name (UPN)** suffixes. By default the UPN suffix for a user account is the DNS domain name that keeps the user account. It is possible to add other UPN suffixes for simplifying administration and user logons (technically you can provide one single UPN suffix for all users). Do remember, an UPN suffix is only useful in AD - it is not meant to be part of any formal DNS domain name.

5.2 CONFIGURE TRUSTS

Configure external, forest, shortcut, and realm trusts

The tools that you can use to create and manage trusts are **Active Directory Domains and Trusts** (i.e. Domain.msc) and Netdom.exe. Nltest is for testing your secured channels. Netdiag is for testing the network health. Dcdiag is for testing the domain controller health.

Communication between different domains has to take place through trusts, which are authentication pipelines. The necessary default trusts are created when you use the Active Directory Installation Wizard. You may also use the Netdom command line tool to create new trusts by hand.

You want to create external trusts for providing access to resources located on a Windows NT 4.0 domain. You also want to make use of forest trusts to share resources between forests. Shortcut trusts are for improving user logon times between two different domains.

A realm trust is for establishing communication between non-Windows Kerberos V5 realm and Windows based domain. Simply put, it provides cross-platform interoperability with security services running other Kerberos V5 versions.

Configure trust authentication

Kerberos is the default in Windows so there are no prerequisites at all for implementing Kerberos based authentication. You can set the various Kerberos security policy parameters via the Group Policy snap-in. Keep in mind, with Kerberos authentication transparent transitive trust is used among the domains inside a forest. It does not authenticate between domains in different forests though. In order to use a resource in another forest, the user has to provide credentials for formally logging on to a domain in that particular forest.

The integrity of communications that take place along interforest trusts can be protected via SID filtering and selective authentication. The former can be used to stop a malicious user with admin credentials in a trusted forest from taking control over the trusting forest. The latter can restrict the quantity of authentication requests allowed to pass through an interforest trust.

Configure SID filtering

SID filtering may be set on all trusts. You want to know that SID history allows for legitimate uses, just that there is a security threat when being used to exploit an unprotected trust - a malicious user who has admin credentials may manipulate the SID history attribute of a security principal in the trusted forest to gain full access to the trusting forest! SID filtering works by verifying the incoming authentication request made by a security principal in the trusted domain to make sure it contains only the SID of the security principal originated from the trusted domain.

A SID filter quarantine is even stricter - when being applied to a trusted domain only those SIDs from the trusted domain can traverse the trust relationship.

Configure name suffix routing

Name suffix routing is for managing the way authentication requests are routed across forests joined by forest trusts. Whenever a forest trust is created, by default all the unique name suffixes are routed. A unique name suffix is not subordinate to any other name suffix. All names that subordinate a unique name suffix are implicitly routed. If you have a need to selectively exclude members of a child domain from authenticating in a pre-specified forest, you may consider to disable name suffix routing for the corresponding name. You may even disable routing entirely for the forest name itself!

5.3 CONFIGURE SITES

Configure sites and subnets

A **site topology** serves as a logical representation of the physical network. Designing a site topology involves planning for domain controller placement as well as designing site links and site link bridges to ensure efficient routing of query and traffics for replication. You will also need to plan the creation of subnet objects for representing all IP addresses within a site.

Subnet objects can be created in AD via the AD Site and Services UI. These objects serve as the logical representation of your physical subnets. You may pick a site object for the subnet object you create - in other words, a site is actually defined by the subnet applied to it. Note that all subnet names in AD take the form of network/bits masked.

It makes sense for each physical location to be represented by a site. For every location with a site you need to plan to create site objects and associate subnets with these sites. You should also plan to create subnet objects that represent all IP addresses within the site. In the case that you have several networks connected with fast and reliable WAN links then you may include all of the subnets in one single site.

Create and configure site links

To connect your sites you need to use site links. You should first identify the sites that you want to connect with the site link, then create a site link object in the respective Inter-Site Transports container, and then give the site link a name before setting the site link properties. Each link object is for representing an actual WAN link, and you may assign cost values to different site links to favor certain connections over the others.

When measuring logon performance requirements over the WAN link, you should consider factors such as link speed and available bandwidth, number of users and patterns of use, and the estimated amount of network traffic. Having too many domain controllers in a location may push up support costs and produce excessive replication traffic.

