Study Guide

Microsoft 70-411

Administering Windows Server 2012

ExamForce

ABOUT THE EXAM

The Microsoft 70-411 exam is part two 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 administer the tasks required to maintain a Windows Server 2012 infrastructure, such as user and group management, network access, and data security. 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 70-411 Certification. The topics are as follows:

- Deploy, Manage, and Maintain Servers
- Configure File and Print Services
- Configure Network Services and Access
- Configure a Network Policy Server Infrastructure
- Configure and Manage Active Directory
- Configure and Manage Group Policy

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

OBJECTIVES

CHAPTER 1: DEPLOY, MANAGE, AND MAINTAIN SERVERS

1.1 Deploy and manage server images
1.2 Implement patch management
1.3 Monitor servers

CHAPTER 2: CONFIGURE FILE AND PRINT SERVICES

2.1 Configure Distributed File System (DFS)
2.2 Configure File Server Resource Manager (FSRM)
2.3 Configure file and disk encryption
2.4 Configure advanced audit policies

CHAPTER 3: CONFIGURE NETWORK SERVICES AND ACCESS

3.1 Configure DNS zones
3.2 Configure DNS records
3.3 Configure VPN and routing
3.4 Configure DirectAccess

CHAPTER 4: CONFIGURE A NETWORK POLICY SERVER INFRASTRUCTURE

4.1 Configure Network Policy Server (NPS)
4.2 Configure NPS policies
4.3 Configure Network Access Protection (NAP)

CHAPTER 5: CONFIGURE AND MANAGE ACTIVE DIRECTORY

5.1 Configure service authentication
5.2 Configure Domain Controllers
5.3 Maintain Active Directory
5.4 Configure account policies

CHAPTER 6: CONFIGURE AND MANAGE GROUP POLICY

6.1 Configure Group Policy processing
6.2 Configure Group Policy settings
6.3 Manage Group Policy objects (GPOs)
6.4 Configure Group Policy preferences

CHAPTER 1 – DEPLOY, MANAGE, AND MAINTAIN SERVERS

1.1 DEPLOY AND MANAGE SERVER IMAGES

Install the Windows Deployment Services (WDS) role

Windows Deployment Services (WDS) is used to facilitate OS deployment. The WDS role is the updated and redesigned version of **Remote Installation Services (RIS)**. Through it you may deploy Windows operating systems over a network.

To use WDS an existing server must configured as the **Deployment Server** and the **Transport Server**. They must members of or join a domain that has DHCP and DNS running and properly configured.

Configure and manage boot, install, and discover images

At least one boot image and one install image must be created and made available in order to boot to the WDS server and subsequently install from an image. Note that the client computer must be capable of performing a **PXE boot** and meet the minimum hardware requirements for the operating system of the install image. The client must have a minimum of 512 MB of **RAM**.

Update images with patches, hotfixes, and drivers

OCSetup is a command-line tool used for applying updates to an online Windows image. This allows installation of ***.msi*** files via **MSIExec.exe**. It can also install and remove **Component-Based Servicing (CBS)** packages online by passing them to **DISM**.

In order to install the system MSI packages via OCSetup, they must first be staged. Additionally, the paths to the packages must be specified in an **answer file**. Staging an installer file involves placing it in the location specified in the **CustomSetup** registry key.

If the installation package requires a custom installer, it must first be registered. This is accomplished by adding the name of the package to the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\OC Setup\Components**

Install features for offline images

Oscdimg is used to create an image in the ***.iso*** format for customized **Windows PE**. You use **Expand.exe** to decompress the update files. **Intlcfg.exe** is used to change the language & locale, fonts, input settings, etc., for a given installation.

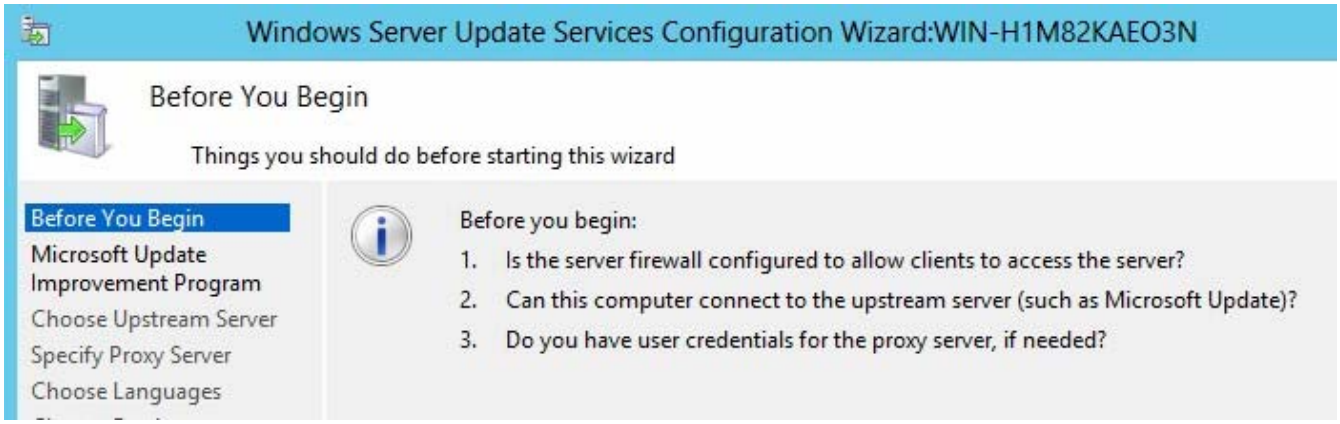
Through the **Deployment Image Servicing and Management (DISM)** tool you can build and deploy offline Windows images. It is a scriptable command-line utility used to mount/unmount system images as well as update operating system components.

For DISM to work properly, the Windows image must be local. If the answer file for an image is named **unattend.xml**, only the settings specified in the **offlineServicing configuration pass** can be applied.

1.2 IMPLEMENT PATCH MANAGEMENT

Install and configure the Windows Server Update Services (WSUS) role

Windows Server Update Services (WSUS) is a server role configured via the **WSUS Configuration Wizard**.



For proper operation, ensure the server's firewall allows client access to the server so that updates can be retrieved. The server itself must be able to connect to the **Upstream Server** if is designated to download updates from elsewhere. If there is a proxy server, its name and user credentials must be known and provided when prompted.

Configure group policies for updates

The **WSUS Setup** program can configure **IIS** to automatically distribute the latest version of **Automatic Updates** to clients that contact WSUS. This can also be done via domain based GPO to configure updates. Without **AD DS** only the **Local Group Policy Editor** can be used to configure Automatic Updates.

Note that the **Default Domain** or **Default Domain Controller** GPOs should not be altered for configuring WSUS settings. Also, prior to setting any Group Policy options for WSUS, the latest administrative template should be applied to the computer used to manage Group Policy. The administrative template that contains the relevant WSUS settings is called **Wuau.adm**. The following Automatic Updates options can be made available to the clients:

- Notify for download and notify for install.
- Auto download and notify for install.
- Auto download and schedule the install.
- Allow local admin to choose setting.

Configure client-side targeting

When computers are assigned to computer groups you have two options to choose from: **server-side targeting** and **client-side targeting**. The former involves adding each computer to its group manually. The latter involves automatically assigning the computers via Group Policy or registry settings.

Configure WSUS synchronization

WSUS must first be synchronized before attempting to migrate content. Note that by default WSUS is configured to use Microsoft Update to retrieve updates. Synchronization means the WSUS server contacts Microsoft Update to determine if new updates have been made ready for download since the last time synchronization was performed. This can be done via the WSUS console.

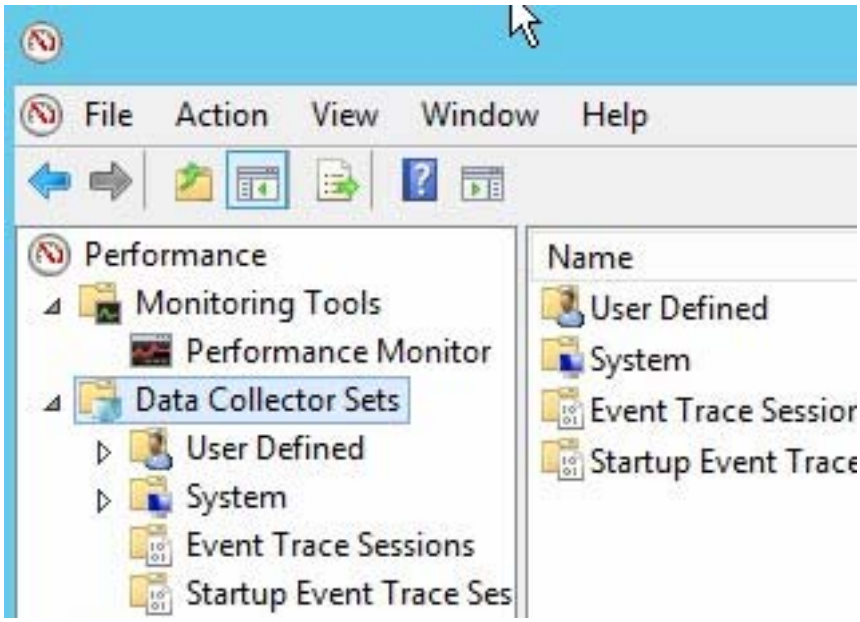
Configure WSUS groups

WSUS allows you to target updates to specific groups of client computers. By default, each client-side targeted computer is assigned to the **All Computers** group. Server-side targeted computers are assigned to the **Unassigned Computers** group unless manually added elsewhere. Remember, computers can be assigned to groups by either server-side targeting or client-side targeting (manual or automatic).

