**Administering Windows Server 2012**

Òco †Zvgvi cÖf‚i bv‡g whwb †Zvgv‡K m„wó K‡i‡QÓ



**Abdur Razzak**

**MCSA**

**IT Professional Diploma in Networking Technologies**

**BSc (Hon’s) & MSc in Mathematics (Both 1st Class)**

**Mobile: 01723090660, 01535114660**

**Email: a.razzak660@gamil.com  
Website: www.selftics.net**

|  |  |  |  |
| --- | --- | --- | --- |
| **INDEX** | | | |
| **Article** | **Topic** | | **page** |
| Chapter-1 | Deploying and updating Windows Server 2012 | |  |
| Lesson-1 |  |  |  |
| Lesson-2 |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-2 | Managing account policies and service accounts | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-3 | Configuring name resolution | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chpter-4 | Administering Active Directory | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-5 | Managing Group Policy application and infrastructure | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-6 | Group Policy settings and preferences | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-7 | Administering network policies | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-8 | Administering remote access | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-9 | Managing file services | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Chapter-10 | Monitoring and auditing Windows Server 2012 | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  | |  |
|  |  |  |  |

**Chapter-4: Administering Active Directory**

**FSMO Roles:**

There are five operations mastersin a single domain Active Directory forest. Two of these operations masters are unique and can be held by only a single computer in the forest. Three operations masters are present in each domain in the forest.

* You can determine the location of the forest-level operations masters by running the get-AdForest cmdlet.
* You can determine the location of the domain-level operations masters by running the get-ADDomain cmdlet.
* You can also determine the location of the domain-level operations masters by right-clicking  
  the domain in Active Directory Users And Computers and then clicking Operations Masters.

**Five operations masters:**

1. **Schema master:**

The domain controller that hosts the *schema master* role is responsible for processing updates to the Active Directory schema. This forest-level FSMO is present on a domain controller in the forest root domain. Some products that need to update the Active Directory schema, such as Microsoft Exchange, must run in the same site as the schema master. Other products that need to update the schema may need to run on the computer that hosts the schema master.  
You can locate the schema master using the Active Directory Schema snap-in for the Microsoft Management Console (MMC). This snap-in is available only if you register the schmmgmt.dll by running the following command from an elevated command prompt:  
Regsvr32.exe Schmmgmt.dll

1. **Domain naming master:**

The *domain naming master* is a forest-level FSMO role, meaning that there is only one domain controller that holds this role in an Active Directory forest. The domain naming master is responsible for managing the addition and removal of domains and application partitions in the forest. The computer that hosts this role is also responsible for handling references to domains in forests that have a trust relationship with the source forest. You can move the domain naming master role using the Operations Master dialog box, available through the Active Directory Domains And Trusts console.

1. **PDC emulator:**

The PDC emulatoris a domain-based role that manages the following:  
**i. Changing domain account passwords:** The PDC emulator ensures that password changes replicate to other domain controllers as soon as possible.  
**ii. Time synchronization across domain members:** As PDC emulators in child domains in a forest perform time synchronization against the PDC emulator in the root domain, you should ensure that you configure the PDC emulator in the root domainto perform time synchronization against a trusted external time source. Doing this ensures that all computers in the forest keep correct time.

**iii. Group Policy changes:** The PDC emulator ensures that there are no conflicts in the event that the same Group Policy Object (GPO) is being edited by two or more different people at the same time.

**iv. Domain master browser:** The PDC emulator provides clients with a list of workgroups and domains when the client is browsing the network.

1. **Infrastructure master:**

The domain controller that holds the *infrastructure master* role keeps track of changes made in other domains in the forest and their impact on objects in the local domain. There is a domain controller hosting the infrastructure master role in each domain in a forest. Unless each domain controller in a domain also holds the Global Catalog server role for performance reasons, you should avoid placing the infrastructure master role on a domain controller that also functions as a Global Catalog server.

You can move the infrastructure master to another domain controller using the Operations Masters dialog box, which is available by right clicking the target domain in Active Directory Users And Computers.

1. **RID master:**

The *RID master* is a domain-level FSMO role that processes requests for relative identifiers (RIDs). Whenever a user, group, or computer account is created on a domain controller, that object is assigned a security identifier (SID). SIDs consist of both a domain SID and a unique RID generated by the RID master. When moving objects between domains using tools including movetree.exe, you must perform the move on the domain controller that holds the RID master role for the source domain.

You can move the RID master to another domain controller using the Operations Masters dialog box, which is available by right-clicking the target domain in Active Directory Users And Computers.

**Summary of FSMO roles:**

1. Schema master controls updates to the schema.
2. The domain naming master manages additions and removals of domains in the forest.
3. The PDC emulator processes password changes and manages time synchronization.
4. The infrastructure master keeps track of changes made in other domains that affect objects in the local domain.
5. The RID master processes requests for relative IDs.

