

Windows Server 2008 Active Directory Interview Questions Part 1

Q. What is Active Directory?

Active Directory is the directory service used by Windows 2000. A directory service is a centralized, hierarchical database that contains information about users and resources on a network. In Windows 2000, this database is called the *Active Directory data store*. The Active Directory data store contains information about various types of network objects, including printers, shared folders, user accounts, groups, and computers. In a Windows 2000 domain, a read/write copy of the Active Directory data store is physically located on each domain controller in the domain.

Three primary purposes of Active Directory are:

- · To provide user logon and authentication services
- · To enable administrators to organize and manage user accounts groups, and network resources
- · To enable authorized users to easily locate network resources, regardless of where they are located on the network

A *directory service* consists of two parts—a centralized, hierarchical database that contains information about users and resources on a network, and a service that manages the database and enables users of computers on the network to access the database. In Windows 2008, the database is called the Active Directory data store, or sometimes just the directory. The Active Directory data store contains information about various types of network objects, including printers, shared folders, user accounts, groups, and computers. Windows 2000 Server computers that have a copy of the Active Directory data store, and that run Active Directory are called *domain controllers*. In a Windows 2008 domain, a read/write copy of the Active Directory data store is physically located on each domain controller in the domain.

Q. What are the physical components of active directory?

Logical Components of Active Directory

In creating the hierarchical database structure of Active Directory, Microsoft facilitated locating resources such as folders and printers by name rather than by physical location. These **logical building blocks include domains, trees, forests, and OUs**. The physical location of objects within Active Directory is represented by including all objects in a given location in its own site. Because a domain is the basic unit on which Active Directory is built, the domain is introduced first; followed by trees and forests (in which domains are located); and then OUs, which are containers located within a domain.

Domain:

A *domain* is a logical grouping of networked computers in which one or more of the computers has one or more shared resources, such as a shared folder or a shared printer, *and* in which all of the computers share a common central domain directory database that contains user account security information. One distinct advantage of using a domain, particularly on a large network, is that administration of user account security for the entire network can be managed from a centralized location. In a domain, a user has only one user account, which is stored in the domain directory database. This user account enables the user to access shared resources (that the user has permissions to access) located on any computer in the domain.

Active Directory domains can hold millions of objects, as opposed to the Windows NT domain structure, which was limited to approximately 40,000 objects. As in previous versions of Active Directory, the Active Directory database file (ntds.dit) defines the domain. Each domain has its own ntds.dit file, which is stored on (and replicated among) all domain controllers by a process called *multimaster replication*. The domain controllers manage the configuration of domain security and store the directory services database. This arrangement permits central administration of domain

account privileges, security, and network resources. Networked devices and users belonging to a domain validate with a domain controller at startup. All computers that refer to a specific set of domain controllers make up the domain. In addition, group accounts such as global groups and domain local groups are defined on a domain-wide basis.

Trees

A *tree* is a group of domains that shares a contiguous namespace. In other words, a tree consists of a parent domain plus one or more sets of child domains whose name reflects that of a parent. For example, a parent domain named examcram.com can include child domains with names such as products.examcram.com, sales.examcram.com, and manufacturing.examcram.com. Furthermore, the tree structure can contain grandchild domains such as america.sales.examcram.com or europe.sales.examcram.com, and so on, as shown in Figure 1-2. A domain called que.com would not belong to the same tree. Following the inverted tree concept originated by X.500, the tree is structured with the parent domain at the top and child domains beneath it. All domains in a tree are linked with two-way, transitive trust relationships; in other words, accounts in any one domain can access resources in another domain and vice versa.

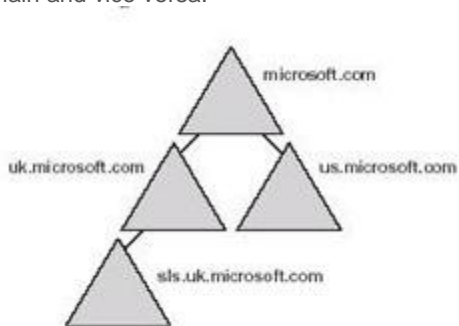


Figure 1-6 A domain tree

Forests

A *forest* is a grouping or hierarchical arrangement of one or more separate, completely independent domain trees. As such, forests have the following characteristics:

- All domains in a forest share a common schema.
- All domains in a forest share a common global catalog.
- All domains in a forest are linked by implicit two-way transitive trusts.

Trees in a forest have different naming structures, according to their domains. Domains in a forest operate independently, but the forest enables communication across the entire organization.

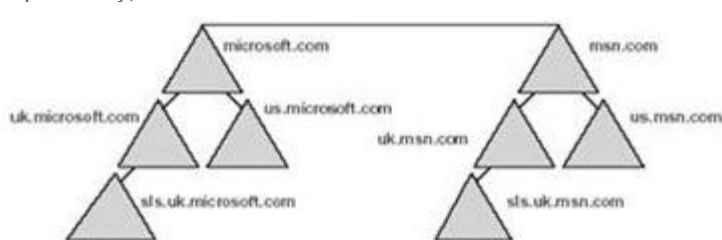


Figure 1-7 A forest of trees

Organizational Unit:

An organizational unit (OU) is a container used to organize objects within one domain into logical administrative groups. An OU can contain objects such as user accounts, groups, computers, printers, applications, shared folders, and other OUs from the same domain. OUs are represented by a folder icon with a book inside. The Domain

Controllers OU is created by default when Active Directory is installed to hold new Microsoft Windows Server 2003 domain controllers. OUs can be added to other OUs to form a hierarchical structure; this process is known as nesting OUs. Each domain has its own OU structure—the OU structure within a domain is independent of the OU structures of other domains.

There are three reasons for defining an OU:

- To delegate administration – In the Windows Server 2003 operating system, you can delegate administration for the contents of an OU (all users, computers, or resource objects in the OU) by granting administrators specific permissions for an OU on the OU's access control list.
- To administer Group Policy
- To hide object

Physical Components of Active Directory

There are two physical components of Active Directory:

- Domain Controllers
- Sites

Domain Controllers

Any server on which you have installed Active Directory is a *domain controller*. These servers authenticate all users logging on to the domain in which they are located, and they also serve as centers from which you can administer Active Directory in Windows Server 2008. A domain controller stores a complete copy of all objects contained within the domain, plus the schema and configuration information relevant to the forest in which the domain is located.

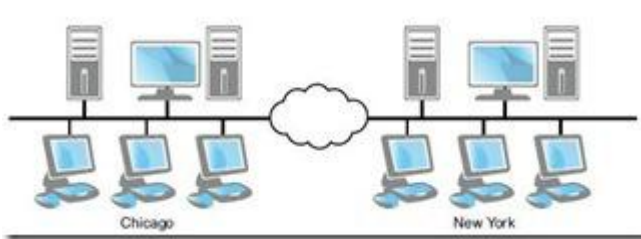
Unlike Windows NT, there are no primary or backup domain controllers. Similar to Windows 2000 and Windows Server 2003, all domain controllers hold a master, editable copy of the Active Directory database.

Every domain must have at least one DC. A domain may have more than one DC; having more than one DC provides the following benefits:

- **Fault tolerance:** If one domain controller goes down, another one is available to authenticate logon requests and locate resources through the directory.
- **Load balancing:** All domain controllers within a site participate equally in domain activities, thus spreading out the load over several servers. This configuration optimizes the speed at which requests are serviced.

Sites

By contrast to the logical grouping of Active Directory into forests, trees, domains, and OUs, Microsoft includes the concept of sites to group together resources within a forest according to their physical location and/or subnet. A *site* is a set of one or more IP subnets, which are connected by a high-speed, always available local area network (LAN) link. Figure 1-5 shows an example with two sites, one located in Chicago and the other in New York. A site can contain objects from more than one tree or domain within a single forest, and individual trees and domains can encompass more than one site. The use of sites enables you to control the replication of data within the Active Directory database as well as to apply policies to all users and computers or delegate administrative control to these objects within a single physical location. In addition, sites enable users to be authenticated by domain controllers in the same physical location rather than a distant location as often as possible. You should configure a single site for all work locations connected within a high-speed, always available LAN link and designate additional sites for locations separated from each other by a slower wide area network (WAN) link. Using sites permits you to configure Active Directory replication to take advantage of the high-speed connection. It also enables users to connect to a domain controller using a reliable, high-speed connection.