1.3 MONITOR SERVERS

Configure Data Collector Sets (DCS)

The **Data Collector Set** is an **XML** object that works by grouping data collectors into reusable elements to fit into different performance monitoring scenarios. The default Data Collector Set templates can collect performance data immediately without the need for complicated configuration. Additional counters can be added to the various log files. These can be scheduled to start, stop, and define the duration of the collection as needed. To create a Data Collector Set a given user must be logged on as a member of the **Local Administrators** or **Performance Log Users** group.

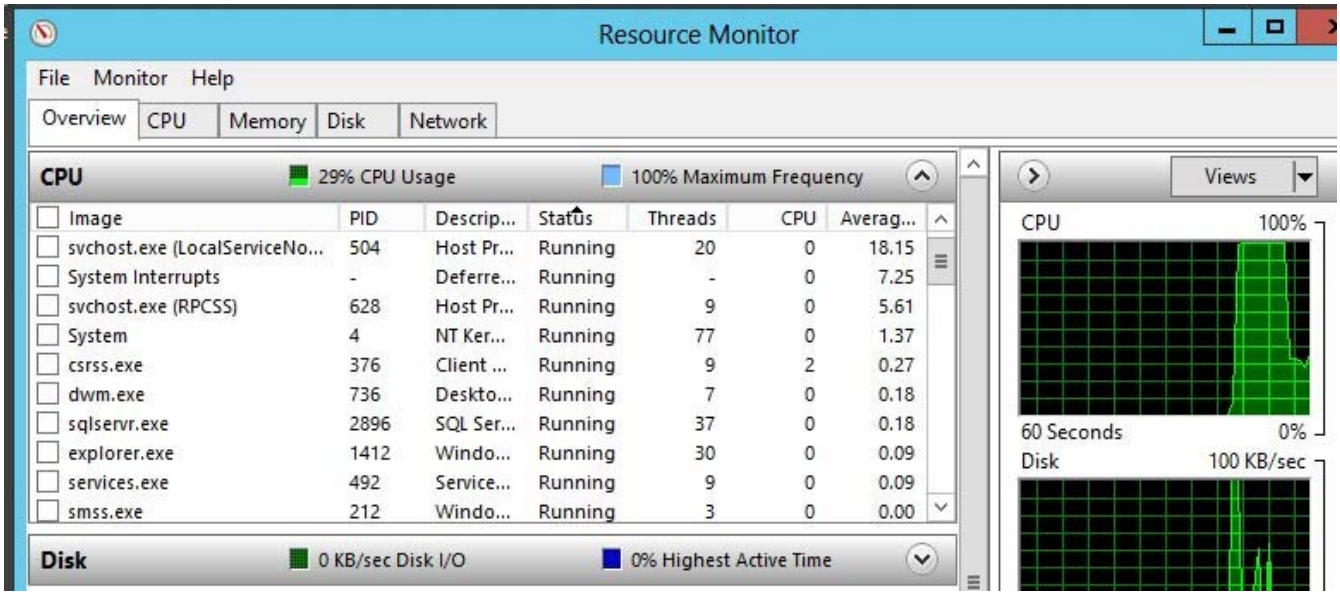


Configure alerts

Alerts can be configured to give notice when particular events take place or predefined performance thresholds are reached. Alerts can be sent as messages or as logged as events in the **Application Event log**. To configure an alert, start the **Create New Data Collector Set Wizard** and choose the **Create Manually** option. On the subsequent **What Type of Data Do You Want to Include** page, select the desired **Performance Counter Alert** option.

Monitor real-time performance

Resource Monitor is a tool that provides real time information regarding CPU, disk, network, and memory usage. It is very useful for identifying files that are causing process lock-ups. In order to use Resource Monitor, the user must be a member of the Local Administrators group or equivalent privilege level. Constantly high utilization in a particular area indicates further investigation may be necessary.



Monitor virtual machines (VMs)

Resource metering can track system resource usage for a single **VM** or for a group of VMs. By default it is not enabled, but you can be via **Enable-VMResourceMetering**. Resource metering statistics are collected once every hour by default, but can be configured for different parameters via **Set-VMHost** with the **-ResourceMeteringSaveInterval** option. To display the measurement data, simply use **Measure-VM**.

Monitor events; configure event subscriptions

It is possible to collect copies of events from multiple remote computers. To precisely specify the remote event to collect, create an **event subscription**. However, before a subscription can be used to collect events on a remote computer, both the collector and the source computer must be properly configured.

In a workgroup only environment, only **Normal mode (pull subscriptions)** can be used. A Windows Firewall exception for **Remote Event Log Management** must be created on the source computer. An account with admin privileges to the Event Log Readers group is also required on the source machine.

Configure network monitoring

Network Monitor 3.4 is a protocol analyzer utility that can capture and view network traffic. This tool is available for x86, ia64 and x64. It requires at least 1 GB RAM and 60MB free hard disk space.

A network trace can also be performed without using a protocol analyzer. This can be done by starting a trace via command line using the command **Netsh Trace start capture = yes**. To stop the trace, enter the command **Netsh Trace stop**. This will create a ****.etl*** file, which can then be converted to XML format for further analysis.

CHAPTER 2 – CONFIGURE FILE AND PRINT SERVICES

2.1 CONFIGURE DISTRIBUTED FILE SYSTEM (DFS)

Install and configure DFS namespaces

DFS Namespaces allows grouping of shared folders that are located on different servers into one or more logically structured namespaces. When you create a namespace you may choose to use either a stand-alone namespace or a domain-based namespace. If you go ahead with a domain-based namespace, you must choose a namespace mode which is Windows Server dependant. You should pick a stand-alone namespace only if you do not use AD DS, or that you want to create a single namespace that has oven 5000 DFS folders in a domain.

If you want to use the Windows Server 2008 mode, the forest must be of the Windows Server 2003 or higher forest functional level, and that the domain must be of the Windows Server 2008 or higher domain functional level. All namespace servers must be at least Windows Server 2008.

You may use the Set-DfsnRoot –GrantAdminAccounts and Set-DfsnRoot –RevokeAdminAccounts Windows PowerShell cmdlets to delegate administration of the DFs namespace, as long as the users belong to the local admin group of the namespace server.

Configure DFS Replication Targets

DFS Replication allows you to keep folders synchronized between servers across very slow and weak network connections. You use DFS Replication to keep folder contents in sync. To replicate folder targets you need to use DFS Management to invoke the Replicate Folder Wizard.

Technically speaking, a folder target is simply the UNC path of a shared folder. You may add multiple folder targets to increase folder availability. You may add a folder target via DFS Management or the New-DfsnFolderTarget cmdlet.

Configure Replication Scheduling

The **Distributed File System Replication (DFSR)** can replicate changes according to the schedule created during site topology design. It has an efficient multi-master replication engine which uses RPC for replicating a folder scope. The possible configuration modes for this service are WMI-based and Active Directory–based.

You may edit the replication schedule or bandwidth via the Set-DfsrConnectionSchedule cmdlet and the Set-DfsrGroupSchedule cmdlet. You may also force replication via the Sync-DfsReplicationGroup cmdlet. To immediately suspend replication, use Suspend-DfsReplicationGroup.

Configure Remote Differential Compression settings

Remote Differential Compression (RDC) is a feature with APIs for determining and detecting if a set of files have changed. There are functions to detect insertions, removals, and rearrangements of data in files. The goal is to allow an application to replicate only the changed parts of a file. To install RDC, use Servermanagercmd -Install Rdc.

Configure staging; configure fault tolerance

DFS Replication makes use of staging folders for each replicated folder as caches for caching the new and changed files that are ready to be replicated. By default the cached files are saved in the local path of the replicated folder. This folder resides in the DfsrPrivate\Staging folder. The quota size of each staging folder is 4096 MB. On the other hand, each Conflict and Deleted folder occupies 660 MB. DFS Replication may create multiple staging and Conflict and Deleted folders, each maintaining its very own quota. Do keep in mind, you can change their sizes. In fact, if you have a staging folder quota configured to be way too small, additional CPU and disk resources will be necessary for regenerating the staged files.