**Global Catalog servers:**  
*Global Catalog servers* provide information on universal group membership in forests that have multiple domains. When a local domain controller authenticates users, it uses the Global Catalog server to determine whether the user account it is authenticating is a member of any universal groups. Global Catalog servers are extremely important in environments in which you have deployed products such as Microsoft Exchange.  
The first domain controller in a new domain is a Global Catalog server by default. You can configure a domain controller to be a Global Catalog server in the Domain Controller Options page of the Active Directory Domain Services Configuration Wizard.

**Global Catalog servers:** Global Catalog servers assist with determining the universal group membership of user accounts in multiple-domain forests.

■ Use UGMC for branch offices that have fewer than 100 users.

**Read-only domain controllers:**  
A read-only domain controller (RODC) is a special type of domain controller that stores the passwords of only some users, but not all. You deploy a RODC when you are concerned about the physical security of a domain controller. For example, suppose that you need to have a domain controller at a branch office site, but the branch office site doesn’t have a special secure locked server room, and the local servers instead sit in a cabinet in the same room that holds the shared printer, photocopier, and fax machine.

■ You can control password replication to RODCs by configuring RODC password replication policy.

■ Cloning domain controllers requires that the virtualization platform supports VM-GenerationID, the domain controller must be running Windows Server 2012, and the PDC emulator must be online and also running Windows Server 2012.  
■ The source domain controller must be a member of the Cloneable Domain Controllers security group

**Q.** Which FSMO role is responsible for processing account password changes in a domain?  
**Answer:** The PDC emulator role is responsible for processing account password changes in a domain.

Q. What console can you use to configure a domain controller as a Global Catalog server or enable UGMC at a site?

**Answer:**  
You use the Active Directory Sites And Services console to configure a domain controller as a Global Catalog server or enable UGMC at a site.

**Chapter-8: Administering remote access**

Lesson-1:

1. What is RADIUS server?

Ans. A RADIUS serverperforms authentication, authorization, and accounting for VPN, 802.1x wireless access point and authenticating switches, and dial-up connections. The Network Policy Server (NPS) role is Microsoft’s implementation of a RADIUS server.

Or,

A RADIUS server performs authentication and authorization for traffic forwarded to it  
from a RADIUS client.

NPS is the Windows Server 2012 role that enables Windows Server 2012 to function as  
a RADIUS server.

1. **RADIUS proxy:**  
   A RADIUS proxy forwards traffic from RADIUS clients to RADIUS servers. A RADIUS  
   proxy can forward traffic to different RADIUS servers based on the properties of the traffic.
2. What is the main difference between a RADIUS server and a RADIUS proxy?

Ans. A RADIUS proxy forwards authentication and authorization requests to a RADIUS server. A RADIUS server performs authentication and authorization tasks.

1. Define RADIUS clients.

Ans. A RADIUS client is a device that sends authentication and authorization traffic to a RADIUS server. A VPN server can be a RADIUS client.

1. Define RADIUS accounting.

Ans. RADIUS accounting records authentication and authorization request data. RADIUS accounting data can be written to the event log, to a local log file, or to an SQL Server database.

**Lesson-2:**

The Routing And Remote Access role enables you to configure a computer running Windows Server 2012 to provide dial-up, VPN, NAT, and LAN routing services.

**VPN protocols:**

A Windows Server 2012 VPN server supports four VPN tunneling protocols. They are:

1. IKEv2
2. SSTP
3. L2TP/IPSec
4. PPTP

Note:

* You can use the PPTP or L2TP/IPSec protocols if you need to support VPN clients  
  running the Windows XP operating system.
* SSTP is supported only on clients running the Windows Vista, Windows 7, and Windows 8 client operating systems.
* IKEv2 is supported only on clients running the Windows 7 and Windows 8 client operating  
  systems.

**Network Address Translation (NAT):**

Network Address Translation(NAT) enables you to share an Internet connection with computers on an internal network. In a typical NAT configuration, the NAT server has two network interfaces. One network interface is connected to the Internet; the second network interface  
connects to a network with a private IP address range.

■ NAT enables a single Internet connection to be shared by multiple computers.  
■ LAN routing enables the routing of network traffic between subnets. LAN routing supports routing of both IPv4 and IPv6 traffic.  
■ The SSTP VPN protocol uses HTTPS to carry VPN traffic. It can be used in firewalled environments that block other VPN protocols.  
■ IKEv2 supports VPN reconnect. VPN reconnect enables disrupted VPN connections to  
be reestablished up to 8 hours later without requiring user re-authentication.

**Lesson-3:**

1. **What do you understand DirectAccess?**

**Ans.** DirectAccess is an always-on, computer-authenticated IPv6 VPN connection that becomes  
active any time a client computer can establish an Internet connection when on an untrusted network.

■Any IPv6-capable application on the DirectAccess client has full access to resources on the trusted network.