Q. What are the components of Active Directory:

Object:

An *object* is any specific item that can be cataloged in Active Directory. Examples of objects include users, computers, printers, folders, and files. These items are classified by a distinct set of characteristics, known as *attributes*. For example, a user can be characterized by the username, full name, telephone number, email address, and so on. Note that, in general, objects in the same container have the same types of attributes but are characterized by different values of these attributes. The Active Directory schema defines the extent of attributes that can be specified for any object.

Classes

The Active Directory service, in turn, classifies objects into *classes*. These classes are logical groupings of similar objects, such as users. Each class is a series of attributes that define the characteristics of the object.

Schemas

The *schema* is a set of rules that define the classes of objects and their attributes that can be created in Active Directory. It defines what attributes can be held by objects of various types, which of the various classes can exist, and what object class can be a parent of the current object class. For example, the User class can contain user account objects and possess attributes such as password, group membership, home folder, and so on.

When you first install Active Directory on a server, a default schema is created, containing definitions of commonly used objects and properties such as users, computers, and groups. This default schema also contains definitions of objects and properties needed for the functioning of Active Directory.

Global catalog

A *global catalog server* is a domain controller that has an additional duty—it maintains a global catalog. A global catalog is a master, searchable database that contains information about every object in every domain in a forest. The global catalog contains a complete replica of all objects in Active Directory for its host domain, and contains a partial replica of all objects in Active Directory for every other domain in the forest.

- A global catalog server performs two important functions:
- Provides group membership information during logon and authentication
- Helps users locate resources in Active Directory

Q. What are the protocols used by AD?

Because Active Directory is based on standard directory access protocols, such as Lightweight Directory Access Protocol (LDAP) version 3, and the Name Service Provider Interface (NSPI), it can interoperate with other directory services employing these protocols.

LDAP is the directory access protocol used to query and retrieve information from Active Directory. Because it is an industry-standard directory service protocol, programs can be developed using LDAP to share Active Directory information with other directory services that also support LDAP.

The NSPI protocol, which is used by Microsoft Exchange 4.0 and 5.x clients, is supported by Active Directory to provide compatibility with the Exchange directory.

Q. Minimum requirement to install Win 2008 AD?

1. An NTFS partition with enough free space
2. An Administrator's username and password
3. The correct operating system version
4. A NIC
5. Properly configured TCP/IP (IP address, subnet mask and – optional – default gateway)
6. A network connection (to a hub or to another computer via a crossover cable)
7. An operational DNS server (which can be installed on the DC itself)
8. A Domain name that you want to use

Q. How do you verify whether the AD installation is proper?

1. Default containers: These are created automatically when the first domain is created. Open **Active Directory Users and Computers**, and then verify that the following containers are present: **Computers**, **Users**, and **ForeignSecurityPrincipals**.
2. Default domain controllers organizational unit: Open **Active Directory Users and Computers**, and then verify this organizational unit.
3. Default-First-Site-Name
4. Active Directory database: The Active Directory database is your Ntds.dit file. Verify its existence in the %Systemroot%\Ntds folder.
5. Global catalog server: The first domain controller becomes a global catalog server, by default. To verify this item:
 - a. Click **Start**, point to **Programs**, click **Administrative Tools**, and then click **Active Directory Sites and Services**.
 - b. Double-click **Sites** to expand it, expand **Servers**, and then select your domain controller.
 - c. Double-click the domain controller to expand the server contents.
 - d. Below the server, an **NTDS Settings** object is displayed. Right-click the object, and then click **Properties**.
 - e. On the **General** tab, you can observe a global catalog check box, which should be selected, by default.

Root domain: The forest root is created when the first domain controller is installed. Verify your computer network identification in **My Computer**. The Domain Name System (DNS) suffix of your computer should match the domain name that the domain controller belongs to. Also, ensure that your computer registers the proper computer role. To verify this role, use the **net accounts** command. The computer role should say "primary" or "backup" depending on whether it is the first domain controller in the domain.

Shared system volume: A Windows 2000 domain controller should have a shared system volume located in the %Systemroot%\Sysvol\Sysvol folder. To verify this item, use the **net share** command. The Active Directory also creates two standard policies during the installation process: The Default Domain policy and the Default Domain Controllers policy (located in the %Systemroot%\Sysvol\Domain\Policies folder). These policies are displayed as the following globally unique identifiers (GUIDs):

{31B2F340-016D-11D2-945F-00C04FB984F9} representing the Default Domain policy

{6AC1786C-016F-11D2-945F-00C04FB984F9} representing the Default Domain Controllers policy

SRV resource records: You must have a DNS server installed and configured for Active Directory and the associated client software to function correctly. Microsoft recommends that you use Microsoft DNS server, which is supplied with Windows 2000 Server as your DNS server. However, Microsoft DNS server is not required. The DNS server that you use must support the Service Resource Record (SRV RR) Requests for Comments (RFC) 2052, and the dynamic update protocol (RFC 2136). Use the DNS Manager Microsoft Management Console (MMC) snap-in to verify that the appropriate zones and resource records are created for each DNS zone. Active Directory creates its SRV RRs in the following folders:

- _Msdcs/Dc/_Sites/Default-first-site-name/_Tcp
- _Msdcs/Dc/_Tcp

In these locations, an SRV RR is displayed for the following services:

- o _kerberos
- o _ldap

Q. What is LDAP?

Short for *Lightweight Directory Access Protocol*, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called *X.500-lite*.

Q. What is FRS (File replication services)?

The File Replication Service (FRS) replicates specific files using the same multi-master model that Active Directory uses. It is used by the Distributed File System for replication of DFS trees that are designated as domain root replicas. It is also used by Active Directory to synchronize content of the SYSVOL volume automatically across domain controllers. The reason the FRS service replicates contents of the SYSVOL folder is so clients will always get a consistent logon environment when logging on to the domain, no matter which domain controller actually handles the request. When a client submits a logon request, he or she submits that request for authentication to the SYSVOL directory. A subfolder of this directory, called \scripts, is shared on the network as the netlogon share. Any logon scripts contained in the netlogon share are processed at logon time. Therefore, the FRS is responsible for all domain controllers providing the same logon directory structure to clients throughout the domain.

Q. Can you connect Active Directory to other 3rd-party Directory Services? Name a few options.

Yes you can Connect Active Directory to other 3rd -party Directory Services such as dictionaries used by SAP, Domino etc with the help of MIIS (Microsoft Identity Integration Server)
you can use dirXML or LDAP to connect to other directories (ie. E-directory from Novell).

Q. Where is the AD database held? What other folders are related to AD?

AD Database is saved in %systemroot%\ntds. You can see other files also in this folder. These are the main files controlling the AD structure

- ntds.dit
- edb.log
- res1.log
- res2.log
- edb.chk

When a change is made to the Win2K database, triggering a write operation, Win2K records the transaction in the log file (edb.log). Once written to the log file, the change is then written to the AD database. System performance determines how fast the system writes the data to the AD database from the log file. Any time the system is shut down, all transactions are saved to the database.

During the installation of AD, Windows creates two files: res1.log and res2.log. The initial size of each is 10MB. These files are used to ensure that changes can be written to disk should the system run out of free disk space. The checkpoint file (edb.chk) records transactions committed to the AD database (ntds.dit). During shutdown, a "shutdown" statement is written to the edb.chk file. Then, during a reboot, AD determines that all transactions in the edb.log file have been committed to the AD database. If, for some reason, the edb.chk file doesn't exist on reboot or the shutdown statement isn't present, AD will use the edb.log file to update the AD database.

The last file in our list of files to know is the AD database itself, ntds.dit. By default, the file is located in \NTDS, along with the other files we've discussed.

Q. What is the SYSVOL folder?

The SYSVOL folder is critical because it contains the domain's public files. This directory is shared out (as SYSVOL), and any files kept in the SYSVOL folder are replicated to all other domain controllers in the domain using the File Replication Service (FRS)—and yes, that's important to know on the exam.

The SYSVOL folder also contains the following items:

- The NETLOGON share, which is the location where domain logon requests are submitted for processing, and where logon scripts can be stored for client processing at logon time.
- Windows Group Policies
- FRS folders and files that must be available and synchronized between domain controllers if the FRS is in use. Distributed File System (DFS), for example, uses the FRS to keep shared data consistent between replicas.

You can go to SYSVOL folder by typing : %systemroot%/sysvol on DC.

Q. Name the AD NCs and replication issues for each NC

*Schema NC, *Configuration NC, * Domain NC

Schema NC: This NC is replicated to every other domain controller in the forest. It contains information about the Active Directory schema, which in turn defines the different object classes and attributes within Active Directory.