2.2 Configure File Server Resource Manager (FSRM)

Install the FSRM role

In a pre 2012 R2 setup, you may rely on the **File Server Resource Manager (FSRM)** to control, and manage the quantity and type of data being stored on a server. This role can be added via the Server Manager. In fact, when you install FSRM you can also configure Storage Usage Monitoring (you select disk volumes for monitoring and specify volume usage threshold for report generation) and Report Options page (this is where you pick a save location for usage reports or have reports sent to you by email - you will be asked to specify recipient email addresses as well as the SMTP server to use).

Configure quotas

To create a quota, you need to choose a quota path which is a volume or folder with storage limit applied. Then you may use a template to create a single quota that limits space usage on an entire volume or folder, or an auto apply quota which allows quotas to be automatically generated and applied to subfolders. A quota template has space limit, quota type (hard VS soft) and notifications defined. You may use the Dirquota.exe tool to define and manage quotas, auto apply quotas and quota templates.

Configure file screens

File Screening Management allows you to create file screens for controlling the types of files that users can save and use. File screening templates can be applied to new volumes or folders, while file screening exceptions are for use with file screening rules. Active screening disallows users from saving unauthorized files, while passive screening would only send configured notifications but does not stop anything. A file group defines a namespace for a file screen. It has a set of file name patterns grouped as either Files to include or Files to exclude. You may use the Filescrn.exe tool to create and manage file screens, templates, exceptions and file groups.

Configure reports

Storage Reports Management allows you to schedule periodic storage reports, monitor attempts to save unauthorized files, and generate storage reports accordingly. If you want to generate a set of reports based on a regular schedule, you should schedule a report task. In any case you may use storrept.exe to further configure report parameters and produce storage reports on demand (which means Generate Reports Now).

2.3 CONFIGURE FILE AND DISK ENCRYPTION

Configure Bitlocker encryption

BitLocker is a disk encryption tool with features for protecting against unauthorized access to local drive data. It supports fixed data drive when the drive is formatted with exFAT, FAT16, FAT32, or NTFS and that there is 64 MB of available disk space. To allow the drive to be unlocked automatically, the OS drive itself must be protected by BitLocker.

Configure the Network Unlock feature

Network Unlock provides automatic unlock of volumes upon system reboot at the time it is connected to a wired network. For this feature to work the client hardware must have a DHCP driver working from within its UEFI firmware. Simply put, with this feature enabled the volumes protected by TPM+PIN protectors will not require the input of a PIN when the machine reboots.

Configure Bitlocker policies

BitLocker Group Policy settings are in either the Local Group Policy Editor or the GPMC (you can find it under Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption). Most settings are applied at the time BitLocker is initially turned on for a drive. Note that you can have policy settings applied to:

- all BitLocker-protected drives.
- drives on the local computer on which the OS is installed.
- drives permanently installed on the local computer.
- removable data drives.

Configure the EFS recovery agent

You should ensure that the private key for the data recovery agent is not always kept online for the sake of security. To be precise, the data recovery agent's key should be made offline (as .pfx file) at all time unless it is needed for use by a recovery process.

You may add data recovery agents to the **EFS Policy**. However, it has no effect on the existing encrypted files. Any user who can decrypt an EFS file can add other users' public keys to it. Also, you cannot assign keys from a group of users - each user's public key has to be accessed on an individual basis.

Manage EFS and Bitlocker certificates including backup and restore

By default the data recovery agent is contained in the personal certificate store of the administrator account of the first domain controller. However, on standalone/workgroup machines it would be contained in the personal certificate store of the local administrator.

Encrypting File System (EFS) certificates allow the certificate holder to encrypt and decrypt data. Ordinary EFS users should be granted this type of certificate. File Recovery certificates are for recovering encrypted files. Domain admins and/or designated data recovery agents should be granted this type of certificate instead. In any case you should use the Certificates MMC snap-in to back up the default recovery keys.

2.4 CONFIGURE ADVANCED AUDIT POLICIES

Implement auditing using Group Policy and AuditPol.exe

You may implement audit policy using GPO. You need to first specify the categories of events that are to be audited (it is the event categories that constitute your audit policy). You then specify the size and behavior of the Security log. Basic audit policy is never compatible with the advanced audit policy settings applied via Group Policy. When the advanced audit policy settings are applied through using Group Policy, the current computer's local audit policy settings are cleared.

At the command line, you use auditpol /get to show the current audit policy. You use auditpol /set to set the audit policy. You use auditpol /clear to clear a policy. You use auditpol /backup to save the policy to a file, or use /restore to restore the policy from the backup file.

Create expression-based audit policies

Expression-based audit policy allows the use of complex logic for filtering auditing to specific criteria. In particular you can specify the use of the boolean AND and OR operators. You may further group together criteria to make script-like complex expressions.

Create removable device audit policies

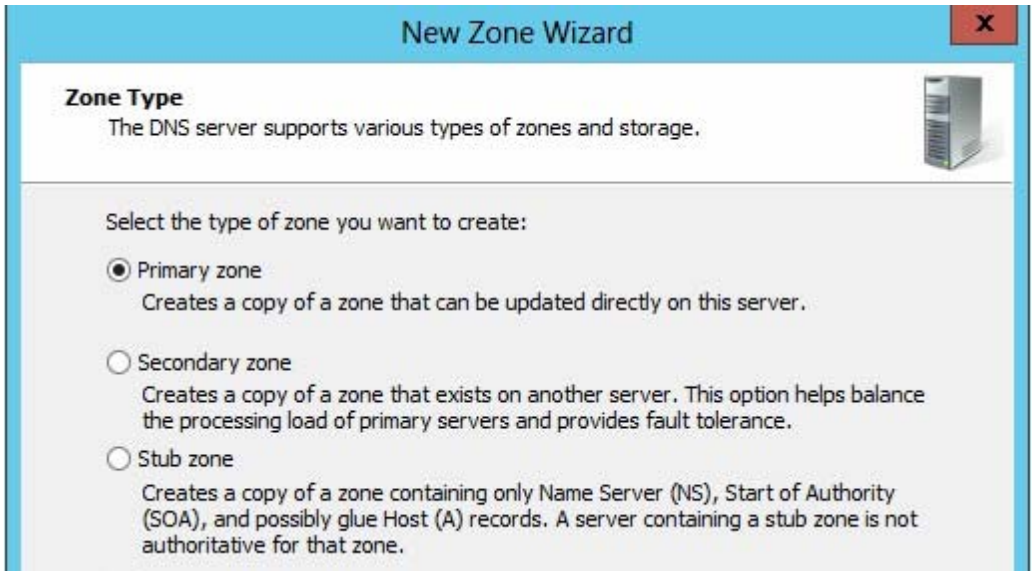
You may want to monitor attempts to use removable storage devices for accessing network resources. Under **Advanced Audit Policy Configuration** - Object Access there is an item known as Audit Removable Storage. Once enabled, from the Event Viewer - Security Log you should see event 4663 for successful attempts and event 4656 for failure attempts.

CHAPTER 3 – CONFIGURE NETWORK SERVICES AND ACCESS

3.1 CONFIGURE DNS ZONES

Configure primary and secondary zones

You use the **New Zone Wizard** to create the zones. In particular you need to have a primary zone for your domain. Other zones can also be created through it. You want to create a secondary zone for load sharing and fault tolerance.



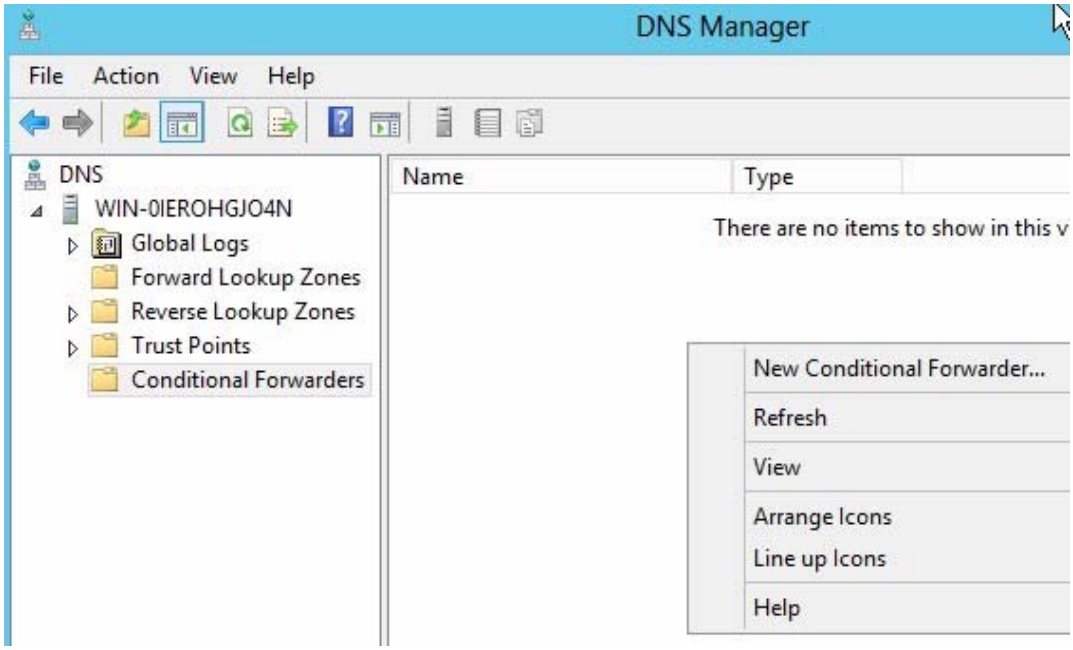
Only primary zones can be stored in AD. A secondary zone is simply a secondary source for information of a zone. It must be obtained from a remote DNS server and can be stored in text file only. Because AD implements a multimaster replication model, secondary zones become quite unnecessary.