Manage site coverage

Talking about **Automatic Site Coverage**, by default each domain controller will perform a check on all sites in the forest and then examine the replication cost matrix. A domain controller will try to advertise itself in sites that do not have a domain controller in there, such that every site can have a domain controller defined by default. Therefore, in theory domain controllers published in DNS are those that come from the closest site (as judged by examining the replication topology). Automatic site coverage can calculate and determine the way in which a site covers another that has no domain controller in it. Do remember, site coverage is ALWAYS determined by site-link costs (domain controllers will accordingly register themselves in sites).

Manage registration of SRV records

Windows based domain controllers always register DNS records that indicate the site they belong to. Whenever DNS is used, a Locator will first search for a site-specific DNS record before looking for non site-specific records. IP/DNS-compatible Locator is used when the domain name is DNS compatible. Windows NT 4.0-compatible Locator is used if the domain name is a NetBIOS name.

A computer client may or may not be located physically in the site associated with its address. A domain controller will need to use site information to check the IP address of the client computer against a list of subnets of the same forest. Because the relevant Configuration container is replicated to all domain controllers, any domain controller in the same forest can identify the site where a client resides.

You need to know that during the registration of SRV records in DNS, it is the Site Coverage Algorithm that is being used to determine which domain controllers can register site SRV records that designate them as the preferred domain controllers for sites that are not represented by any specific domain controller.

Move domain controllers between sites

Domain controller placement is important as it relies on site information to inform clients about the domain controllers that present within the closest site as the clients. Generally you should place forest root domain controllers primarily in hub locations or at locations that host use-intensive datacenters. You should also consider placing regional domain controllers for each domain represented in each hub location.

5.4 MANAGE ACTIVE DIRECTORY AND SYSVOL REPLICATION

Configure replication to Read-Only Domain Controllers (RODCs)

A **RODC Read Only DC** is simply an additional domain controller that hosts read-only partitions of the Active Directory database. It is primarily for use in branch office with poor WAN link. Since it can keep cached credentials, faster login can be made possible.

Note that a RODC can only replicate from a writable Windows Server domain controller. You may trigger replication to a RODC via `repadmin /replicate` or `repadmin /syncall`. Management of a RODC can be performed remotely via the Remote Server Administration Tools RSAT or the Windows Remote Shell WinRS.

Configure Password Replication Policy (PRP) for RODCs

You may configure **Password Replication Policy (PRP)** via the AD Users and Computers MMC snap-in or the `repadmin` command. You may also view the cached passwords on a RODC via these tools. Keep in mind, RODCs of the same domain in the same site cannot share cached credentials.

Monitor and manage replication

When you have multiple sites configured, intersite replication will progress via `DEFAULTIPSITELINK`, which uses a mesh topology that is reliable but relatively bandwidth demanding. You may control site link availability through setting a schedule for site links. Do remember, the time settings in the site link schedules would conform only to the local time of the site. You need to also set the site link replication interval property to indicate how frequently you want replication to take place during the times when the schedule allows replication. A small interval can reduce latency at the expense of WAN traffics. Generally, low latency is preferred unless your WAN link is slow.

Upgrade SYSVOL replication to Distributed File System Replication (DFSR)

SYSVOL replication relies on the File Replication Service (FRS) or the **Distributed File System Replication (DFSR)** to replicate changes, and they both replicate according to the schedule created during site topology design.

The DFSR service is a new and more efficient multi-master replication engine which works using RPC for replicating a folder scope defined by the replicated folder path. It caches configuration information stored in XML files. The possible configuration modes are WMI-based and Active Directory-based. It is said that DFSR is more secure due to the use of Active Directory security and WMI security.

CHAPTER 6 – CONFIGURE IDENTITY AND ACCESS SOLUTIONS

6.1 IMPLEMENT ACTIVE DIRECTORY FEDERATION SERVICES 2.1 (AD FSV2.1)

Implement claims-based authentication including Relying Party Trusts

Active **Directory Federation Services (ADFS)** is the role that provides Web based single-sign-on mechanism for authenticating user to multiple Web applications within a single session. Its Web Agent is a role service that creates an AD FS-enabled Web server. An AD FS-enabled Web server can authenticate and authorize federated access to locally hosted Web applications.