Configuration NC: Also replicated to every other DC in the forest, this NC contains forest-wide configuration information pertaining to the physical layout of Active Directory, as well as information about display specifiers and forest-wide Active Directory quotas.

Domain NC: This NC is replicated to every other DC within a single Active Directory domain. This is the NC that contains the most commonly-accessed Active Directory data: the actual users, groups, computers, and other objects that reside within a particular Active Directory domain.

Q. What are application partitions? When do I use them?

A1) Application Directory Partition is a partition space in Active Directory which an application can use to store that application specific data. This partition is then replicated only to some specific domain controllers.

The application directory partition can contain any type of data except security principles (users, computers, groups).

**A2) These are specific to Windows Server 2003 domains.

An application directory partition is a directory partition that is replicated only to specific domain controllers. A domain controller that participates in the replication of a particular application directory partition hosts a replica of that partition. Only domain controllers running Windows Server 2003 can host a replica of an application directory partition.

Q. How do you create a new application partition?

The DnsCmd command is used to create a new application directory partition. Ex. to create a partition named "NewPartition" on the domain controller DC1.contoso.com, log on to the domain controller and type following command.

DnsCmd DC1/createdirectorypartition NewPartition.contoso.com

Q. How do you view replication properties for AD partitions and DCs?

By using replication monitor

go to start > run > type replmon

Q. What is the Global Catalog?

The *global catalog* is the central repository of information about objects in a tree or forest. By default, a global catalog is created automatically on the initial domain controller in the first domain in the forest. A domain controller that holds

a copy of the global catalog is called a *global catalog server*. You can designate any domain controller in the forest as a global catalog server. Active Directory uses multimaster replication to replicate the global catalog information between global catalog servers in other domains. It stores a full replica of all object attributes in the directory for its host domain and a partial replica of all object attributes contained in the directory for every domain in the forest. The partial replica stores attributes most frequently used in search operations (such as a user's first and last names, logon name, and so on). Attributes are marked or unmarked for replication in the global catalog when they are defined in the Active Directory schema. Object attributes replicated to the global catalog inherit the same permissions as in source domains, ensuring that data in the global catalog is secure.

Another Definition of Global Catalog:

Global Catalog Server

A *global catalog server* is a domain controller that has an additional duty—it maintains a global catalog. A global catalog is a master, searchable database that contains information about every object in every domain in a forest. The global catalog contains a complete replica of all objects in Active Directory for its host domain, and contains a partial replica of all objects in Active Directory for every other domain in the forest.

- A global catalog server performs two important functions:
- Provides group membership information during logon and authentication
- Helps users locate resources in Active Directory

Q. What is schema?

The Active Directory schema defines objects that can be stored in Active Directory. The *schema* is a list of definitions that determines the kinds of objects and the types of information about those objects that can be stored in Active Directory. Because the schema definitions themselves are stored as objects, they can be administered in the same manner as the rest of the objects in Active Directory. The schema is defined by two types of objects: schema class objects (also referred to as schema classes) and schema attribute objects (also referred to as schema attributes).

Q. GC and infrastructure master should not be on same server, why?

Unless your domain consists of only one domain controller, **the infrastructure master should not be assigned to a domain controller that's also a Global Catalog server**. If the infrastructure master and Global Catalog are stored on the same domain controller, the infrastructure master will not function because it will never find data that is out of date. It therefore won't ever replicate changes to the other domain controllers in the domain. There are two exceptions:

- If all your domain controllers are Global Catalog servers, it won't matter because all servers will have the latest changes to the Global Catalog.
- If you are implementing a single Active Directory domain, no other domains exist in the forest to keep track of, so in effect, the infrastructure master is out of a job

Q. Why not make all DCs in a large forest as GCs?

When all the DC become a GC replication traffic will get increased and we could not keep the Infrastructure master and GC on the same domain ,so atleast one dc should be act without holding the GC role .

Q. Trying to look at the Schema, how can I do that?

Register the schmmgmt.dll with the command regsvr32

Q. What are the Support Tools? Why do I need them?

Support Tools are the tools that are used for performing the complicated tasks easily. These can also be the third party tools. Some of the Support tools include DebugViewer, DependencyViewer, RegistryMonitor, etc.

Q. What is LDP? What is REPLMON? What is ADSIEDIT? What is NETDOM? What is REPADMIN?

LDP – Label Distribution Protocol (LDP) is often used to establish MPLS LSPs when traffic engineering is not required. It establishes LSPs that follow the existing IP routing, and is particularly well suited for establishing a full mesh of LSPs between all of the routers on the network.

Replmon – Replmon displays information about Active Directory Replication.

ADSIEDIT – ADSIEdit is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for Active Directory. It is a Graphical User Interface (GUI) tool. Network administrators can use it for common administrative tasks such as adding, deleting, and moving objects with a directory service. The attributes for each object can be edited or deleted by using this tool. ADSIEdit uses the ADSI application programming interfaces (APIs) to access Active Directory. The following are the required files for using this tool: ADSIEDIT.DLL ADSIEDIT.MSC

NETDOM - NETDOM is a command-line tool that allows management of Windows domains and trust relationships. It is used for batch management of trusts, joining computers to domains, verifying trusts, and secure channels.

REPADMIN – REPADMIN is a built-in Windows diagnostic command-line utility that works at the Active Directory level. Although specific to Windows, it is also useful for diagnosing some Exchange replication problems, since Exchange Server is Active Directory based. REPADMIN doesn't actually fix replication problems for you. But, you can use it to help determine the source of a malfunction.

Q. What are the Naming Conventions used in AD?

Within Active Directory, each object has a name. When you create an object in Active Directory, such as a user or a computer, you assign the object a name. This name must be unique within the domain—you can't assign an object the same name as any other object (regardless of its type) in that domain.

At the same time that you create an object, not only do you assign a name to the object, but Active Directory also assigns identifiers to the object. Active Directory assigns every object a globally unique identifier (GUID), and assigns many objects a security identifier (SID). A *GUID* is typically a 32-digit hexadecimal number that uniquely identifies an object within Active Directory. A *SID* is a unique number created by the Windows 2000 Security subsystem that is assigned only to *security principal objects* (users, groups, and computers) when they are created. Windows 2000 uses SIDs to grant or deny a security principal object access to other objects and network resources.

Active Directory uses a hierarchical naming convention that is based on Lightweight Directory Access Protocol (LDAP) and DNS standards.

Objects in Active Directory can be referenced by using one of three Active Directory name types:

- Relative distinguished name (RDN)
- Distinguished name (DN)
- User principal name (UPN)

A relative distinguished name (RDN) is the name that is assigned to the object by the administrator when the object is created. For example, when

I create a user named AlanC, the RDN of that user is AlanC. The RDN only identifies an object—it doesn't identify the object's location within Active Directory. The RDN is the simplest of the three Active Directory name types, and is sometimes called the common name of the object.

A distinguished name (DN) consists of an object's RDN, plus the object's location in Active Directory. The DN supplies the complete path to the object. An object's DN includes its RDN, the name of the organizational unit(s) that contains the object (if any), and the FQDN of the domain. For example, suppose that I create a user named AlanC in an organizational unit called US in a domain named Exportsinc.com. The DN of this user would

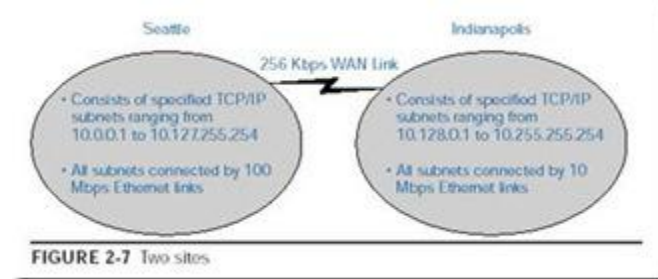
be: [AlanC@US.Exportsinc.com](#)

A user principal name (UPN) is a shortened version of the DN that is typically used for logon and e-mail purposes. A UPN consists of the RDN plus the FQDN of the domain. Using my previous example, the UPN for the user named AlanC would be: AlanC@Exportsinc.com

Another way you can think of a UPN is as a DN stripped of all organizational unit references.