Configure stub zones

With a **stub zone** the DNS server serves as a source only for information about the authoritative name servers for the zone, which must also be obtained from a remote DNS server. You can use stub zones to keep delegated zone information current, to enable a DNS server to perform recursion via the stub zone's list of name servers without querying somewhere else, and to simplify administration.

Configure conditional forwards

You may have your DNS server designated as a forwarder. You can use the DNS Manager or the dnscmd command with the /ResetForwarders option to configure this. DNS Manager also has a section for configuring the so called conditional forwarder.



Configure zone and conditional forward storage in Active Directory

You can specify that the DNS server only uses forwarders and not attempt any further recursion if the forwarders fail by checking the Do not use recursion for this domain check box. You can also disable recursion for the DNS server so that it will never perform recursion on any query. By doing so you will not be able to use forwarders on the same server anymore. Keep in mind, you are not allowed to use a domain name in a conditional forwarder if this DNS server is hosting a primary zone, secondary zone, or stub zone for that domain name.

Configure zone delegation

You use the **New Delegation Wizard** to add a new delegated domain. Zone delegation works like "dividing" your DNS namespace. You do this to distribute traffic loads among multiple servers and improve DNS name resolution performance/resiliency. You also do this to extend the namespace to accommodate the opening of a new branch office or remote site.

Configure zone transfer settings

You use the DNS Manager to perform zone transfer. You should allow zone transfers only for DNS servers in the NS resource records for a zone or for the specified DNS servers and nothing else. In the command line you use dnscmd. /NonSecure means transfer can be made to any server. /SecureNs means transfers can be made only to those listed in the zone's NS resource records. /SecureList means to a specific server only.

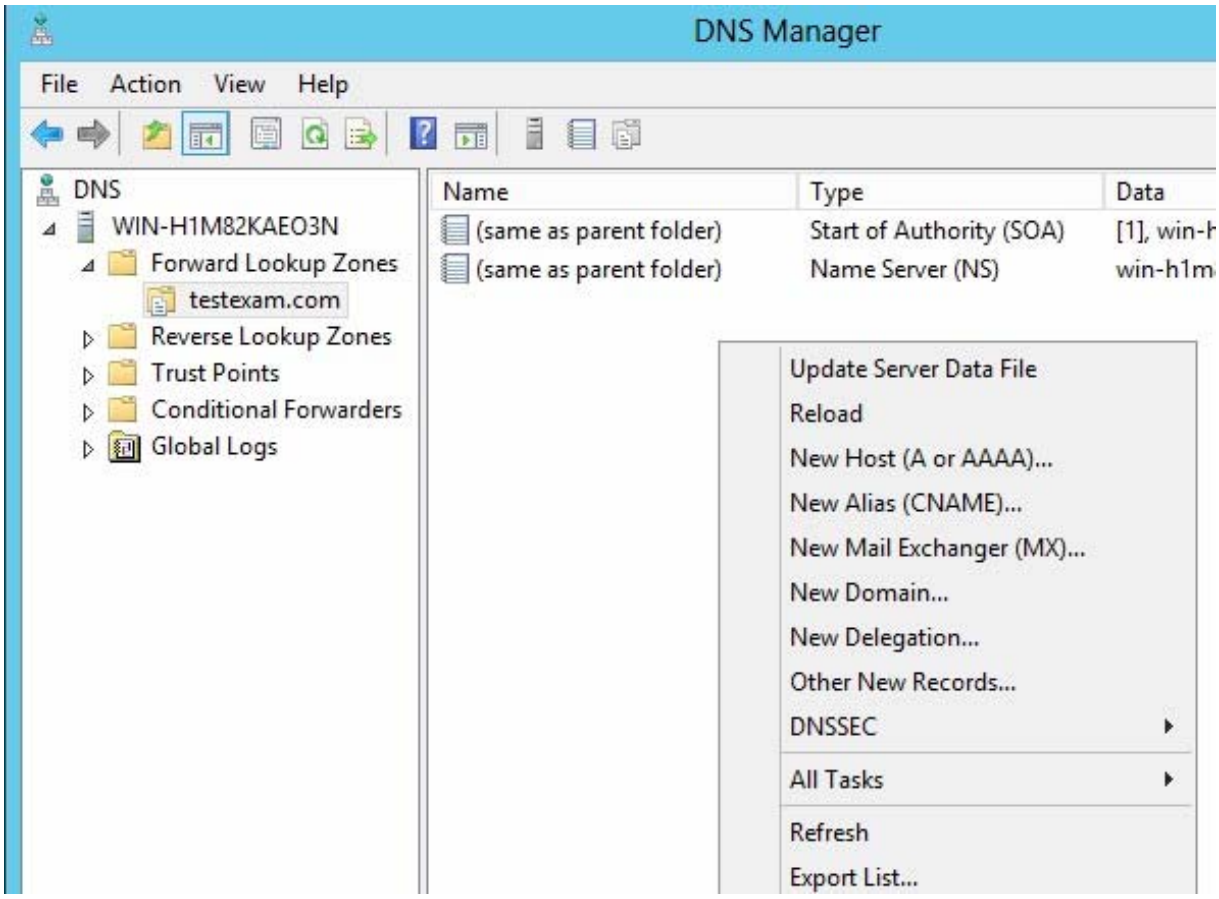
Configure notify settings

DNS Notify means the master server for a zone would first notify some secondary servers in that zone of changes. Those secondary servers then check to determine whether they should initiate a zone transfer. This is done to improve consistency of zone data among the secondary servers.

3.2 CONFIGURE DNS RECORDS

Create and configure DNS Resource Records (RR) including A, AAAA, PTR, SOA, NS, SRV, CNAME, and MX records

With a DNS zone ready you can right click on it and add records as necessary. Except for important servers that use static addresses, records should not need to be manually created. When Active Directory is configured, the Wizard will automatically configure DNS on a new domain controller and will create resource records necessary for the proper operation of the DNS server.



Configure zone scavenging

Both **aging and scavenging** are for performing cleanup and removal of stale resource records so they don't accumulate in zone data. The DNS Manager UI can be used to configure these. Or, if you use dnscmd, /Aging is for enabling aging for zones, while /RefreshInterval is for specifying the Refresh interval for a scavenging-enabled zone. /ScavengingInterval is for fine tuning the scavenging interval.

Configure record options including Time To Live (TTL) and weight

Time to Live (TTL) is used by name servers for determining the length of time a name can be cached. By default the TTL is 60 minutes. You can modify the TTL values via the DNS Manager UI. On the client side, registry editing would become necessary (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters).

It is also possible to cut down the workload on the PDC emulator operations master by adjusting the weight for DNS service SRV resource records by editing the registry under HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters. The valid value is between 0 and 65535, with a default of 100. A higher value always indicates a lower priority.

Configure round robin

Round Robin Load Balancing is primarily for DNS service. You have a built-in round robin feature of the BIND DNS server which works by cycling through the IP addresses corresponding to a server group. Hardware load balancers, I contrast, are dedicated for routing TCP/IP packets to various servers in a cluster.

From inside the DNS Manager there is a Server options section which provides you with the Enable round robin check box. dnscmd also has a /RoundRobin option. 1 means on while 0 means off.

Configure secure dynamic updates

DNSSEC includes extensions for hardening the DNS infrastructure as specified in several IETF RFC standards, including 4033, 4034 and 4035. With it, there are several new types of record, which are DNSKEY, RRSIG, DS, and NSEC/NSEC3. Dynamic DNS updates can be enabled for DNSSEC-signed zones as long as active directory is there, and that the scavenging stale record option can be used for purging old DNSSEC records. For the setup to work, a primary server must be in place to serve key management and key generation service to the network environment.