**Network Location Server**:  
The Network Location Server (NLS) is a specially configured server that enables clients to determine whether they are on a trusted or an untrusted network.

■DirectAccess clients send traffic to the NLS server to determine whether they are located on the trusted network or on the Internet.  
■ You need to install an SSL/web server certificate from a trusted CA on the NLS server  
and the DirectAccess server.  
■ You must remove ISATAP from the DNS global query block list on all DNS servers in  
order to use DirectAccess.

■ A DirectAccess Edge deployment requires two network adapters. One adapter is connected to the Internet; the other to an internal trusted network.  
■ A DirectAccess server can be deployed behind an edge device, such as a firewall, with  
one or two network adapters.  
■ The DirectAccess server must be a member of an Active Directory domain.  
■ If deployed behind a NAT device, DirectAccess can use only IP over HTTPS.  
■ DirectAccess can be deployed with a single public IPv4 address.  
■ To support two-factor authentication or one-time password, the DirectAccess server  
requires two consecutive public IPv4 addresses.  
■ Only computers running Windows 8 Enterprise edition and Windows 7 Enterprise and  
Ultimate editions can be configured to use DirectAccess.  
■ DirectAccess clients must be members of an Active Directory domain. It is possible to  
configure remote domain join with DirectAccess.

**Chapter-9: Managing file services**

Lesson 1:

1. **What are Quotas?**

Ans. Quotas enable you to control the amount of storage space (data) consumed by a user on a volume, folder tree, or individual folder.

Or, Quotas enable you to limit the amount of data that can be written to a specific path.

1. **What is the different between a hard quota and a soft quota?**

Ans. The difference between a hard quota and a soft quota is as follows:  
■ A hard quota blocks users from exceeding the specified limit. They can’t write additional data to the folder tree to which the quota template applies.  
■ A soft quota doesn’t block users from exceeding the specified limit.

**Note:**

* In previous versions of the Windows server operating system, NTFS quotas enabled you to apply quotas on a per-volume basis.
* FSRM quotas are more sophisticated, enabling you to apply different quotas to different folder trees on the same volume.
* Quotas are path based, you can have different and separate quotas applied on the same volume.

1. **What are file screens?**

Ans. File screens enable you to block users from writing specific types of files, on the basis of the file name extension to volumes, folder trees, or individual folders.

You apply file screens to shared folders by applying them to the folder on the file server that is associated with the shared folder.

**Note:**

* You configure file screens by selecting a specific file group to the screen or by selecting a file screen template and applying it to a specific location.
* A file group is a collection of file types associated with a particular kind of file. For ex- ample, the Image Files file group includes the file extensions associated with common image file formats such as .bmp, .jpg, .gif, and .png.
* You can edit which file extensions are associated with existing file groups or create custom file groups.
* A file screen exception enables you to create an exemption to an existing file screen.

1. **You want to allow file types to be written to a subfolder that are blocked by a file screen applied to the folder. How can you accomplish this goal?**  
   **Ans.** Configure a file screen exception.
2. **What is File classification? 486p**

Ans. File classification enables you to apply metadata to files based on file properties.

Note:

File classification properties can use one of the following property types:

* **Yes/no** A Boolean value of either YES or NO. When multiple values apply, NO overrides YES.
* **Date-Time** A date and time property.
* **Number** A numeric property.
* **Multiple Choice List** A list of values that can be assigned to a property. Multiple  
  values are allowed.
* **Ordered List** A fixed list of values. If multiple values apply, the one closest to the top of the list is used.
* **String** A text string that can be assigned to the property.
* **Multi-string** A list of strings that can be assigned to a property.

1. What are file management tasks?

Ans. File management tasks enable you to perform tasks on files based on the file metadata.

1. What is report?

Ans. A Storage report enables you to generate information about the type and nature of files stored on a storage server. Storage reports give you the information that you need to configure effective file screens and quotas.

Lesson-2:

1. What is DFS?

Ans. A Distributed File System (DFS) enables you to create a unified namespace that users can browse when attempting to locate a specific network folder. You can also use a DFS to create replicas of important shared folders.

Or, DFS enables you to simplify the location of shared folders by enabling their placement under a single tree.

1. What are DFS namespaces?

Ans. DFS namespaces enable you to group shared folders hosted on different servers into one or  
more logical namespaces.

There are two types of DFS namespaces that you can create on computers running Windows Server 2012

1. Domain-based namespace
2. Stand-alone namespace
3. **What is Domain-based namespace?**

A domain-based DFS enables you to deploy multiple namespace servers for redundancy.

Or, Domain-based DFS namespaces are stored in Active Directory, and you deploy them when  
you need to ensure that the namespace remains available, even if one of the servers hosting  
the namespace is offline.

1. **What are Stand-alone namespaces?**

Ans. Stand-alone namespaces enable you to deploy a DFS on file servers that are not members of an Active Directory domain. You can also deploy a stand-alone namespace on a server that is a member of an Active Directory domain.