A federation server authenticates and routes requests from user accounts outside of the internal network. A federation server proxy provides intermediary proxy services between an Internet client and a federation server behind the firewall. A federation partner is trusted by the Federation Service to provide security tokens to its users. A resource partner is a federation partner that trusts the Federation Service to issue claims-based security tokens. A resource federation server refers to the federation server that resides in the resource partner organization.

You may setup federation trust relationships between two partner organizations. Do realize that federation trusts do not involve any direct communication over the network between the account Federation Service and the resource Federation Service.

Configure Claims Provider Trust rules

Claims are statements used primarily for authorizing access to claims-based applications while a claim type is for providing context for the claim value. A claim rule is for representing an instance of business logic that will take incoming claims, apply conditions to these claims and accordingly produce outgoing claims. Through the AD FS you define the claims that are to be exchanged between federated partners.

You may add a new claims provider trust via the AD FS Management snap-in. With this wizard there are options to use the WS-Federation Passive protocol and the SAML 2.0 WebSSO protocol. Alternatively you may use the AD FS Management snap-in to automatically import configuration data from the federation metadata that your partner has published.

Configure attribute stores including Active Directory Lightweight Directory Services (AD LDS)

An organization may host an AD FS-secured application in a perimeter network that maintains a separate store of customer accounts in the perimeter network. This arrangement allows you to more easily isolate customer accounts and employee accounts. You can accordingly manage the local accounts for customers in the perimeter network via the AD DS or the AD Lightweight Directory Services as the account store. Note that AD LDS is LDAP based - it offers flexible support for directory-enabled applications. You can run it on member servers or even standalone server computers. AD LDS has its own server role. However, it can run concurrently with AD DS in the same network.

Manage AD FS certificates

A federation server must possess at least a server authentication certificate and a token-signing certificate before it is allowed to take part in AD FS communications. The trust policy will also require a verification certificate which is in fact the public key portion of the token-signing certificate.

The server authentication certificate is SSL based - you use it to secure web services traffic with your clients and proxy. It may be installed via the IIS snap-in. The token-signing certificate is for signing all the security tokens it produces. The verification certificate is for verifying that a security token was in fact issued by a valid federation server. It is in fact the token-signing certificate of another federation server. On the other hand, a server that runs the Federation Service Proxy role service needs to have a SSL client authentication certificate and also a server authentication certificate.

Configure AD FS proxy

An account federation server is the server located in the corporate network of your partner organization. It is the server that issues security tokens to users. On the other hand, an account federation server proxy is located in the perimeter network of the partner organization. It can collect authentication credentials from web browser clients that log on over the Internet.

Using a federation server proxy can provide additional security layers to your AD FS deployment since it isolates AD FS from the outside world. When you place a federation server proxy in the perimeter network of the account partner, it collects user credential information. If you place it in the perimeter network of your resource partner, it relays security token requests to the resource federation server and accordingly produces the necessary organizational security tokens. You may create it via the AD FS Federation Server Proxy Configuration Wizard GUI or Fsconfig.exe.

Integrate with cloud services

You want to know that AD FS 2.0 supports Security Assertion Markup Language SAML 2.0, which is essential in providing interoperability with cloud services. It is also known that you may use Dirsync and ADFS to synchronize your local AD users with the cloud based Office365 and then configure ADFS to implement single signon accordingly.

6.2 INSTALL AND CONFIGURE ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS)

Install an Enterprise Certificate Authority (CA)

A **Certificate Authority (CA)** generates and validates digital certificates. It typically adds its own signature to the public key of the client so to indicate that the public key is valid if you trust this CA. From Server Manager you need to use the Add Roles Wizard to add Active Directory Certificate Services by hand.

You need to determine the type of CA you prefer. A stand-alone CA does not require the use of AD. If you choose to use an Enterprise CA, it means the CA is AD integrated so all the manual tasks become automatic UNLESS you are serving people who do not belong to AD.

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☐ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☒ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

Enterprise CAs can only issue certificates to members of the AD forest. Certificate templates that define the format and content of the certificates can only be used with enterprise CAs.

Configure CRL distribution points

When the outstanding certificates issued by this CA are revoked, a **Certificate Revocation List (CRL)** should be published to reflect the change. You use the Certification Authority MMC snap-in to add or change CRL distribution points, which are paths represented as attributes on a certificate issued. You can also fine tune the relationship between a full CRL and delta CRL (which holds a list of all the revoked certificates since the last time a full CRL was made) through specifying an overlap period between them. This overlap period specifies the amount of time at the end of a CRL's lifetime that a certificate client may still use for obtaining a new CRL before the old one stops working.