3.3 Configure VPN and routing

Install and configure the Remote Access role

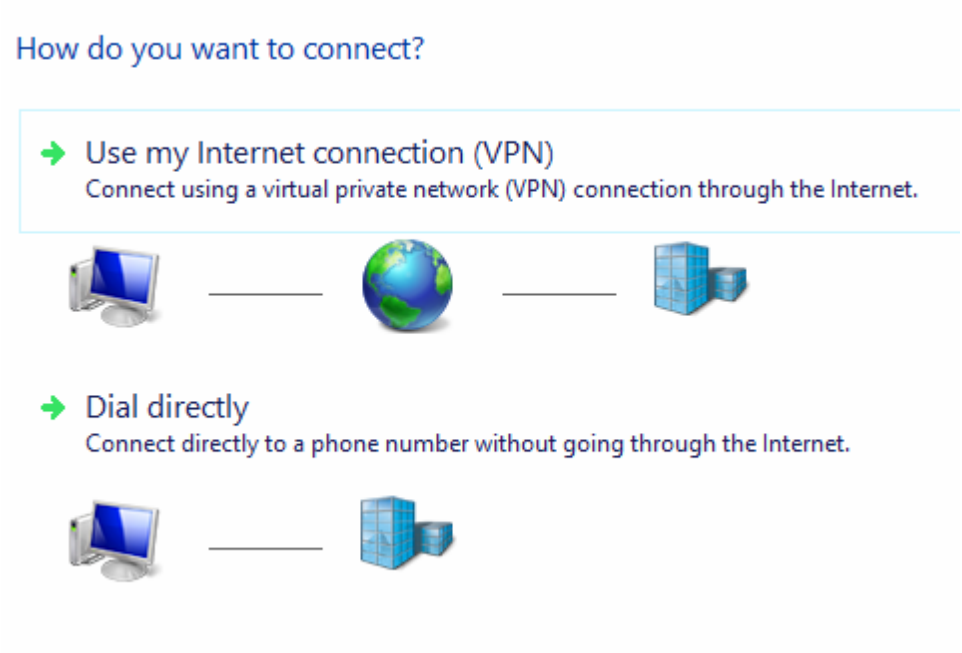
The **Routing and Remote Access Server** has three sub-roles, which are Remote Desktop Services Connection Broker; Licensing; and Virtualization. You do not configure any of these server roles during server installation. Instead, you add roles through the Server Manager Dashboard upon setup completion.

Implement Network Address Translation (NAT)

Through RRAS it is possible to implement **Network Address Translation (**NAT). NAT already includes addressing and name resolution features that provide DHCP and DNS services to clients, you are advised to not run DHCP service or DHCP Relay Agent with NAT addressing enabled. You should also NOT run the DNS service unless NAT TCP/IP networking name resolution is currently disabled.

Configure VPN settings

The Set up a new connection or network link can be used for starting up the Set Up a Connection or Network wizard, which is a helpful UI to all of the network connection types you can create. The first option is for configuring internet connectivity, while the second is for setting up a VPN. VPN can be through either the internet or via direct dial up (through phone line).

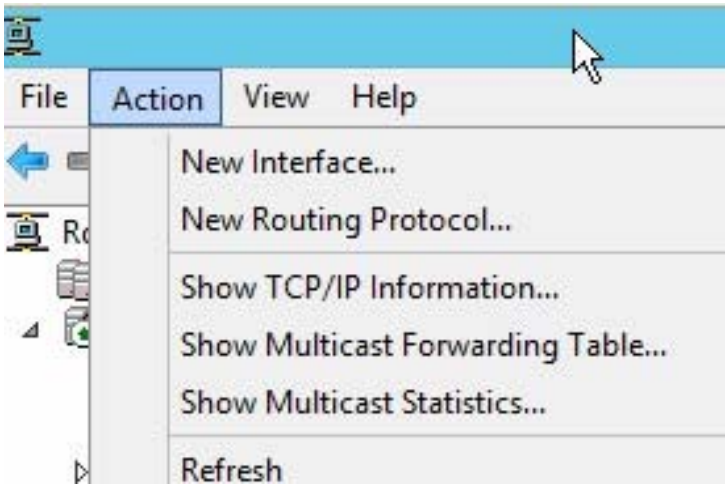


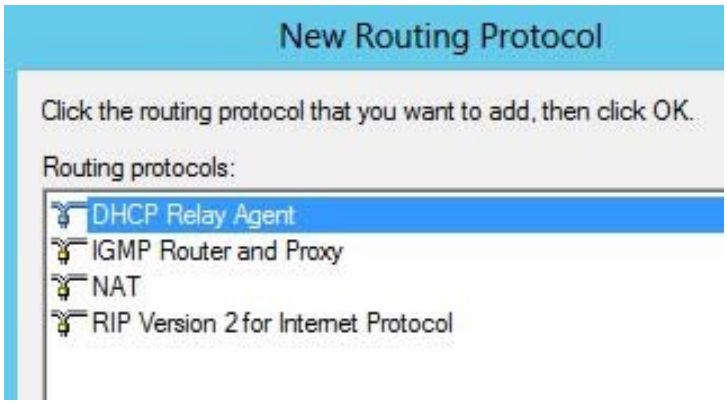
Configure remote dial-in settings for users

When RRAS has been added via the Server Manager, you may invoke the Routing and Remote Access Server Setup Wizard via the Routing and Remote Access snap-in. From there you may click Configure and Enable Routing and Remote Access. In the Remote Access page you may enable dial up support for end users. You may setup an IPv4 Remote access server or an IPv6 Remote access server. Both IPv4 Forwarding and IPv6 Forwarding are supported.

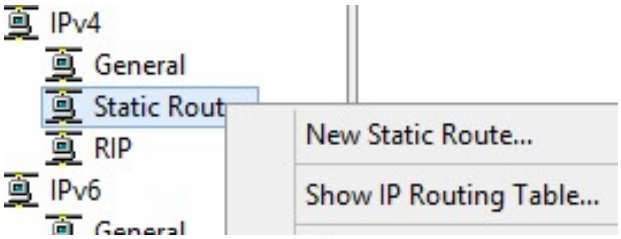
Configure routing

To allow RRAS to be operated as a Ipv4 router, you should also enable and configure RIP. You can do so by first clicking on Ipv4-General and then click on the Action menu.





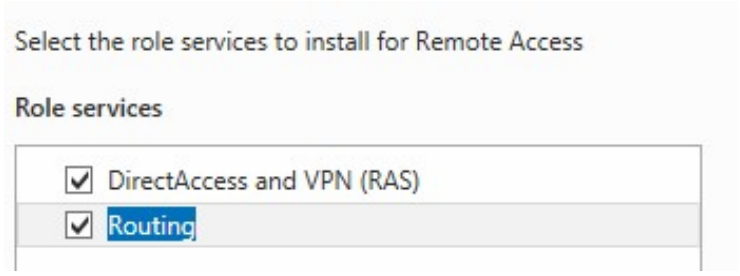
For IPv4, RIP Version 2 for Internet Protocol is the most populr choice. You may add it, then right-click RIP and choose New Interface. You will need to pick the interface that is connected to a subnet on which the remote router is connected so your interface can communicate using RIP. You can also right click on RIP and choose Show neighbors to find out about the routing partners on the network. Static routes can be manually added by right clicking on the Static Routes item.



3.4 CONFIGURE DIRECTACCESS

Implement server requirements

You need to install the DirectAccess and VPN role and the corresponding role services. In fact we would recommend that you also install routing:



After role installation you may call up the wizard for further configuration. Your server must be a member of a domain or configuration will fail.

A complete DirectAccess solution for mobile access would require a DirectAccess server running Windows Server 2012 with dual network adapters. You need one facing the internet and another facing the intranet. The former needs to have two consecutive public IPv4 addresses assigned. There must also be a domain controller and DNS server running Windows Server 2012, as well as a public key infrastructure issuing computer certificates.

Implement client configuration

DirectAccess aims to allow connectivity to the corporate network without the need for using traditional VPN connections. It supports domain-joined Windows 7 Enterprise and Ultimate edition clients as well as Windows 8 clients. Earlier clients, however, are not supported.

Configure DNS for Direct Access

Split-brain DNS refers to the use of the same DNS domain for both Internet and intranet resources. For this kind of setup to work, you need to list the FQDNs that are duplicated on the Internet and intranet. You can then accordingly decide which resources your DirectAccess client may reach. In a non-split-brain setup the Internet namespace is not the same as the intranet namespace so you would not need to make such decision.

If you are using ISATAP for IPv6 connectivity to support your DirectAccess clients, you better use DNS servers that run Windows Server 2008 R2 or later since their DNS Server service can support the processing of DNS traffics on the ISATAP interfaces. If your IPv6-capable non-Windows based DNS server do not support DNS dynamic update for IPv6 addresses, you will need to manually add AAAA records for your servers.

The DirectAccess Setup Wizard allows you to configure local name resolution behavior. The possible options are Use local name resolution only if the internal network DNS servers determined that the name does not exist; Use local name resolution if the internal network DNS servers determined that the name does not exist or if the internal network DNS servers are not reachable and the DirectAccess client computer is on a private network; and Use local name resolution if there is any type of error when attempting to resolve the name using internal network DNS servers. The first option is the most secure.