Q. What are sites? What are they used for?

A *site* consists of one or more TCP/IP subnets, which are specified by an administrator. Additionally, if a site contains more than one subnet, the subnets should be connected by high-speed, reliable links. Sites do not correspond to domains: You can have two or more sites within a single domain, or you can have multiple domains in a single site. A site is solely a grouping based on IP addresses. Figure 2-7 shows two sites connected by a slow WAN link.



The purpose of sites is to enable servers that regularly copy data to other servers (such as Active Directory replication data) to distinguish between servers in their own site (which are connected by high-speed links) and servers in another site (which are connected by slower-speed WAN links). Replication between domain controllers in the same site is fast, and typically administrators can permit Windows 2000 to automatically perform this task. Replication between a domain controller in one site and domain controllers in other sites is slower (because it takes place over a slow WAN link) and often should be scheduled by the administrator so that use of network bandwidth for replication is minimized during the network's peak-activity hours.

Sites and Active Directory replication can be configured by using Active Directory Sites and Services.

Uses of site:

Sites are primarily used to control replication traffic. Domain controllers within a site are pretty much free to replicate changes to the Active Directory database whenever changes are made. Domain controllers in different sites compress the replication traffic and operate based on a defined schedule, both of which are intended to cut down on network traffic.

More specifically, sites are used to control the following:

- Workstation logon traffic
- Replication traffic
- Distributed File System (DFS)

What's the difference between a site link's schedule and interval?

Site Link is a physical connection object on which the replication transport mechanism depends on. Basically to speak it is the type of communication mechanism used to transfer the data between different sites. Site Link Schedule is nothing but when the replication process has to be takes place and the interval is nothing but how many times the replication has to be takes place in a give time period i.e Site Link Schedule.

Q. What is replication? How it occurs in AD? What is KCC and ISTG

Each domain controller stores a complete copy of all Active domain controllers in the same domain. Domain controllers in a domain automatically replicate directory information for all objects in the domain to each other. When you perform an action that causes an update to Active Directory, you are actually making the change at one of the domain controllers. That domain controller then replicates the change to all other domain controllers within the

domain. You can control replication of traffic between domain controllers in the network by specifying how often replication occurs and the amount of data that each domain controller replicates at one time. Domain controllers immediately replicate certain important updates, such as the disabling of a user account.

Active Directory uses multimaster replication, in which no one domain controller is the master domain controller. Instead, all domain controllers within a domain are peers, and each domain controller contains a copy of the directory database that can be written to. Domain controllers can hold different information for short periods of time until all domain controllers have synchronized changes to Active Directory.

Although Active Directory supports multimaster replication, some changes are impractical to perform in multimaster fashion. One or more domain controllers can be assigned to perform single-master replication (operations not permitted to occur at different places in a network at the same time). *Operations master roles* are special roles assigned to one or more domain controllers in a domain to perform single-master replication.

Domain controllers detect collisions, which can occur when an attribute is modified on a domain controller before a change to the same attribute on another domain controller is completely propagated. Collisions are detected by comparing each attribute's property version number, a number specific to an attribute that is initialized upon creation of the attribute. Active Directory resolves the collision by replicating the changed attribute with the higher property version number.

Q. What can you do to promote a server to DC if you're in a remote location with slow WAN link?

Install from Media In Windows Server 2003 a new feature has been added, and this time it's one that will actually make our lives easier... You can promote a domain controller using files backed up from a source domain controller!!! This feature is called "Install from Media" and it's available by running DCPROMO with the /adv switch. It's not a replacement for network replication, we still need network connectivity, but now we can use an old System State copy from another Windows Server 2003, copy it to our future DC, and have the first and basic replication take place from the media, instead of across the network, this saving valuable time and network resources.

What you basically have to do is to back up the systems data of an existing domain controller, restore that backup to your replica candidate, use DCPromo /Adv to tell it to source from local media, rather than a network source.

This also works for global catalogs. If we perform a backup of a global catalog server, then we can create a new global catalog server by performing DCPromo from that restored media.

IFM Limitations

It only works for the same domain, so you cannot back up a domain controller in domain A and create a new domain B using that media.

It's only useful up to the tombstone lifetime with a default of 60 days. So if you have an old backup, then you cannot create a new domain controller using that, because you'll run into the problem of reanimating deleted objects.

Q. How can you forcibly remove AD from a server, and what do you do later?

Demoting Windows Server 2003 DCs: DCPROMO (Active Directory Installation Wizard) is a toggle switch, which allows you to either install or remove Active Directory DCs. To forcibly demote a Windows Server 2003 DC, run the following command either at the Start, Run, or at the command prompt:

`dcpromo /forceremoval`

Note: If you're running Certificate Services on the DC, you must first remove Certificate Services before continuing. If you specify the /forceremoval switch on a server that doesn't have Active Directory installed, the switch is ignored and the wizard pretends that you want to install Active Directory on that server.

Once the wizard starts, you will be prompted for the Administrator password that you want to assign to the local administrator in the SAM database. If you have Windows Server 2003 Service Pack 1 installed on the DC, you'll benefit from a few enhancements. The wizard will automatically run certain checks and will prompt you to take appropriate actions. For example, if the DC is a Global Catalog server or a DNS server, you will be prompted. You will also be prompted to take an action if your DC is hosting any of the operations master roles.

Demoting Windows 2000 DCs: On a Windows 2000 domain controller, forced demotion is supported with Service Pack 2 and later. The rest of the procedure is similar to the procedure I described for Windows Server 2003. Just make sure that while running the wizard, you clear the "This server is the last domain controller in the domain" check box. On Windows 2000 Servers you won't benefit from the enhancements in Windows Server 2003 SP1, so if the DC you are demoting is a Global Catalog server, you may have to manually promote some other DC to a Global Catalog server.

Cleaning the Metadata on a Surviving DC : Once you've successfully demoted the DC, your job is not quite done yet. Now you must clean up the Active Directory metadata. You may be wondering why I need to clean the metadata manually. The metadata for the demoted DC is not deleted from the surviving DCs because you forced the demotion. When you force a demotion, Active Directory basically ignores other DCs and does its own thing. Because the other DCs are not aware that you removed the demoted DC from the domain, the references to the demoted DC need to be removed from the domain.

Although Active Directory has made numerous improvements over the years, one of the biggest criticisms of Active Directory is that it doesn't clean up the mess very well. This is obvious in most cases but, in other cases, you won't know it unless you start digging deep into Active Directory database.

To clean up the metadata you use NTDSUTIL. The following procedure describes how to clean up metadata on a Windows Server 2003 SP1. According to Microsoft, the version of NTDSUTIL in SP1 has been enhanced considerably and does a much better job of clean-up, which obviously means that the earlier versions didn't do a very good job. For Windows 2000 DCs, you might want to check out Microsoft Knowledge Base article 216498, "How to remove data in Active Directory after an unsuccessful domain controller demotion."

Here's the step-by-step procedure for cleaning metadata on Windows Server 2003 DCs:

1. Logon to the DC as a Domain Administrator.
2. At the command prompt, type `ntdsutil`.
3. Type `metadata cleanup`.
4. Type `connections`.
5. Type `connect to server servername`, where `servername` is the name of the server you want to connect to.
6. Type `quit` or `q` to go one level up. You should be at the Metadata Cleanup prompt.
7. Type `select operation target`.
8. Type `list domains`. You will see a list of domains in the forest, each with a different number.
9. Type `select domain number`, where `number` is the number associated with the domain of your server.
10. Type `list sites`.
11. Type `select site number`, where `number` is the number associated with the site of your server.
12. Type `list servers in site`.
13. Type `select server number`, where `number` is the number associated with the server you want to remove.
14. Type `quit` to go to Metadata Cleanup prompt.
15. Type `remove selected server`. You should see a confirmation that the removal completed successfully.
16. Type `quit` to exit `ntdsutil`.

You might also want to cleanup DNS database by deleting all DNS records related to the server.

In general, you will have better luck using forced promotion on Windows Server 2003, because the naming contexts and other objects don't get cleaned as quickly on Windows 2000 Global Catalog servers, especially servers running Windows 2000 SP3 or earlier. Due to the nature of forced demotion and the fact that it's meant to be used only as a last resort, there are additional things that you should know about forced demotion.

Even after you've used NTDSUTIL to clean the metadata, you may still need to do additional cleaning manually using ADSIEdit or other such tools

Q. Can I get user passwords from the AD database?

As of my Knowledge there is no way to extract the password from AD Database. By the way there is a tool called **cache dump**. Using it we can extract the cached passwords from Windows XP machine which is joined to a Domain.