**Note:**  
■ If a domain is at the Windows Server 2008 or higher functional level, and the forest is at the Windows Server 2003 functional level, you can implement Windows 2008 mode.  
■ A Windows 2008 domain-based DFS enables up to 50,000 folder targets, access-based enumeration, and remote differential compression.

You can deploy two types of domain-based namespace: Windows 2008 mode or Windows 2000 mode. Windows 2008 mode provides better features, increasing the number of folder targets from 5,000 to 50,000 and providing support for accessed-based enumeration. The 50,000 folder targets supported by domain-based namespaces can all be located on the same server or spread across up to 50,000 file servers, although this would limit each server to a single folder.  
■ Stand-alone mode enables you to support up to 50,000 folder targets, but does not provide redundancy for namespace servers.

Stand-alone DFS namespaces support up to 50,000 folders spread across up to 50,000 separate servers. You might consider deploying a standalone DFS namespace when you need to support more than 5,000 DFS folders, but you can’t deploy a domain-based DFS because the domain isn’t at the Windows Server 2008 or higher functional level.

1. **What is DFS replication?**   
   Ans. DFS replication enables you to configure folder replication so that folder replicas remain synchronized. The default is for replication to occur 24 hours per day and to use all available bandwidth.
2. **What is Replication topology?**

Ans. Replication topology determines how DFS servers that are members of a replication group communicate with each other. When you create a replication group, you need to decide which topology you will use. There are two replication topologies:

1. Hub And Spoke
2. Full Mesh

■ Hub and spoke mode is appropriate for replication groups in which updates occur on few servers and replication topology must be managed.  
■ Full mesh topology is appropriate for replication groups that have fewer than 10 members.

7. What are Replication schedules?

Ans. Replication schedules enable you to configure replication times and how much bandwidth is allocated to replication.

Lesson-3:

1. What is encryption?

Ans. Encryption enables you to protect data from being accessed by unauthorized people. Unlike file and folder permissions, which are often incorrectly applied, decryption of encrypted data can occur only if a user or computer has access to the correct private key.

1. What is BitLocker?

Ans. BitLocker is a full-volume encryption and boot environment protection technology. By deploying BitLocker, you can ensure that a nefarious third party can’t use a USB boot device to boot a computer in your organization and extract data from the hard disk, or simply remove the hard disk for later data extraction.

Or,

BitLocker provides a full volume encryption solution that is transparent to users of the operating system.

1. **What is BitLocker Network Unlock?**

Ans. BitLocker Network Unlock enables computers configured for BitLocker that are connected  
to the internal wired network to bypass the requirement to enter the PIN or password. BitLocker  
Network Unlock works only if the computer is connected to the internal wired network and  
only if the computer meets a specific set of hardware requirements.

Or,   
BitLocker Network Unlock enables computers connected to a wired network to bypass the requirement for entering a password or PIN at startup.

■ BitLocker Network Unlock requires computers that support UEFI DHCP. It also requires the deployment of the BitLocker Network Unlock role, DHCP, WDS, and specially prepared certificates.  
■ BitLocker recovery passwords and keys can be backed up to Active Directory.  
■ You can confiure a DRA for BitLocker, which enables data recovery on BitLockerprotected drives without needing to enter a specific recovery key.

1. What type of network connection must a computer have to use BitLocker Network  
   Unlock?

Ans. A computer must have a wired Internet connection to use BitLocker Network Unlock.

1. What type of network connection must a computer have to use BitLocker Network  
   Unlock?

Ans. A computer must have a wired Internet connection to use BitLocker Network Unlock.

What is Encrypting File System?

Ans. The EncryptingFile System (EFS) enables per-user encryption of files and folders. EFS has been  
available in Windows operating systems since the release of Windows 2000 and has supported encrypting files for multiple users since the release of Windows XP. When a user encrypts a file using EFS, only that user and a user who holds a DRA certificate (if one is configured) can read the contents of that file.

* EFS is supported only on NTFS file system volumes; you can’t use EFS on ReFS volumes.
* You also can’t use EFS on FAT and FAT32-formatted volumes.
* EFS enables file- and folder-level encryption.
* You can configure a DRA for EFS. The DRA can access all EFS encrypted data.
* If you configure a custom certificate template for EFS, you can configure a KRA.
* This enables individual EFS private keys to be recovered from the certificate services database, enabling the decryption on a per-user basis.

**Access-based enumeration:** Access-based enumeration enables users to see only files and folders they have permissions set up on. Without access-based enumeration, users can’t see files and folders they can’t open.

**Chapter-10: Monitoring and auditing Windows Server 2012**

Lesson-1:

1. What are Data collector sets?

Ans. Data collector setsenable you to collect performance counter data, system configuration information, and statistics into a single file. You can use Performance Monitor or other third-party tools to analyze this information to make a determination about how well a server is functioning against an assigned workload.