Configure certificates for Direct Access

There should be one certificate per client and one per Direct Access server. You may use certutil to display information on the digital certificates that have been installed on a DirectAccess client, DirectAccess server, or any other intranet resources.

CHAPTER 4 – CONFIGURE A NETWORK POLICY SERVER INFRASTRUCTURE

4.1 CONFIGURE NETWORK POLICY SERVER (NPS)

Configure multiple RADIUS server infrastructures

A RADIUS server group refers to a group of multiple RADIUS servers. The setup allows network access requests to be load balanced dynamically by a RADIUS proxy. Do note that each RADIUS server group represents one uniquely distinct set of remote access policies. You may in fact have separate RADIUS server groups defined for separate forests or untrusted domains, while allowing the connection request policies to stay at the RADIUS proxy.

Configure RADIUS clients

When NPS is used as a RADIUS server or proxy, the corresponding network access servers are called RADIUS clients. Types of clients may include Windows based network access servers that provide remote access connectivity, wireless APs, switches and RADIUS proxies that forward connection requests.

NPS sends and receives RADIUS traffic via UDP ports 1812, 1813, 1645, and 1646. Windows Firewall on the NPS server will allow these RADIUS traffics to get through by default. Should you change these ports by hand, Windows Firewall must be modified accordingly.

Manage RADIUS templates

The template type known as RADIUS Clients is for configuring RADIUS client settings that can be reused through selecting the template in the proper location of the NPS console. Remote RADIUS Servers is another template type which can help you configure the various remote RADIUS server settings.

Configure RADIUS accounting

From inside the NPS console you can invoke the Accounting Configuration wizard which provides these accounting settings:

- SQL logging only - you need to configure a data link to a SQL Server for this to work
- Text logging only - this is simple as it simply logs accounting data to a text file.
- Parallel logging - you log both to SQL Server and to a text file

- SQL logging with backup - you log first to SQL, and use text file as backup if SQL fails.

Configure certificates

For client authentication to take place a digital certificate must be installed on the RADIUS server for providing authentication, encryption, and validation. This can be done via the Certificate Console.

4.2 CONFIGURE NPS POLICIES

Configure connection request policies

Network policies refer to conditions, constraints, and settings that designate who is authorized to connect to the network and the revelant circumstances. You may view your network policies as rules with conditions and settings. NPS will compare the conditions of the rule to the properties of the connection requests.

Connection request policies are the conditions and settings that allow you to indicate the RADIUS servers that perform the authentication and authorization of connection requests. If you use NPS as the RADIUS server, the default connection request policy will be the only configured policy. However, if NPS serves as a proxy only, NPS will not process any connection requests locally.

Configure network policies for VPN clients (multilink and bandwidth allocation, IP filters, encryption, IP addressing)

You can configure these parameters in the client side network policies:

- Multilink and Bandwidth Allocation Protocol BAP deals with using multiple dial-up connections from one computer.
- IP Filters are for creating IPv4 and IPv6 filters for controlling the IP traffic that the clients can send or receive.
- Encryption is for specifying the encryption level required.
- IP Settings are for specifying the client IP address assignment rules that are for use in the network policy.
- Idle Timeout is for specifying the max time in minutes that the network access server can stay idle before cutting off the connection.
- Session Timeout is for specifying the max time in minutes that a user may stay connected.

Manage NPS templates

You can use NPS templates to configure NPS on servers. There are many templates available, which include:

- Shared Secrets
- RADIUS Clients
- Remote RADIUS Servers
- IP Filters
- Health Policies
- Remediation Server Groups

To create a template, you need to use the NPS Console (you simply right-click on a template type and click New). To use a template, from within the RADIUS client properties you choose the option known as Select an existing Shared Secrets template.

Import and export NPS policies

You may export NPS configuration and policies via Netsh (you need to use netsh nps export) or Windows PowerShell (via Export-NpsConfiguration). With the later, a XML file will be created for import later. Do realize that the exported NPS server configurations are never encrypted in the XML file so you must be careful in protecting it.

4.3 Configure Network Access Protection (NAP)

Configure System Health Validators (SHVs)

When you need NPS to be configured to block certain clients or traffics (in other words, to perform validation), the steps involved are:

- Creating a System Health Validator SHV (you can do so via the Network Policy snap-in).
- Creating a health policy for the compliant clients and also the noncompliant clients.
- Creating a network policy for the compliant clients and also the noncompliant clients.

Configure health policies

You use the NAP Client Configuration console to configure NAP user interface settings, NAP enforcement client settings, as well as Health Registration Authority HRA settings on the client computers. If you configure NAP client settings via Group Policy, the settings will be automatically configured when the Group Policy is refreshed.

Configure NAP enforcement using DHCP and VPN

NAP has different enforcement mechanisms. The DHCP enforcement mechanism makes use of the DHCP server as its gatekeeper. Clients that connect to your network will request an IP address from DHCP. This is when the NAP-enabled DHCP server will perform enforcement - the client must give a correct response in order to receive an IP address with full network access. VPN enforcement is similar - a VPN server can enforce health policy when a client attempts to connect via a VPN connection.

Configure isolation and remediation of non-compliant computers using DHCP and VPN

Noncompliant clients computers are those that fail to meet your NAP health requirements. Strictly speaking, only NAP client computers are either compliant or noncompliant. NAP remediation server is for providing services to the noncompliant clients. In fact, the number and type of remediation servers to be made available determines the level of access restriction by the noncompliant clients. Without help from a remediation server the noncompliant computers will fail to perform properly in the network. For the sake of security you may even have the noncompliant computers further isolated in a separate remediation network.

With VPN enforcement, you may want to place your remediation servers on either the corporate network or a perimeter network. Limited access to corporate resources may be made available via IP packet filters applied to the VPN connection. With DHCP enforcement, your remediation servers may be placed inside the corporate network but access is limited to the DHCP NAP enforcement server and any other remediation servers that you explicitly allow.

Configure NAP client settings

If you want to use NAP to enforce health policies on the client computers, you will have to first configure NAP settings on them. You may do so via the NAP Client Configuration console NAPCLCFG.MSC or the Netsh nap client command line (you may also use the NAP client configuration settings from within the GPMC). The client components compile health status statements on client computers for analysis by the server. The NAP enforcement client enforces network access restrictions. Generally, you should make use of the NAP Client Configuration through Group Policy in AD when there are a lot of client computers to manage.

CHAPTER 5 – CONFIGURE AND MANAGE ACTIVE DIRECTORY

5.1 CONFIGURE SERVICE AUTHENTICATION

Create and configure Service Accounts

A **service account** is a user account, just that it is created for providing a security context for services. You may create and manage service accounts individually via Active Directory Users and Computers.

On a computer not joined to a domain, you may configure an application to run as Local Service, Network Service, or Local System. The problem with these accounts is that they are shared among many services and there is no way to have them managed at the domain level. If you use a domain account instead of a local one, you can isolate its privileges, just that you must manually manage the passwords.

Create and configure Group Managed Service Accounts

When **group Managed Service Accounts (gMSA)** is used as service principal, Windows will manage the password for the account. gMSA is like a Managed Service Accounts MSA but with functionality extended across multiple servers. With it you can tie a group of servers to one single service account, which is particularly useful for multi-instance Server cluster.

Do note that this is a feature that requires Windows Server 2012 R2 Domain Controller with Active Directory PowerShell Module imported into it.

Create and configure Managed Service Accounts

A **managed service** account (MSA) allows services to have isolation of their own domain accounts and at the same time avoiding the need for manually administering the account credentials. The goal is to create a class of domain accounts for managing and maintaining services on the local computers. The client computer must be running at least Windows Server 2008 R2 or Windows 7 to enjoy the feature. The domain must be at least Windows Server 2008 R2, or you will need to prepare the schema using adprep /forestprep and adprep /domainprep respectively. In any case, a MSA can only be used on one domain server.

Configure Kerberos delegation

Constrained delegation is a feature of Kerberos V5. It allows a service to obtain service tickets using the delegated user's identity. These service tickets allow access to only a restricted list of services running on specific servers. You may accordingly limit the network resources that a service trusted for delegation may reach.

Unconstrained delegation is slightly different - it is supported only when a user initially renders credentials for obtaining a ticket granting ticket that can be forwarded to any service trusted for delegation.

Manage Service Principal Names (SPNs)

A **service principal name (SPN)** is associated with the security principal, which is either a user or a group. It is used to support mutual authentication between the client application and the service. A SPN can be associated with only one account, but an account can have more than one SPNs. It may be formed either using information that a client learned about a service, or as supplied by Active Directory.

You don't normally need to create a SPN by hand. A client can and should create the SPN for a service. It is a must have. When a client uses Kerberos to authenticate itself, it will request a session ticket for the SPN. With certificate-based authentication, this SPN will have to be validated against the certificate of the server.