Q. Name some OU design considerations.

- Design OU structure based on Active Directory business requirements
- NT Resource domains may fold up into OUs
- Create nested OUs to hide objects
- Objects easily moved between OUs
- Departments , Geographic Region, Job Function, Object Type

Q. What is tombstone lifetime attribute?

The number of days before a deleted object is removed from the directory services. This assists in removing objects from replicated servers and preventing restores from reintroducing a deleted object. This value is in the Directory Service object in the configuration NC.

Q. How would you find all users that have not logged on since last month?

If you are using windows 2003 domain environment, then goto Active Directory Users and Computers, select the Saved Queries, right click it and select new query, then using the custom common queries and define query there is one which shows days since last logon

Q. What are the DS* commands?

- [DSmod – modifyActiveDirectoryattributes](#)
- **DSrm** – to delete Active Directory objects
- **DSmove** - to relocate objects
- [DSadd – createnewaccounts](#)
- [DSquery- tofindobjectsthatmatchyourqueryattributes](#)
- [DSget- listthepropertiesofanobject](#)

What's the difference between LDIFDE and CSVDE? Usage considerations?

CSVDE is a command that can be used to import and export objects to and from the AD into a CSV-formatted file. A CSV (Comma Separated Value) file is a file easily readable in Excel. I will not go to length into this powerful command, but I will show you some basic samples of how to import a large number of users into your AD. Of course, as with the DSADD command, CSVDE can do more than just import users. Consult your help file for more info. Like CSVDE, LDIFDE is a command that can be used to import and export objects to and from the AD into a LDIF-formatted file. A LDIF (LDAP Data Interchange Format) file is a file easily readable in any text editor; however it is not readable in programs like Excel. The major difference between CSVDE and LDIFDE (besides the file format) is the fact that LDIFDE can be used to edit and delete existing AD objects (not just users), while CSVDE can only import and export objects

What is DFS?

The Distributed File System is used to build a hierarchical view of multiple file servers and shares on the network. Instead of having to think of a specific machine name for each set of files, the user will only have to remember one name; which will be the 'key' to a list of shares found on multiple servers on the network. Think of it as the home of all file shares with links that point to one or more servers that actually host those shares.

DFS has the capability of routing a client to the closest available file server by using Active Directory site metrics. It can also be installed on a cluster for even better performance and reliability.

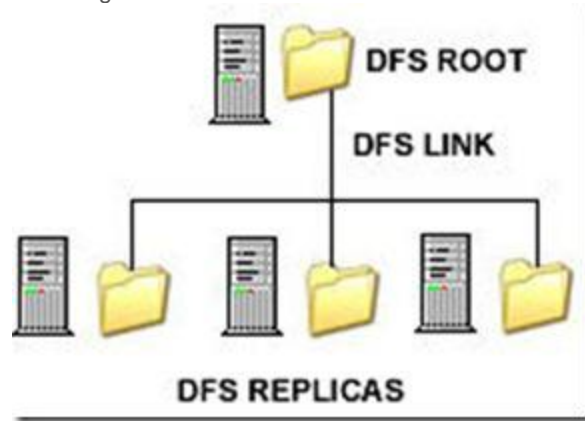
It is important to understand the new concepts that are part of DFS. Below is an definition of each of them.

Dfs root: You can think of this as a share that is visible on the network, and in this share you can have additional files and folders.

Dfs link: A link is another share somewhere on the network that goes under the root. When a user opens this link they will be redirected to a shared folder.

Dfs target (or replica): This can be referred to as either a root or a link. If you have two identical shares, normally stored on different servers, you can group them together as Dfs Targets under the same link.

The image below shows the actual folder structure of what the user sees when using DFS and load balancing.



The actual folder structure of DFS and load balancing

Q. What are the types of replication in DFS?

There are two types of replication:

- Automatic – which is only available for Domain DFS
- Manual – which is available for stand alone, DFS and requires all files to be replicated manually.

Q. Which service is responsible for replicating files in SYSVOL folder?

File Replication Service (FRS)

Windows 2008 Server Interview Questions Part II

1. What are the Important Windows port numbers:

RDP – 3389 – (windows rdp port number and remote desktop port number)
FTP – 21 – (file transfer protocol)
TFTP – 69 – (tftp port number)
Telnet – 23 – (telnet port number)
SMTP – 25 – (SMTP port number)
DNS – 53 – (dns port number and Domain Name System port number)
DHCP – 68 – (DHCP port number and Dynamic Host Configuration Protocol port number)
POP3 – 110 – (post office Protocol 3 port)
HTTP – 80 – (http port number)
HTTPS – 443 – (https port number)
NNTP – 119 – (Network News Transfer Protocol Port number)
NTP – 123 – (ntp port number and network Time Protocol and SNTP port number)
IMAP – 143 – (Internet Message Access Protocol port number)
SSMTP – 465 – (SMTP Over SSI)
SIMAP – 993 – (IMAP Over SSL)
SPOP3 – 995 – (POP# Over SS L)
Time – 123 – (ntp port number and network Time Protocol and SNTP port number)
NetBios – 137 – (Name Service)
NetBios – 139 – (Datagram Service)
DHCP Client – 546 – (DHCP Client port number)
DHCP Server – 547 – (DHCP Server port number)
Global Catalog – 3268 – (Global Catalog port number)
LDAP – 389 – (LDAP port number and Lightweight Directory Access Protocol port number)
RPC – 135 – (remote procedure call Port number)
Kerberos – 88 – (Kerberos Port Number)
SSH – 22 – (ssh port number and Secure Shell port number)

2. How to check tombstone lifetime value in your Forest

Tombstone lifetime value different from OS to OS, for windows server 2000/2003 it's 60 days, In Windows Server 2003 SP1, default tombstone lifetime (TSL) value has increased from 60 days to 180 days, again in Windows Server 2003 R2 TSL value has been decreased to 60 days, Windows Server 2003 R2 SP2 and windows server 2008 it's 180 days

If you migrating windows 2003 environment to windows 2008 then its 60 day's
you can use the below command to check/view the current tombstone lifetime value for your Domain/Forest
dsquery * "cn=directory service,cn=windows nt,cn=services,cn=configuration,dc=" –scope base –attr
tombstonelifetime

Replace forestDN with your domain partition DN, for domainname.com the DN would be dc=domainname, dc=com

Source: [http://technet.microsoft.com/en-us/library/cc784932\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc784932(WS.10).aspx)

3. How to find the domain controller that contains the lingering object

If we enable Strict Replication Consistency

Lingering objects are not present on domain controllers that log Event ID 1988. The source domain controller contains the lingering object

If we doesn't enable Strict Replication Consistency

Lingering objects are not present on domain controllers that log Event ID 1388. Domain controller that doesn't log Event ID 1388 and that domain controller contain the lingering object

You have a 100 Domain controllers which doesn't enable Strict Replication Consistency, then you will get the Event ID 1388 on all the 99 Domain controllers except the one that contain the lingering object

Need to Remove Lingering Objects from the affected domain controller or decommission the domain controller

You can use Event Comb tool (Eventcombmt.exe) is a multi-threaded tool that can be used to gather specific events from the Event Viewer logs of different computers at the same time.

You can download these tools from the following location:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en>

4. What are Active Directory ports:

List of Active Directory Ports for Active Directory replication and Active Directory authentication, this ports can be used to configure the Firewall

Active Directory replication- There is no defined port for Active Directory replication, Active Directory replication remote procedure calls (RPC) occur dynamically over an available port through RPCSS (RPC Endpoint Mapper) by using port 135

File Replication Services (FRS)- There is no defined port for FRS, FRS replication over remote procedure calls (RPCs) occurs dynamically over an available port by using RPCSS (RPC Endpoint Mapper) on port 135

Other required ports for Active Directory

TCP 53 – DSN (DNS Download)

UDP 53 – DSN (DNS Queries)

TCP 42- WINS

UDP 42- WINS

TCP 3389- RDP (Remote Desktop)

TCP 135 – MS-RPC

TCP 1025 & 1026 – AD Login & replication

TCP 389 – LDAP

TCP 639 – LDAP over SSL/TLS

TCP 3268 -Global Catalog

TCP 3268 – Global Catalog over SSL/TSL

UDP 137 & 138 – NetBIOS related

UDP 88 – Kerberos v5

TCP 445 – SMB , Microsoft-ds

TCP 139 – SMB

5. How to do active directory health checks?

As an administrator you have to check your active directory health daily to reduce the active directory related issues, if you are not monitoring the health of your active directory what will happen

Let's say one of the Domain Controller failed to replicate, first day you will not have any issue. If this will continue then you will have login issue and you will not find the object change and new object, that's created and changed in other Domain Controller this will lead to other issues

If the Domain Controller is not replicated more than 60 day's then it will lead to Linging issue

Command to check the replication to all the DC's(through this we can check Active Directory Health)

```
Repadmin /replsum /bysrc /bydest /sort:delta
```

You can also save the command output to text file, by using the below command

```
Repadmin /replsum /bysrc /bydest /sort:delta >>c:\replication_report.txt
```

this will list the domain controllers that are failing to replicate with the delta value

You can daily run this to check your active directory health

6. GPRESULT failed with access denied error:

Unable to get the result from gpresult on windows 2003 server, gpresult return with the access denied errors, you can able to update the group policy without issue

Run the following commands to register the userenv.dll and recompile the rsop mof file

To resolve the access denied error while doing the gpresult.