**Or,** Data collector sets enable you to collect performance counter data, event trace data, and system configuration information.

**You can configure data collector sets to include the following:**

1. Performance counter data
2. Event trace data
3. System configuration information
4. Active Directory Diagnostics
5. System Diagnostics
6. System Performance
7. What are Performance counter alerts?

Ans. Performance counter alerts enable you to configure a task to run when a performance counter, such as available disk space or memory, falls under or exceeds a specific value.

Note: To configure a performance counter alert, you create a new data collector set, choose the Create  
Manually option, and select the Performance Counter Alert option.

1. What is Event Viewer?

Event Viewer enables you to access recorded event information.

Note: The Windows Server 2012 Event Viewer differs from the Event Viewer in earlier versions of the Windows Server operating system, such as Windows Server 2003, in that it not only offers the application, security, setup and system logs but it also contains separate application and service Logs.

1. You want to view specific events across multiple event logs. What tool should you  
   use to accomplish this goal?

Ans. You should use custom views.

1. **What do you mean Network monitoring?**

Ans. Network monitoring enables you to track how a computer interacts with the network. Through network monitoring, you can determine which services and applications are using specific network interfaces, which services are listening on specific ports, and the volume of traffic that exists.

There are two primary tools through which you can perform network monitoring on computers running Windows Server 2012:  
■ Resource Monitor  
■ Message Analyzer

1. **What is Resource Monitor?**

Resource Monitor enables you to monitor how a computer running the Windows Server 2012 operating system uses CPU, memory, disk, and network resources. Resource Monitor provides real time information.

**Note**: You can’t use Resource Monitor to perform a traffic capture and review activity that occurred in the past. You can use Resource Monitor to view activity that is currently occurring.

■ Performance counter alerts enable an event to be written to the event log and a command to be run when a specified performance counter exceeds or falls below a configured value.  
■ Event log filters apply to a single event log and are not persistent.  
■ Event log views are persistent, can include items from multiple event logs, and can be  
imported and exported.  
■ Event subscriptions enable you to configure one computer to consolidate the event  
logs of multiple computers.  
■ Event-driven tasks enable you to configure a program or script to be run when a specific event is written to the event log.  
■ Message Analyzer, which is the successor to Network Monitor, enables you to capture  
and analyze network traffic.

Lesson-2:

1. What are advanced audit policies?

Ans. Advanced audit policies enable you to perform more granular auditing than is possible with the traditional auditing policies available in earlier versions of Windows server.

1. What are expression-based audit policies?

Ans. Expression-based audit policies enable you to configure auditing based on object metadata. You can also use expression-based audit policies to perform conditional auditing.

■ After you have enabled the auditing of object access, you can configure auditing at the file and folder level. File- and folder-level auditing supports expression-based audit policies.

**3. Why do we use auditpol.exe command?**

Ans. We can use the auditpol.exe command-line utility from an elevated command prompt to configure and manage audit policy settings.

**Short Note:**

1. **WDS**

Windows Deployment Services enables you to deploy Windows operating systems. You can use it to set up new computers by using a network-based installation. This means that you do not have to install each operating system directly from installation media, for example a DVD or USB drive.

1. **capture image**

A special image type that enables a prepared computer to be booted so that its operating system state can be captured as an install image. You add capture images as boot images in WDS.

1. **discover image**

This special image is for computers that cannot PXE boot to load

appropriate network drivers to begin a session with a WDS server.

1. **guest operating system**

A guest OS is an operating system (OS) that is installed in a virtual machine or disk partition in addition to the host or main OS.

1. **host operating system**

A host operating system (OS) is the original OS installed on a computer

**Or**

A host operating system is the primary operating system (OS) installed on a computer system's hard drive. In most cases, there is only one host OS. Other OSs, known as virtual OSs, may operate within the host OS

1. **install image**

The main type of image discussed in this chapter. Contains the operating system as well as any other included components, such as software updates and

additional applications. A default install image, named Install.wim, is present in the

sources folder of the Windows Server 2012 installation media.

1. **boot image**

A special image that enables the computer to boot and begin installing

the operating system using the install image. A default boot image, named Boot.wim,

is located in the sources folder of the Windows Server 2012 installation media.

1. **Data collector set**

A Data Collector Set is the building block of performance monitoring and reporting in Windows Performance Monitor. It organizes multiple data collection points into a single component that can be used to review or log performance. A Data Collector Set can be created and then recorded individually, grouped with other Data Collector Set and incorporated into logs, viewed in Performance Monitor, configured to generate alerts when thresholds are reached, or used by other non-Microsoft applications. It can be associated with rules of scheduling for data collection at specific times. Windows Management Interface (WMI) tasks can be configured to run upon the completion of Data Collector Set collection.