A SPN is formed like this service_class/host_name:port: Note that Windows provides many built-in service classes but you can also define your own. The host name is the name of the computer host. By registering the SPN in Active Directory the SPN is mapped to the Windows account under which the service specified is running. Automatic SPN management can make your life much easier. When a Windows Server that belongs to a gMSA change its host name, the corresponding SPN will be automatically updated as well. Still, you can use Setspn.exe to manually register, edit and verify SPNs.

5.2 Configure Domain Controllers

Configure Universal Group Membership Caching (UGMC)

Universal group membership caching (UGMC) is a feature which can locally cache a user's membership in universal groups on the domain controller authenticating the user. It is mostly useful for deployment in branch office without a global catalog due to concern on WAN traffic. Since UGMC is site specific, you may enable it via Active Directory Sites And Services (under NTDS Site Settings).

Transfer and seize operations masters

You use Ntdsutil.exe to transfer and seize operations master role. The tool will first try to make a transfer from the current role owner. It will go ahead and seize the role if the current role owner is unavailable. You may view the current operations master role holders via the roles option of Ntdsutil. To actually seize a role, at the fsmo maintenance prompt you use the seize command.

Install and configure a read-only domain controller (RODC)

A **Read Only DC (RODC)** is an additional domain controller that hosts read-only partitions of the Active Directory database. It is mostly for use in branch office with poor WAN link. It can keep cached credentials so that faster login can become possible. However, the first domain controller in a forest must NOT be an RODC. Unless you have a mix of different Windows Server versions running as domain controllers, you should not need to run adprep /rodcprep before installing a RODC.

Configure Domain Controller cloning

Cloning virtualized domain controllers makes things easy when deploying multiple domain controllers. As long as both the source and target servers are running the Hyper-V server role, cloning is possible without th eneed to use sysprep and the like. You may use the Active Directory Administrative Center ADAC UI to locate the virtualized domain controller object and accordingly grant permissions to be cloned. Then you run the Get-ADDCCloningExcludedApplicationList cmdlet to identify programs or services that are not really clonable. And then you run New-ADDCCloneConfigFile to produce the necessary configuration file (which is DCCloneConfig.xml) for facilitating the export and import of VMs. Normally the clone domain controller will be placed in the same site as the source unless there is a different site explicitly specified in DCCloneConfig.xml.

5.3 Maintain Active Directory

Back up Active Directory and SYSVOL

It is the **system volume (SYSVOL)** on the domain controller that provides a default Active Directory location for files being shared for access throughout a domain. The SYSVOL folder has a bunch of NETLOGON shared folders, user logon scripts for earlier Windows clients, file system junctions and FRS staging directories and files. On the other hand, AD itself has the Ntds.dit file which is the AD database, the Edb.chk checkpoint file, the Edb*.log transaction log files, as well as the Res1.log and Res2.log files. They are all considered as system state data.

A good backup should include at least the system state together with the contents of the system disk. You must back up at least 2 domain controllers in each domain, with one being an operations master role holder excluding the RID master. Do note that you cannot use a backup from one domain controller to restore another one. Also note that a backup older than the tombstone lifetime set in AD should not be considered as a good backup. At least 2 backups should be made within the tombstone lifetime (keep in mind, the default value for the tombstone lifetime is 60 days).

Manage Active Directory offline

You use net stop ntds to stop AD locally. This cannot be done via any GUI. If you start the system and press F8 to enter the Directory Services Restore Mode, you are also working offline (you need to logon locally as a local admin).

Optimize an Active Directory database

Active Directory (AD) can automatically perform online defragmentation of the database at the default intervals of every 12 hours during Garbage Collection. Online defragmentation can optimize the database without reducing its size. It can reclaim space in the directory for new objects though. In fact, the process will create a new and compacted version of Ntds.dit.

Another option is to defrag the database offline, which is a more thorough defrag also capable of compacting the database. Before attempting offline defragmentation, you are strongly recommended to make a full system state backup of the domain controller. Do make sure there is enough free space on the drive. When you perform offline defragmentation Windows is not going to change the original Active Directory database. Instead it will produce a defragmented copy. This is why the process needs to use a large amount of free space on the drive as the work space plus space for storing the copy (which should be at least 115% of the original size).

As said before you use net stop ntds to stop AD locally. From within ntdsutil you need to use activate instance ntds and then files to reach the file maintenance prompt, then start the defrag process via compact to. When done you need to quit ntdsutil entirely and manually copy the new database to the original directory database location.

Clean up metadata

Metadata cleanup is a process you need to perform on a domain controller after AD DS removal. The process primarily removes those data items that identify a domain controller to the AD DS replication system as well as all FRS/DFS Replication connections. The process will also try to transfer or seize any remaining operations master roles.

You use Active Directory Users and Computers or Active Directory Sites and Services to delete a domain controller permanently. You may also use ntdsutil's metadata cleanup command to clean up the metadata.

Configure Active Directory snapshots

A **snapshot** is in fact a shadow copy of the volumes that contain the Active Directory database. With it you can view the data inside it without the need to run the server in Directory Services Restore Mode. Do note that it does not let you to copy items from inside the snapshot to the live database, unless you manually export the objects out of it. You can use ntdsutil under the elevated command prompt to create a snapshot. You reach the snapshot: prompt via the snapshot command and then use create to create the snapshot. You may view the available snapshots via list all. And you may mount one via mount.

Perform object- and container-level recovery

With an authoritative restore you return a deleted object or container to its pre-deletion state at the time it was backed up. There are usually 2 parts to such restore process. First there is a nonauthoritative restore from backup, then there is an authoritative restore of the deleted objects. You need to do this before allowing replication to occur.

To perform an authoritative restore, you need to use the authoritative restore subcommand of Ntdsutil or Dsdbutil (which is available if you have the AD LDS server role in place). You need to first stop the AD DS service or the AD LDS service, and you must set the active instance accordingly.

Since Windows Server 2012 there is the Active Directory recycle bin facility which allows you to restore active directory user objects natively, as long as your forest has the "Windows server 2008 R2" functional level or beyond. The process does take time to complete since replication is necessary.

Perform Active Directory restore

As said before, if you start the system and press F8 to enter the Directory Services Restore Mode, you are also working offline. You will need to logon locally as a local admin. A Nonauthoritative restore means you have a domain controller restored from backup media, then allow the restored data to be updated through normal replication. This process usually requires that you take the domain controller offline.

After going offline, you may invoke the Restore Wizard to restore the System State data. You click Start - Run, then type in Ntbackup to invoke the Backup tool. From the Tools menu you click Restore Wizard to call up the wizard.

5.4 CONFIGURE ACCOUNT POLICIES

Configure domain user password policy

Password policies are for domain accounts or local accounts - they determine a number of settings for passwords, such as:

- Enforcing password history
- Enforcing maximum password age
- Enforcing minimum password age
- Enforcing minimum password length
- Enforcing password complexity requirements
- Storing passwords using reversible encryption

At the domain level the best thing to do for applying password policies is to use Group Policy. The tool to use is Active Directory Users and Computers. PSO is another solution you can use. We will talk about this in the next section.

Configure and apply Password Settings Objects (PSOs)

Note that since Windows Server 2008 you can use fine-grained password policies to specify multiple password policies to different groups of users within a single domain. There are two object classes in Active Directory that deal with these. They are the Password Settings Container and the Password Settings object PSO. You can create a PSO using ADSI Edit, or you can use the New-ADFineGrainedPasswordPolicy cmdlet to achieve the same.

Delegate password settings management

You may delegate password management to someone else. From within Active Directory Users and Computers you call up the Delegation of Control Wizard. This wizard allows you to pick the password related tasks to delegate.

Configure local user password policy

Local security policy is local server specific – the policies are not stored in Active Directory. As a local admin you may open up the Local Security Policy UI via secpol.msc. The UI has a Navigation pane with an option known as Account Policies. You can click Password Policy to make the necessary policy settings.

Configure account lockout settings

You all know what account lockout is about. Technically, Account Lockout Policy settings are configured in Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy through the GPMC. In terms of duration, the valid range is from 1 through 99,999 minutes. If you set the value to 0, the account is locked out until you explicitly have it unlocked. Account lockout threshold determines the number of failed logon attempts that can be tolerated. The number of minutes that can be specified is between 1 and 999.

CHAPTER 6 – CONFIGURE AND MANAGE GROUP POLICY

6.1 CONFIGURE GROUP POLICY PROCESSING

Configure processing order and precedence

By default, Group Policy settings are processed in this order: Local Group Policy object -> Site -> Domain -> OU

Keep in mind, local GPOs are always processed first, while GPOs linked to the OU are always processed last. The last one being processed can overwrite settings made in the earlier GPOs should conflicts arise. Exceptions may be possible if a GPO link is enforced or disabled, or that an OU has Block Inheritance enabled.

Configure blocking of inheritance

You may set a container to block any policies from higher levels from being applied. Do note that **Block Policy Inheritance** is a container property, NOT a link property. In fact, Enforced at a higher level will always take precedence over Block Policy Inheritance at a lower level. Simply put, GPO links that are enforced is not allowed to be blocked.