Install and configure Online Responder

Online Responder service may be used to implement **Online Certificate Status Protocol (OCSP)**. This service works by decoding revocation status requests for specific certificates and performing evaluation accordingly. In fact you may use it as an alternative to or an extension of CRLs for providing certificate revocation data to your clients.

Keep in mind, for an OCSP to function correctly there must be a valid Response Signing certificate (even if you are not using a Microsoft OCSP responder). In addition to configuring the certificate templates and issuance properties for the OCSP Response Signing certificates (which may be done via the Certificate Templates snap-in), the location of the OCSP responder must be added to the authority information access extension on the CA. And you must enable the OCSP Response Signing certificate template for this CA.

Implement administrative role separation

Administrator Role Separation (ARS) can be configured to a user who is not a domain admin. The goal is to allow some local admin tasks to be delegated.

Configure CA backup and recovery

You should regularly back up the certification authority database, the CA certificate, and the CA keys on a regular basis given consideration on the number of certificates issued. The more certificates you issue the more frequently the CA should be backed up. When you login as a CA administrator or a member of the Backup Operators group you can back up a CA via the Certification Authority snap-in. From its Action menu there is a task known as Back Up CA. On the other hand, there is an action known as Restore CA for calling up the Certification Authority Restore Wizard.

6.3 MANAGE CERTIFICATES

Manage certificate templates

Certificate templates have different versions. Since Windows Server 2008 there are new version 3 certificate templates updated to support new features, encryption and hash algorithms. There are template properties options in the Certificate Templates MMC snap-in. Kerberos Authentication template serves a different purpose - to issue certificates to domain controllers which in turn present the certificates to client computers during authentication. To create a new template, the best thing to do is to duplicate an existing template and use its properties as the default for yours.

Implement and manage certificate deployment, validation, and revocation

Keep in mind, if you are using an Enterprise CA, your certificate templates will be stored in AD.

As previously said, certificate templates have different versions. If you upgrade a CA, you may also need to update the AD schema for supporting the new certificate template attributes. You may as well upgrade the certificate templates to include the new attributes. You may do so before or after upgrading your CAs to Windows Server 2012.

When configuring new templates there is an option known as Do not store certificates and requests in the CA database. With it, your CA will process certificate requests without adding records to the CA database (so to save workload and space). On the other hand, the Do not include revocation information in issued certificates option can be used to exclude revocation information from the issued certificates (so to cut down validation time).

The Enterprise PKI MC snap-in is a monitoring tool. You need to manually add it (under Active Directory Certificate Services). With it you can view the CA status information. The status may be OK, Warning, Error, or Unable to download.

You may use certificate trust policy to make the necessary certificate path validation settings (so to facilitate automatic certificate management). With these settings you may manage:

- Trusted Root Certificates.
- Trusted Publishers.
- Network Retrieval and Path Validation.
- Revocation Checking Policy.

Manage certificate renewal

When configuring enrollment, you should not assign permissions to domain local groups since assigning permissions to local groups may lead to result in inconsistency in the application of permissions. If you want to use autoenrollment (which may be configured to work in background task that require no user input at all), the user or computer must belong to domain groups with Read, Enroll, and Autoenroll permissions. To enable enrollment via the Certificates snap-in, Web-based enrollment or automatic renewal, make sure the Read and Enroll permissions are properly assigned. For certificate renewal in particular, the Read and Enroll permissions must be present.

Manage certificate enrollment and renewal to computers and users using Group Policies

As previously said, proper permissions are necessary for renewal and enrollment. You may use group policies to assign these permissions as needed.

Configure and manage key archival and recovery

Enterprise CAs have a key recovery agent certificate template with default configuration that grants permissions to the Domain Admins/Enterprise Admins so they may enroll for key recovery agent certificates. You may also add a key recovery agent certificate template via the Certification Authority MMC snap-in. This UI can also be used to configure key recovery. Remember, key recovery may be performed on a CA only for those certificates issued by that same CA. If there are multiple issuing CAs you will need to configure each CA one by one.