1. **Security Templates**

A security template contains hundreds of possible settings that can control a single or multiple computers. The security templates can control areas such as user rights, permissions, and password policies. Security templates can be deployed centrally using Group Policy objects (GPOs). Finally, security templates can be customized to include almost any security setting on a target computer.

1. **Root Hints**

You can use root hints to prepare servers that are authoritative for non root zones so that they can discover authoritative servers that manage domains at a higher level or in other sub trees of the DNS domain namespace. These root hints are essential for servers that are authoritative at lower levels of the namespace when locating and finding other servers under these conditions.

***or***

The root hints file , also called the cache hints file , contains host information that is needed to resolve names outside of the authoritative DNS domains. It contains the names and addresses of root DNS servers.

1. **dynamic updates**

Dynamic update enables DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use DHCP to obtain an IP address.

1. **Forwarder**

A forwarder is a Domain Name System (DNS) server on a network used to forward DNS queries for external DNS names to DNS servers outside of that network. You can also forward queries according to specific domain names using conditional forwarders.

1. **Conditional Forwarder**

A conditional forwarder is a Domain Name System (DNS) server on a network that you use to forward DNS queries according to the DNS domain name in the query. For example, you can configure a DNS server to forward all the queries it receives for names ending with widgets.contoso.com to the IP address of a specific DNS server or to the IP addresses of multiple DNS servers.

1. **fully qualified domain name (FQDN)**

A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN for a hypothetical mail server might be mymail.somecollege.edu. The hostname is mymail, and the host is located within the domain somecollege.edu.

1. **MX record**

A **mail exchanger record** (**MX record**) is a type of [resource record](http://en.wikipedia.org/wiki/Resource_record) in the [Domain Name System](http://en.wikipedia.org/wiki/Domain_Name_System) that specifies a [mail server](http://en.wikipedia.org/wiki/Mail_server) responsible for accepting [email](http://en.wikipedia.org/wiki/Email) messages on behalf of a recipient's domain, and a preference value used to prioritize mail delivery if multiple mail servers are available. The set of MX records of a domain name specifies how email should be routed with the [Simple Mail Transfer Protocol](http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) (SMTP).

**Or**

**What is a mail exchange?**

"Mail exchange" is just another name for the machine whose primary function is receiving and sending email. Also known as mailhost, mailhub, or even postoffice, this machine usually has a mail server (software written specifically for distributing files) listening on port 25 to receive incoming email.

**What is an MX record?**

An MX (Mail eXchange) record will redirect email sent to any user's machine (**joe@norbert.dept1.cornell.edu**, for example) to a designated mailhost. It tells the MDA where to route email.  
  
The MX record uses preference values to specify the routing order--low value = high priority. In the example below, when mail is sent to **norbert.dept1.cornell.edu** the MDA (see Mail Delivery Agent above) tries to reroute the mail to **mailhost.dept1.cornell.edu** which has the lowest value, and therefore the highest priority. If that fails, it tries **mailhost2.dept1.cornell.edu** and finally **mailhost3.dept1.cornell.edu**.

1. **Host A, AAAA record**
2. **CNAME**
3. **PTR record**

**SOA (Start of Authority) Indicates that the server is the best authoritative source**

**for data concerning the zone. Each zone must have an SOA record and only one SOA**

**record can be in a zone.**

**■ ■ NS (Name Server) Identifies a DNS server functioning as an authority for the zone.**

**Each DNS server in the zone (whether primary master or secondary) must be represented by an NS record.**

**■ ■ A (Address) Provides a name-to-address mapping that supplies an IPv4 address**

**for a specific DNS name. This record type performs the primary function of the DNS:**

**converting names to addresses.**

**■ ■ AAAA (Address) Provides a name-to-address mapping that supplies an IPv6 address**

**for a specific DNS name. This record type performs the primary function of the DNS:**

**converting names to addresses.**

**■ ■ PTR (Pointer) Provides an address-to-name mapping that supplies a DNS name for**

**a specific address in the in-addr.arpa domain. This is the functional opposite of an A**

**record, used for reverse lookups only.**

**■ ■ CNAME (Canonical Name) Creates an alias that points to the canonical name (that**

**is, the “real” name) of a host identified by an A record. Administrators use CNAME**

**records to provide alternative names by which systems can be identified.**

**■ ■ MX (Mail Exchanger) Identifies a system that will direct email traffic sent to an address in the domain to the individual recipient, a mail gateway, or another mail server**

1. **Aging**
2. **Scavenging**

These features are provided as a mechanism for performing cleanup and removal of stale resource records (RRs), which can accumulate in zone data over time.

With dynamic update, RRs are automatically added to zones when computers start on the network. However, in some cases, they are not automatically removed when computers leave the network. For example, if a computer registers its own host (A) RR at startup and is later improperly disconnected from the network, its host (A) RR might not be deleted. If your network has mobile users and computers, this situation can occur frequently.