Configure enforced policies

You may set a policy at a higher level to always apply via enforcement (i.e. no override). Do note that Enforced is a link property, NOT a container property. It always takes precedence over Block Policy Inheritance. As said previously, GPO links that are enforced is not allowed to be blocked.

Configure security filtering and WMI filtering

WMI and **security group filters** can both be used to restrict each GPO to the computers of a membership group running the version of Windows for which the GPO is targeting. To be precise, security filtering applies policy settings to only a particular set of users and computers that you choose, while WMI filters can be used based on the target computer specifications (make, model, OS...etc).
When you define a new WMI filter, you will need to supply a WMI query, which is a WMI Query Language WQL string that can return a value of TRUE when applied to the correct Windows version.

Configure loopback processing

By default Group Policy is applied depending on where both the user and the computer objects are located. If you want to have policy applied based only on the location of the computer object, the Group Policy loopback feature may be of great use, assuming your client computers are at least Windows 2000. With Merge Mode, the computer's GPOs have higher precedence than the user's GPOs. With Replace Mode, the user's list of GPOs is never gathered so only the computer's GPOs are used.

Configure and manage slow-link processing

When processing GPO over a slow link, not all components are processed. A rate that is slower than 500 Kbps is considered a slow link. You may use the Group Policy Object Editor to specify settings for slow link detection for computers (you want to pay attention to the Allow processing across a slow network connection policy option). The options that are available for processing include IP Security policy, EFS recovery policy, Internet Explorer Maintenance policy, Scripts policy and Folder Redirection policy.

Configure client-side extension (CSE) behavior

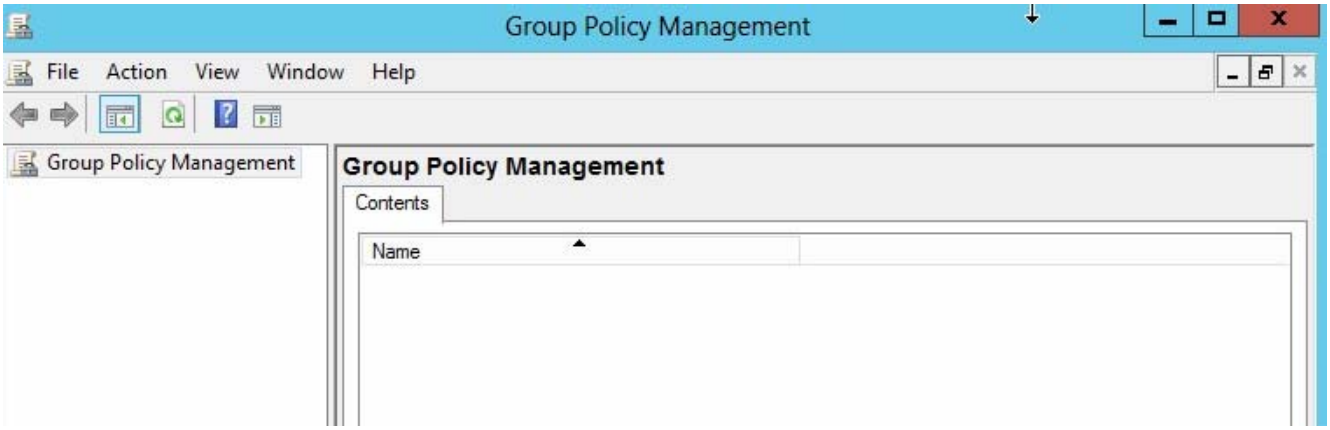
Client-side extensions (CSE) are almost always implemented as .dll files. They are for processing and applying Group Policy settings at the target computers. With each CSE the GPO processing order is determined by obtaining a list of GPOs. A computer policy can be used to control the behavior of the CSE. You may set a computer policy accordingly via the Group Policy Object Editor. The possible computer policy options you can configure are Allow processing across a slow network connection (which should be used with Group Policy slow link detection), Do not apply during periodic background processing (the policy is applied both at boot time and regularly every 90 minutes), and Process even if the Group Policy objects have not changed.

6.2 CONFIGURE GROUP POLICY SETTINGS

Configure settings including software installation, folder redirection, scripts, and administrative template settings

You may use Group Policy to configure computer and user settings on networks based on the **Active Directory Domain Services (AD DS)**. For Group Policy to work, your network must be based on AD DS and that the computers you want to manage must be joined to the domain. You must also have the relevant permissions to create and edit the policy objects. Although you may configure Group Policy settings locally, you should avoid doing so since domain-based Group Policy can centralize management while localized policy cannot.

You may manage all aspects of Group Policy via the **Group Policy Management Console (GPMC)**.



Import security templates

You may want to deploy **security templates** through importing them into a GPO. First you should create OUs for the different types of computers that are to use a different security template. Then you add the computer accounts for these computers to the proper OU. Finally you add a link to a GPO for each of these computer OUs. You can always import a security template into a GPO via the Group Policy Object Editor.

Import custom administrative template file

Administrative Templates for GPOs can be used to set and control registry settings. Administrative Template files are XML based for defining registry-based Group Policy settings that can be configured via the Group Policy Management Editor. With the language-neutral ADMX file it is possible to determine the number, types and locations of policy settings by category in the editor. ADML files, on the other hand, are for supplying language-specific information to the ADMX files. Note that when you use GPEDIT.msc to launch the Group Policy Object Editor, it will automatically read all ADMX files that are stored in the %systemroot%\PolicyDefinitions\ folder.

Convert administrative templates using ADMX Migrator

The **ADMX Migrator** utility is a free MMC snap in tool you can use to convert legacy ADM files into the new ADMX format. You can also use the ADMX Migrator's ADMX Editor to edit ADMX file via a GUI. This tool can be downloaded from:
http://www.microsoft.com/en-hk/download/details.aspx?id=15058

The tool requires .NET framework 2.0 at the least. The minimum OS version required is Windows XP SP 2.

Configure property filters for administrative templates

From within the GPMC you may change the criteria for displaying Administrative Template policy settings using property filters. The available property filters are Managed, Configured and Commented. Keep in mind, with the Managed filter the Group Policy service will only govern Managed policy settings. In terms of policy state, a policy setting can be Not Configured (the default), Enabled , and Disabled. The Commented property also has several states, which include Any , Yes , and No.

6.3 Manage Group Policy objects (GPOs)

Back up, import, copy, and restore GPOs

From within the GPMC console tree you can do a lot of things. For example, you can right-click **Group Policy Objects** in the forest and domain in which you want to create a GPO and then click New to create a new object. You may also choose to copy, backup, restore or import GPOs via the console. You use Backup-GPO to make a backup of a GPO. You use the Restore Group Policy Object Wizard or the Restore-GPO cmdlet to restore a GP that has been backed up. You use the Import Settings Wizard to import a GPO from another domain or forest (you may need to update some references by hand). And you may use Copy-GPO to make a GPO copy. To delete one, use Remove-GPO (all links to it will be deleted as well).

Create and configure Migration Table

When you copy or import a GPO from another domain you rely on a migration table to tell how the domain-specific data should be handled. From the GPMC you can open the Migration Table Editor. You may validate your migration table by choosing Tools - Validate. Or you may auto-populate a migration table (by scanning a GPO) by choosing Tools - Auto-populate from GPO. All migration tables store mapping information as XML file with an extension of .migtable.

Reset default GPOs

You are not supposed to modify the default GPOs. However, if you did and you want to fix them by restoring them to the default value, you should use the dcgpofix command with the /target parameter specified.

Delegate Group Policy management

You may delegate some Group Policy tasks to other people. The GPMC (there is a tab named Delegation) offers several categories of Allowed Permissions on a GPO, including Read; Edit settings; Edit, delete, modify security; Read (from Security Filtering) and Custom. You can fine tune these for proper delegation. Note that the right to create new GPOs can only be delegated at the domain's Group Policy Objects container or the Starter GPOs container.

6.4 CONFIGURE GROUP POLICY PREFERENCES

Configure Group Policy Preferences (GPP) settings including printers, network drive mappings, power options, custom registry settings, Control Panel settings, Internet Explorer settings, file and folder deployment, and shortcut deployment

Group Policy Preferences (GPP) can simplify the deployment and standardization of configurations. Preferences are settings that can be changed by users later (in other words, it only sets an initial state for an application configuration). . You can also use GPP to configure applications that are not Group Policy-aware. GPP is considered quite powerful since it can be used to change or remove registry setting, file, folder, and shortcut... etc. Keep in mind, the preference value can remain in the local registry and can overwrite the application's configuration settings.

Configure item-level targeting

Item-level targeting (which is part of the Common Properties with the GPMC) is a feature that can be used with GPP. You use it to set sophisticated targeting for each individual preference configured in a GPO. In other words, you use it to change the scope of individual preference items. Each targeting item has a value which is either true or false. You can use multiple targeting items to a preference item and you can use AND or OR to combine them.