A typical key recovery process involves a number of steps. First you need to identify the archived keys for recovery via Certutil.exe - getkey. Then you need to retrieve the archived keys from the CA database (you may do so through using the certificate's serial number). Then you need to decrypt the archived keys via both Certutil.exe - recoverkey and the key recovery agent certificate (you need to have Certificate Management privileges). Once decrypted, store it in a password protected file and have it transferred to the user who needs it. The user needs to import the certificate and the corresponding recovered keys via Certutil.exe - importPFX into his personal certificate store in order to use it.

You must understand that key recovery agent keys are high value data assets that must be protected against compromise and loss. A private key must be made available for use prior to archival for as long as the data encrypted with that key is still needed. Auditing of the key recovery events should also be considered (which can also be done via the Certification Authority snap-in).

6.4 INSTALL AND CONFIGURE ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES (AD RMS)

Install a licensing or certificate AD RMS server

Active Directory Rights Management Services (AD RMS) is for safeguarding digital information and preventing unauthorized use. You should install AD RMS as a server role via Server Manager. The first RMS server is the root cluster in the case of load-balancing. You should be a member of the Enterprise Admins group to perform the necessary cluster configuration tasks.

Manage AD RMS Service Connection Point (SCP)

The AD RMS **Service Connection Point (SCP)** is an AD object. This object holds the web address of your AD RMS certification cluster. All AD RMS-enabled applications will rely on this SCP for discovering the AD RMS service. In other words, it serves as the first connection point for discovering the AD RMS web services. You can have only one single SCP in AD. To add a new SCP the existing one must first be removed.

Manage AD RMS client deployment

There is an AD RMS client included in the default installation of Vista, Windows Server 2008 and later versions. To properly consume rights-protected content the client must add the AD RMS URL to the Local Intranet security zone of the browser.

You may use the Rights Protected Folder Explorer to work with Rights Protected Folders. You can use it to securely store or send files to authorized users. Also, with it you can control which users will be able to access those files.

Manage Trusted User Domains

You need to know that in the world of AD RMS every single entity is represented by a certificate. The AD RMS server cluster is represented by a Server Licenser Certificate SLC. Client computers have a Security Processor Certificate SPC. Users are identified by a Rights Account Certificate RAC when being authenticated by the RMS server. By default, AD RMS will not process requests from those with RACs issued by another AD RMS cluster UNLESS you add those AD RMS domains to a list of trusted user domains.

Manage Trusted Publishing Domains

The RAC is always used by the server for encrypting licenses being sent to the user. There is also a certificate known as **Client Licenser Certificate (CLC)**, which is obtained during client activation. **Publishing Licenses (PL)** are certificates that express rights over a document. You can have a PL stamped into a protected document and encrypted with the SLC's public key, plus getting signed with the user's CLC. Similarly, you may add trust policies (trusted publishing domain TPD) so that AD RMS can handle licensing requests for contents rights-protected by another AD RMS cluster.

Manage Federated Identity support

Technically speaking, rights can be assigned to users who have a federated trust with AD FS. This allows you to share access to those rights-protected contents with another organization without setting up a separate Active Directory trust. Federated identity support is a feature you can use to allow users to make use of credentials established by a federated trust relationship through AD FS for obtaining a RAC. Do note that when RACs are issued through a federated identity, the standard rights account certificate validity period will be based on those specified in the Federated Identity Support setting.

Manage RMS templates

Rights policy templates in AD RMS are for controlling the rights that a user or group has on a particular rights-protected content item. By default, AD RMS stores rights policy templates in the configuration database and also keeps a copy of all rights policy templates in a shared folder. There is a rights policy template creation wizard you can use for template creation. There is also a rights policy template distribution pipeline that can guide you through the template distribution process.

Configure Exclusion Policies

You may use **exclusion policies** to disallow certain entities to acquire certificate and make license requests. This can be done on the basis of user, application, and lockbox version. Use licenses that are created for that entity by servers of the AD RMS cluster will keep a record in the exclusion list. To enable exclusion, from within the AD RMS console you need to find and turn on the Exclusion Policies - Enable Application Exclusion option. To setup exclusion, you may use the Exclude User Account wizard or the Exclude Application wizard. To setup lockbox exclusion you will need to turn on the Enable Lockbox Exclusion option separately.