1. **primary zone**
2. **secondary zone**
3. **forward lookup zone**

## Forward DNS lookup is using an Internet domain name to find an IP address.

1. **reverse lookup zone**

In most DNS lookups, clients typically perform a forward lookup, which is a search based on the DNS name of another computer as stored in an address (A) resource record. This type of query expects an IP address as the resource data for the answered response.

DNS also provides a reverse lookup process, enabling clients to use a known IP address during a name query and look up a computer name based on its address. A reverse lookup takes the form of a question, such as "Can you tell me the DNS name of the computer that uses the IP address 192.168.1.20?"

1. **WINS**

## Role of WINS in the Network

Although NetBIOS and NetBIOS names can be used with network protocols other than TCP/IP, WINS was designed specifically to support NetBIOS over TCP/IP (NetBT). WINS is required for any environment in which users access resources that have NetBIOS names. If you do not use WINS in such a network, you cannot connect to a remote network resource by using its NetBIOS name unless you use Lmhosts files, and you might be unable to establish file and print sharing connections.

**or**

**Windows Internet Name Service** (WINS) is [Microsoft](http://en.wikipedia.org/wiki/Microsoft)'s implementation of [NetBIOS Name Service](http://en.wikipedia.org/wiki/NBNS) (NBNS), a name server and service for [NetBIOS](http://en.wikipedia.org/wiki/NetBIOS) computer names. Effectively, WINS is to NetBIOS names what [DNS](http://en.wikipedia.org/wiki/Domain_Name_System) is to [domain names](http://en.wikipedia.org/wiki/Domain_name) — a central mapping of host names to network addresses. Like the DNS, it is implemented in two parts, a server service (that manages the [embedded Jet Database](http://en.wikipedia.org/wiki/Microsoft_Jet_Database_Engine), server to server replication, service requests, and conflicts) and a [TCP/IP](http://en.wikipedia.org/wiki/TCP/IP) client component which manages the client's registration and renewal of names, and takes care of queries.

1. **Firewall**
2. **Windows Server Update Services (WSUS)**

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

1. **Fine-grained password policy**

The Windows Server operating system provides organizations with a way to define different password and account lockout policies for different sets of users in a domain.

1. **Kerberos policy**

Kerberos policy is defined at the domain level and is implemented by the domain's Key Distribution Center. Kerberos policy is stored in Active Directory as a subset of the attributes of domain security policy. By default, policy options can be set only by members of the Domain Admins group.

**Or**

Kerberos policies are used for domain user accounts. They determine Kerberos-related settings, such as ticket lifetimes and enforcement. Kerberos policies do not exist in Local Computer Policy.

1. **Internet Protocol Security (IPsec)**

Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on Internet Engineering Task Force (IETF) standards.

1. **Rodc**

Read-only domain controllers (RODCs) are a new feature of Active Directory Domain Services (AD DS) in Windows Server 2008. RODCs are additional domain controllers for a domain that host complete, read-only copies of the partitions of the Active Directory database and a read-only copy of the SYSVOL folder contents. By selectively caching credentials, RODCs address some of the challenges that enterprises can encounter in branch offices and perimeter networks (also known as DMZs) that may lack the physical security that is commonly found in datacenters and hub sites. RODCs also offer a number of manageability improvements that are described in this guide. This section describes how RODCs work with the rest of the Active Directory environment, the main differences between RODCs and writable domain controllers, and the RODC features that can help resolve a number of security or manageability issues.

1. **Vpn**

A **virtual private network** (**VPN**) extends a [private network](http://en.wikipedia.org/wiki/Private_network) across a [public](http://en.wikipedia.org/wiki/Public) network, such as the [Internet](http://en.wikipedia.org/wiki/Internet). It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.[[1]](http://en.wikipedia.org/wiki/Virtual_private_network#cite_note-1) A VPN is created by establishing a virtual [point-to-point](http://en.wikipedia.org/wiki/Point-to-point_%28network_topology%29) connection through the use of dedicated connections, virtual [tunneling protocols](http://en.wikipedia.org/wiki/Tunneling_protocols), or traffic encryptions. Major implementations of VPNs include [OpenVPN](http://en.wikipedia.org/wiki/OpenVPN) and [IPsec](http://en.wikipedia.org/wiki/IPsec).

1. **Routing**

**Routing** is the process of selecting best paths in a network. In the past, the term routing was also used to mean forwarding network traffic among networks. However this latter function is much better described as simply forwarding. Routing is performed for many kinds of networks, including the [telephone network](http://en.wikipedia.org/wiki/PSTN) ([circuit switching](http://en.wikipedia.org/wiki/Circuit_switching)), [electronic data networks](http://en.wikipedia.org/wiki/Computer_network) (such as the [Internet](http://en.wikipedia.org/wiki/Internet)), and [transportation networks](http://en.wikipedia.org/wiki/Transport_network). This article is concerned primarily with routing in electronic data networks using [packet switching](http://en.wikipedia.org/wiki/Packet_switching) technology.