1. Open a cmd

1. re-register the userenv.dll

```
Regsvr32 /n /l c:\winnt\system32\userenv.dll
```

2. CD c:\windows\system32\wbem

3. Mofcomp scersop.mof

4. Gpupdate /force

5. Gpresult

Now you able to run the gpresult without error and even server reboot not required for this procedure

7. What is the command to find out site name for given DC

dsquery server NYDC01 -site

domain controller name = NYDC01

8. Command to find all DCs in the given site

Command to find all the Domain Controllers in the "Default-First-Site-Name" site

dsquery server -o rdn -site Default-First-Site-Name

Site name = Default-First-Site-Name

9. How many types of queries DNS does?

Iterative Query

Recursive Query

Iterative Query

In this query the client ask the name server for the best possible answer, the name server check the cache and zone for which it's authoritative and returns the best possible answer to the client, which would be the full answer like IP address or try the other name server

Recursive Query

Client demands either a full answer or an error message (like record or domain name does not exist)

Client machine always send recursive query to the DNS server, if the DNS server does not have the requested information, DNS server send the iterative query to the other name server (through forwarders or secondary DNS server) until it gets the information, or until the name query fails.

Windows Admins

All you wanted to know about Windows Administration

- [HOME](#)
- [ABOUT ME](#)

[POSTS](#) [COMMENTS](#)

- [WINDOWS TECHNOLOGIES](#)
- [VMWARE VSPHERE](#)
- [CITRIX XENAPP](#)
- [SERVER RELATED](#)

[VMware vSphere performance troubleshooting →](#)

Windows Sever 2008/R2 Interview questions Part 1

JUNE 22, 2011 [10 COMMENTS](#)

Difference between 2003 and 2008

1) 2008 is combination of vista and windows 2003r2. Some new services are introduced in it

1. RODC one new domain controller introduced in it [Read-only Domain controllers.]

2. WDS (windows deployment services) instead of RIS in 2003 server

3. shadow copy for each and every folders

4. boot sequence is changed

5. installation is 32 bit where as 2003 it is 16 as well as 32 bit, that's why installation of 2008 is faster

6. services are known as role in it

7. Group policy editor is a separate option in ads

2) The main difference between 2003 and 2008 is Virtualization, management. 2008 has more inbuilt components and updated third party drivers Microsoft introduces new feature with 2k8 that is Hyper-V Windows Server 2008 introduces Hyper-V (V for Virtualization) but only on 64bit versions. More and more companies are seeing this as a way of reducing hardware costs by running several 'virtual' servers on one physical machine. If you like this exciting technology, make sure that you buy an edition of Windows Server 2008 that includes Hyper-V, then launch the Server Manger, add Roles.

Windows server 2008 new features

1. Virtualization with Hyper V

2. **Server Core** – provides the minimum installation required to carry out a specific server role, such as for a DHCP, DNS or print server. From a security standpoint, this is attractive. Fewer applications and services on the sever make for a smaller attack surface. In theory, there should also be less maintenance and management with fewer patches to install, and the whole server could take up as little as 3Gb of disk space according to Microsoft

3. IIS 7

4. **Role based installation** – rather than configuring a full server install for a particular role by uninstalling unnecessary components (and installing needed extras), you simply specify the role the server is to play, and Windows will install what's necessary — nothing more.

5. **Read Only Domain Controllers (RODC)**

It's hardly news that branch offices often lack skilled IT staff to administer their servers, but they also face another, less talked about problem. While corporate data centers are often physically secured, servers at branch offices rarely have the same physical security protecting them. This makes them a convenient launch pad for attacks back to the main corporate servers. RODC provides a way to make an Active Directory database read-only. Thus, any mischief carried out at the branch office cannot propagate its way back to poison the Active Directory system as a whole. It also reduces traffic on WAN links.

6. **Enhanced terminal services**

Terminal services has been beefed up in Server 2008 in a number of ways. TS RemoteApp enables remote users to access a centralized application (rather than an entire desktop) that appears to be running on the local computer's hard drive. These apps can be accessed via a Web portal or directly by double-clicking on a correctly configured icon on the local machine. TS Gateway secures sessions, which are then tunnelled over https, so users don't need to use a VPN to use RemoteApps securely over the Internet. Local printing has also been made significantly easier.

7. **Network Access Protection**

Microsoft's system for ensuring that clients connecting to Server 2008 are patched, running a firewall and in compliance with corporate security policies — and that those that are not can be remediated — is useful. However, similar functionality has been and remains available from third parties.

8. **Windows PowerShell**

Microsoft's new (ish) command line shell and scripting language has proved popular with some server administrators, especially those used to working in Linux environments. Included in Server 2008, PowerShell can make some jobs quicker and easier to perform than going through the GUI. Although it might seem like a step backward in terms of user friendly operation, it's one of those features that once you've gotten used to it; you'll never want to give up.

Restartable Active Directory Domain Services: You can now perform many actions, such as offline defragmentation of the database, simply by stopping Active Directory. This reduces the number of instances in which you must restart the server in Directory Services Restore Mode and thereby reduces the length of time the domain controller is unavailable to serve requests from

Enhancements to Group Policy: Microsoft has added many new policy settings. In particular, these settings enhance the management of Windows Vista client computers. All policy management is now handled by means of the Group Policy Management Console (GPMC), which was an optional feature first added to Windows Server 2003 R2. In addition, Microsoft has added new auditing capabilities to Group Policy and added a searchable database for locating policy settings from within GPMC. In Windows Server 2008 R2, GPMC enables you to use a series of PowerShell cmdlets to automate many of the tasks (such as maintenance and linking of GPOs) that you would otherwise perform in the GUI. In addition, R2 adds new policy settings that enhance the management of Windows 7 computers.

Windows Server 2008 R2 new features:

Active Directory Recycle Bin

Windows PowerShell 2.0

Active Directory Administrative Center (ADAC)

Offline domain join

Active Directory health check

Active Directory Web Services
Active Directory Management Pack
Windows Server Migration Tools
Managed Service Accounts

What is server core? How do you configure and manage a windows server 2008 core installation?

The Server Core installation option is an option that you can use for installing Windows Server 2008 or Windows Server 2008 R2. A Server Core installation provides a minimal environment for running specific server roles, which reduces the maintenance and management requirements and the attack surface for those server roles. A server running a Server Core installation of Windows Server 2008 supports the following server roles:

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP Server
- DNS Server
- File Services
- Hyper-V
- Print Services
- Streaming Media Services
- Web Server (IIS)

A server running a Server Core installation of Windows Server 2008 R2 supports the following server roles:

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP Server
- DNS Server
- File Services (including File Server Resource Manager)
- Hyper-V
- Print and Document Services
- Streaming Media Services
- Web Server (including a subset of ASP.NET)

A Server Core installation does not include the traditional full graphical user interface. Once you have configured the server, you can manage it locally at a command prompt or remotely using a Terminal Server connection. You can also manage the server remotely using the Microsoft Management Console (MMC) or command-line tools that support remote use.

Benefits of a Server Core installation

The Server Core installation option of Windows Server 2008 or Windows Server 2008 R2 provides the following benefits:

- **Reduced maintenance.** Because the Server Core installation option installs only what is required to have a manageable server for the supported roles, less maintenance is required than on a full installation of Windows Server 2008.
- **Reduced attack surface.** Because Server Core installations are minimal, there are fewer applications running on the server, which decreases the attack surface.

- **Reduced management.** Because fewer applications and services are installed on a server running the Server Core installation, there is less to manage.
- **Less disk space required.** A Server Core installation requires only about 3.5 gigabytes (GB) of disk space to install and approximately 3 GB for operations after the installation.

How do you promote a Server Core to DC?

In order to install Active Directory DS on your server core machine you will need to perform the following tasks:

1. **Configure an unattend text file, containing the instructions for the DCPROMO process. In this example you will create an additional DC for a domain called petrilib.local:**

```
[DCINSTALL]
UserName=administrator
UserDomain=petrilib
Password=P@sswOrd1
SiteName=Default-First-Site-Name
ReplicaOrNewDomain=replica
DatabasePath="%systemroot%\NTDS"
LogPath="%systemroot%\NTDS"
SYSVOLPath="%systemroot%\SYSVOL"
InstallDNS=yes
ConfirmGC=yes
SafeModeAdminPassword=P@sswOrd1
RebootOnCompletion=yes
```

2. **Configure the right server core settings**

After that you need to make sure the core machine is properly configured.

1. Perform any configuration setting that you require (tasks such as changing computer name, changing and configure IP address, subnet mask, default gateway, DNS address, firewall settings, configuring remote desktop and so on).
2. After changing the required server configuration, make sure that for the task of creating it as a DC – you have the following requirements in place:
 - A partition formatted with NTFS (you should, it's a server...)
 - A network interface card, configure properly with the right driver
 - A network cable plugged in
 - The right IP address, subnet mask, default gateway

And most importantly, do not forget:

- The right DNS setting, in most cases, pointing to an existing internal DNS in your corporate network

3. **Copy the unattend file to the server core machine**

Now you need to copy the unattend file from wherever you've stored it. You can run it from a network location but I prefer to have it locally on the core machine. You can use the NET USE command on server core to map to a network path and copy the file to the local drive. You can also use a regular server/workstation to graphically access the core's C\$ drive (for example) and copy the file to that location.

4. **Run the DCPROMO process**

Next you need to manually run DCPROMO. To run the Active Directory Domain Services Installation Wizard in unattended mode, use the following command at a command prompt:

Dcpromo /unattend

Reboot the machine

In order to reboot the server core machine type the following text in the command prompt and press Enter.

shutdown /r /t 0

What are RODCs? What are advantages?

A read-only domain controller (RODC) is a new type of domain controller in the Windows Server® 2008 operating system. With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed. An RODC hosts read-only partitions of the Active Directory Domain Services (AD DS) database.

Before the release of Windows Server 2008, if users had to authenticate with a domain controller over a wide area network (WAN), there was no real alternative. In many cases, this was not an efficient solution. Branch offices often cannot provide the adequate physical security that is required for a writable domain controller. Furthermore, branch offices often have poor network bandwidth when they are connected to a hub site. This can increase the amount of time that is required to log on. It can also hamper access to network resources.

Beginning with Windows Server 2008, an organization can deploy an RODC to address these problems. As a result, users in this situation can receive the following benefits:

- Improved security
- Faster logon times
- More efficient access to resources on the network

What does an RODC do?

Inadequate physical security is the most common reason to consider deploying an RODC. An RODC provides a way to deploy a domain controller more securely in locations that require fast and reliable authentication services but cannot ensure physical security for a writable domain controller.

However, your organization may also choose to deploy an RODC for special administrative requirements. For example, a line-of-business (LOB) application may run successfully only if it is installed on a domain controller. Or, the domain controller might be the only server in the branch office, and it may have to host server applications.

In such cases, the LOB application owner must often log on to the domain controller interactively or use Terminal Services to configure and manage the application. This situation creates a security risk that may be unacceptable on a writable domain controller.

An RODC provides a more secure mechanism for deploying a domain controller in this scenario. You can grant a non-administrative domain user the right to log on to an RODC while minimizing the security risk to the Active Directory forest.

You might also deploy an RODC in other scenarios where local storage of all domain user passwords is a primary threat, for example, in an extranet or application-facing role.

How do you install an RODC?

- 1 Make sure you are a member of Domain Admin group
2. Ensure that the forest functional level is Windows Server 2003 or higher
3. Run adprep /rodcprep
3. Install a writable domain controller that runs Windows Server 2008 – An RODC must replicate domain updates from a writable domain controller that runs Windows Server 2008. Before you install an RODC, be sure to install a writable domain controller that runs Windows Server 2008 in the same domain. The domain controller can run either a full installation or a Server Core installation of Windows Server 2008. In Windows Server 2008, the writable domain controller does not have to hold the primary domain controller (PDC) emulator operations master role.
4. You can install an RODC on either a full installation of Windows Server 2008 or on a Server Core installation of Windows Server 2008. Follow the below steps:

- Click **Start**, type **dcpromo**, and then press ENTER to start the Active Directory Domain Services Installation Wizard.
- On the **Choose a Deployment Configuration** page, click **Existing forest**, click **Add a domain controller to an existing domain**
- On the **Network Credentials** page, type the name of a domain in the forest where you plan to install the RODC. If necessary, also type a user name and password for a member of the Domain Admins group, and then click **Next**.
- Select the domain for the RODC, and then click **Next**.
- Click the Active Directory site for the RODC and click next
- Select the **Read-only domain controller** check box, as shown in the following illustration. By default, the **DNS server** check box is also selected. To run the DNS server on the RODC, another domain controller running Windows Server 2008 must be running in the domain and hosting the DNS domain zone. An Active Directory–integrated zone on an RODC is always a read-only copy of the zone file. Updates are sent to a DNS server in a hub site instead of being made locally on the RODC.
- To use the default folders that are specified for the Active Directory database, the log files, and SYSVOL, click **Next**.
- Type and then confirm a Directory Services Restore Mode password, and then click **Next**.
- Confirm the information that appears on the Summary page, and then click **Next** to start the AD DS installation. You can select the **Reboot on completion** check box to make the rest of the installation complete automatically.

What is the minimum requirement to install Windows 2008 server?

Component	Requirement
Processor	• Minimum: 1GHz (x86 processor) or 1.4GHz (x64 processor) • Recommended: 2GHz or faster Note: An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-based Systems
Memory	• Minimum: 512MB RAM • Recommended: 2GB RAM or greater • Maximum (32-bit systems): 4GB (Standard) or 64GB (Enterprise and Datacenter) • Maximum (64-bit systems): 32GB (Standard) or 2TB (Enterprise, Datacenter and Itanium-based Systems)
Available Disk Space	• Minimum: 10GB • Recommended: 40GB or greater Note: Computers with more than 16GB of RAM will require more disk space for paging, hibernation, and dump files
Drive	DVD-ROM drive
Display and Peripherals	• Super VGA (800 x 600) or higher-resolution monitor • Keyboard • Microsoft Mouse or compatible pointing device

Talk about all the AD-related roles in Windows Server 2008/R2.

Active Directory Domain Services

Active Directory Domain Services (AD DS), formerly known as Active Directory Directory Services, is the central location for configuration information, authentication requests, and information about all of the objects that are stored within your forest. Using Active Directory, you can efficiently manage users, computers, groups, printers, applications, and other directory-enabled objects from one secure, centralized location.

Benefits

- **Lower costs** of managing Windows networks.
- **Simplify identity management** by providing a single view of all user information.
- **Boost security** with the ability to enable multiple types of security mechanisms within a single network.

- **Improve compliance** by using Active Directory as a primary source for audit data.

Active Directory Rights Management Services

Your organization's intellectual property needs to be safe and highly secure. Active Directory Rights Management Services, a component of Windows Server 2008, is available to help make sure that only those individuals who need to view a file can do so. AD RMS can protect a file by identifying the rights that a user has to the file. Rights can be configured to allow a user to open, modify, print, forward, or take other actions with the rights-managed information. With AD RMS, you can now safeguard data when it is distributed outside of your network.

Active Directory Federation Services

Active Directory Federation Services is a highly secure, highly extensible, and Internet-scalable identity access solution that allows organizations to authenticate users from partner organizations. Using AD FS in Windows Server 2008, you can simply and very securely grant external users access to your organization's domain resources. AD FS can also simplify integration between untrusted resources and domain resources within your own organization.

Active Directory Certificate Services

Most organizations use certificates to prove the identity of users or computers, as well as to encrypt data during transmission across unsecured network connections. Active Directory Certificate Services (AD CS) enhances security by binding the identity of a person, device, or service to their own private key. Storing the certificate and private key within Active Directory helps securely protect the identity, and Active Directory becomes the centralized location for retrieving the appropriate information when an application places a request.