1. **RADIUS Server**

**Remote Authentication Dial In User Service** (**RADIUS**) is a networking [protocol](http://en.wikipedia.org/wiki/Communications_protocol) that provides centralized Authentication, Authorization, and Accounting ([AAA](http://en.wikipedia.org/wiki/AAA_protocol)) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the [Internet Engineering Task Force](http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF) standards.[[](http://en.wikipedia.org/wiki/RADIUS#cite_note-Vollbrecht2006-1)

1. **NAT**

NAT enables computers on small- to medium-sized organizations with private networks to access resources on the Internet or other public network.

1. **certification authority (CA)**

A certification authority (CA) is responsible for attesting to the identity of users, computers, and organizations. The CA authenticates an entity and vouches for that identity by issuing a digitally signed certificate. The CA can also manage, revoke, and renew certificates.

1. **Bitlocker**

A certification authority (CA) is responsible for attesting to the identity of users, computers, and organizations. The CA authenticates an entity and vouches for that identity by issuing a digitally signed certificate. The CA can also manage, revoke, and renew certificates.

1. **Efs**

The Encrypting File System (EFS) is a component of the NTFS file system on Windows, it enables transparent encryption and decryption of files by using advanced, standard cryptographic algorithms.

**or**

1. **DRA**

Data recovery agents are accounts that are able to decrypt BitLocker-protected drives by using their smart card certificates and public keys. Recovery of a BitLocker-protected drive can be accomplished by a data recovery agent that has been configured with the proper certificate.

1. **FSRM**

File Server Resource Manager is a suite of tools for Windows Server® 2008 that allows administrators to understand, control, and manage the quantity and type of data that is stored on their servers. By using File Server Resource Manager, administrators can place quotas on folders and volumes, actively screen files, and generate comprehensive storage reports. This set of advanced instruments not only helps the administrator efficiently monitor existing storage resources, but it also aids in the planning and implementation of future policy changes.

1. **Quota**

Windows Server 2008 supports two mutually exclusive methods for setting quotas on the amount of file system resources a user can use—disk quotas or directory quotas. Disk quotas were introduced in Windows 2000, and are applied to specific users and limit the amount of disk space that user can use on a particular volume. Directory quotas are applied to all users and limit the amount of disk space that users can use in a particular folder and its subfolders.

1. **soft quota**
2. **DFS**

## A distributed file system is a client/server-based application that allows clients to access and process data stored on the server as if it were on their own computer.

1. **File Screens**

With File Server Resource Manager (FSRM) you can create file screens that prevent users from saving unauthorized files on volumes or folders.

1. **GPO**

Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory directory service containers: sites, domains, or organizational units (OUs). The settings within GPOs are then evaluated by the affected targets, using the hierarchical nature of Active Directory. Consequently, Group Policy is one of the top reasons to deploy Active Directory because it allows you to manage user and computer objects.

**Evedence Tips:**

1. **Account and Lockout Policy through Security Template with analyze.**
2. **Creating zone and different types of resource record.**
3. **Blocking Control panel through GPO.**
4. **Quota and File screen.**
5. **Windows Backup & restore.**

1. Boot image

2. Capture image

3. Discover image

4. Guest operating system

5. Host operating system

6. Hypervisor

7. Install image

8. WIM File

9. Why we use clustering?

10. Remote Desktop protocol

11. WDS (windows Deployment services)

12. DFS

13. Fine-grained password policies

14. Account Lockout policy

15. WSUS (windows server update services)

16. Primary zone

17. Secondary zone

1. Stub Zone

19. Forward Lookup zone

20. Reverse Lookup zone

21. DNS

22. DNS resource Records

* SOA (start of Authority)
* NS (Name Server)
* A(Address)
* AAAA(Address)
* PTR (Pointer)
* CNAME (Canonical Name)
* MX (Mail Exchanger)

1. DNS Forwarder

24. Conditional forwarder

25. Root Hints

26. Aging

27. Scavenging

28. Caching only name server

29. Round Robin DNS

30. PSO (Password settings objects

31. Difference between Forwarder and Conditional forwarder

32. Quotas

33. The difference between a hard quota and a soft quota.

1. File screens :
2. BitLocker
3. EFS (Encrypting File System)
4. DRA(data recovery agent) and KRA(Key recovery agent)
5. RADIUS servers
6. VPN
7. Direct Access Connection
8. NAT
9. DCS [Data Collector Set]
10. Network Monitoring
11. Resource Monitor
12. Message Analyzer
13. Schema Master
14. Domain naming master
15. Infrastructure master
16. RID Master
17. Global Catalog servers
18. Active Directory Recycle Bin
19. LAN routing
20. Advanced Audit policies
21. Delegation GPO management
22. Folder redirection
23. NPS deployment