Active Directory Lightweight Directory Services

Active Directory Lightweight Directory Service (AD LDS), formerly known as Active Directory Application Mode, can be used to provide directory services for directory-enabled applications. Instead of using your organization's AD DS database to store the directory-enabled application data, AD LDS can be used to store the data. AD LDS can be used in conjunction with AD DS so that you can have a central location for security accounts (AD DS) and another location to support the application configuration and directory data (AD LDS). Using AD LDS, you can reduce the overhead associated with Active Directory replication, you do not have to extend the Active Directory schema to support the application, and you can partition the directory structure so that the AD LDS service is only deployed to the servers that need to support the directory-enabled application.

What are the new Domain and Forest Functional Levels in Windows Server 2008/R2?

Domain Function Levels

To activate a new domain function level, all DCs in the domain must be running the right operating system. After this requirement is met, the administrator can raise the domain functional level. Here's a list of the available domain function levels available in Windows Server 2008:

Windows 2000 Native Mode

This is the default function level for new Windows Server 2008 Active Directory domains.

Supported Domain controllers – Windows 2000, Windows Server 2003, Windows Server 2008.

Windows Server 2003 Mode

To activate the new domain features, all domain controllers in the domain must be running Windows Server 2003. After this requirement is met, the administrator can raise the domain functional level to Windows Server 2003.

Supported Domain controllers – Windows Server 2003, Windows Server 2008.

Windows Server 2008 Mode

Supported Domain controllers – Windows Server 2008.

Windows 2008 Forest function levels

Forest functionality activates features across all the domains in your forest. To activate a new forest function level, all the domain in the forest must be running the right operating system and be set to the right domain function level. After this requirement is met, the administrator can raise the forest functional level. Here's a list of the available forest function levels available in Windows Server 2008:

Windows 2000 forest function level

This is the default setting for new Windows Server 2008 Active Directory forests.

Supported Domain controllers in all domains in the forest – Windows 2000, Windows Server 2003, Windows Server 2008.

Windows Server 2003 forest function level

To activate new forest-wide features, all domain controllers in the forest must be running Windows Server 2003.

Supported Domain controllers in all domains in the forest – Windows Server 2003, Windows Server 2008.

Windows Server 2008 forest function level

To activate new forest-wide features, all domain controllers in the forest must be running Windows Server 2008.

Supported Domain controllers in all domains in the forest – Windows Server 2008.

To activate the new domain features, all domain controllers in the domain must be running Windows Server 2008. After this requirement is met, the administrator can raise the domain functional level to Windows Server 2008.

When a child domain is created in the domain tree, what type of trust relationship exists between the new child domain and the trees root domain?

Transitive and two way.

<http://technet.microsoft.com/en-us/library/cc775736%28WS.10%29.aspx>

Which Windows Server 2008 tools make it easy to manage and configure a servers roles and features?

The Server Manager window enables you to view the roles and features installed on a server and also to quickly access the tools used to manage these various roles and features. The Server Manager can be used to add and remove roles and features as needed

What is WDS? How is WDS configured and managed on a server running Windows Server 2008?

The Windows Deployment Services is the updated and redesigned version of Remote Installation Services (RIS). Windows Deployment Services enables you to deploy Windows operating systems, particularly Windows Vista. 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 a CD or DVD.

Benefits of Windows Deployment Services

Windows Deployment Services provides organizations with the following benefits:

- Allows network-based installation of Windows operating systems, which reduces the complexity and cost when compared to manual installations.
- Deploys Windows images to computers without operating systems.
- Supports mixed environments that include Windows Vista, Microsoft Windows XP and Microsoft Windows Server 2003.
- Built on standard Windows Vista setup technologies including Windows PE, .wim files, and image-based setup.

Prerequisites for installing Windows Deployment Services

Your computing environment must meet the following technical requirements to install Windows Deployment Services:

- **Active Directory.** A Windows Deployment Services server must be either a member of an Active Directory domain or a domain controller for an Active Directory domain. The Active Directory domain and forest versions are irrelevant; all domain and forest configurations support Windows Deployment Services.
- **DHCP.** You must have a working Dynamic Host Configuration Protocol (DHCP) server with an active scope on the network because Windows Deployment Services uses PXE, which relies on DHCP for IP addressing.
- **DNS.** You must have a working Dynamic Name Services (DNS) server on the network to run Windows Deployment Services.
- **An NTFS partition.** The server running Windows Deployment Services requires an NTFS file system volume for the image store.
- **Credentials.** To install the role, you must be a member of the Local Administrators group on the Windows Deployment Services server. To install an image, you must be a member of the Domain Users group.
- **Windows Server 2003 SP1 or SP2 with RIS installed.** RIS does not have to be configured, but must be installed.

http://technet.microsoft.com/en-us/library/cc766320%28WS.10%29.aspx#BKMK_1

Name some of the major changes in GPO in Windows Server 2008.

Cost savings through power options

In Windows Server 2008, all power options have been Group Policy enabled, providing a potentially significant cost savings. Controlling power options through Group Policy could save organizations a significant amount of money. You can modify specific power options through individual Group Policy settings or build a custom power plan that is deployable by using Group Policy.

Ability to block device installation

In Windows Server 2008, you can centrally restrict devices from being installed on computers in your organization. You will now be able to create policy settings to control access to devices such as USB drives, CD-RW drives, DVD-RW drives, and other removable media.

Improved security settings

In Windows Server 2008, the firewall and IPsec Group Policy settings are combined to allow you to leverage the advantages of both technologies, while eliminating the need to create and maintain duplicate functionality. Some scenarios supported by these combined firewall and IPsec policy settings are secure server-to-server communications over the Internet, limiting access to domain resources based on trust relationships or health of a computer, and protecting data communication to a specific server to meet regulatory requirements for data privacy and security.

Expanded Internet Explorer settings management

In Windows Server 2008, you can open and edit Internet Explorer Group Policy settings without the risk of inadvertently altering the state of the policy setting based on the configuration of the administrative workstation. This change replaces earlier behavior in which some Internet Explorer policy settings would change based on the policy settings enabled on the administrative workstation used to view the settings.

Printer assignment based on location

The ability to assign printers based on location in the organization or a geographic location is a new feature in Windows Server 2008. In Windows Server 2008, you can assign printers based on site location. When mobile users move to a different location, Group Policy can update their printers for the new location. Mobile users returning to their primary locations see their usual default printers.

Printer driver installation delegated to users

In Windows Server 2008, administrators can now delegate to users the ability to install printer drivers by using Group Policy. This feature helps to maintain security by limiting distribution of administrative credentials.

What is the AD Recycle Bin? How do you use it?

Active Directory Recycle Bin helps minimize directory service downtime by enhancing your ability to preserve and restore accidentally deleted Active Directory objects without restoring Active Directory data from backups, restarting Active Directory Domain Services (AD DS), or rebooting domain controllers.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion. For example, restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains.

Active Directory Recycle Bin is functional for both AD DS and Active Directory Lightweight Directory Services (AD LDS) environments.

By default, Active Directory Recycle Bin in Windows Server 2008 R2 is disabled. To enable it, you must first raise the forest functional level of your AD DS or AD LDS environment to Windows Server 2008 R2, which in turn requires all forest domain controllers or all servers that host instances of AD LDS configuration sets to be running Windows Server 2008 R2.

To enable Active Directory Recycle Bin using the Enable-ADOptionalFeature cmdlet

1. Click **Start**, click **Administrative Tools**, right-click **Active Directory Module for Windows PowerShell**, and then click **Run as administrator**.
1. At the Active Directory module for Windows PowerShell command prompt, type the following command, and then press ENTER:

```
Enable-ADOptionalFeature -Identity <ADOptionalFeature> -Scope <ADOptionalFeatureScope> -Target <ADEntity>
```

For example, to enable Active Directory Recycle Bin for contoso.com, type the following command, and then press ENTER:

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=contoso,DC=com' -Scope ForestOrConfigurationSet -Target 'contoso.com'
```

What are AD Snapshots? How do you use them?

A snapshot is a shadow copy—created by the Volume Shadow Copy Service (VSS)—of the volumes that contain the Active Directory database and log files. With Active Directory snapshots, you can view the data inside such a snapshot on a domain controller without the need to start the server in Directory Services Restore Mode.

Windows Server 2008 has a new feature allowing administrators to create snapshots of the Active Directory database for offline use. With AD snapshots you can mount a backup of AD DS under a different set of ports and have read-only access to your backups through LDAP.

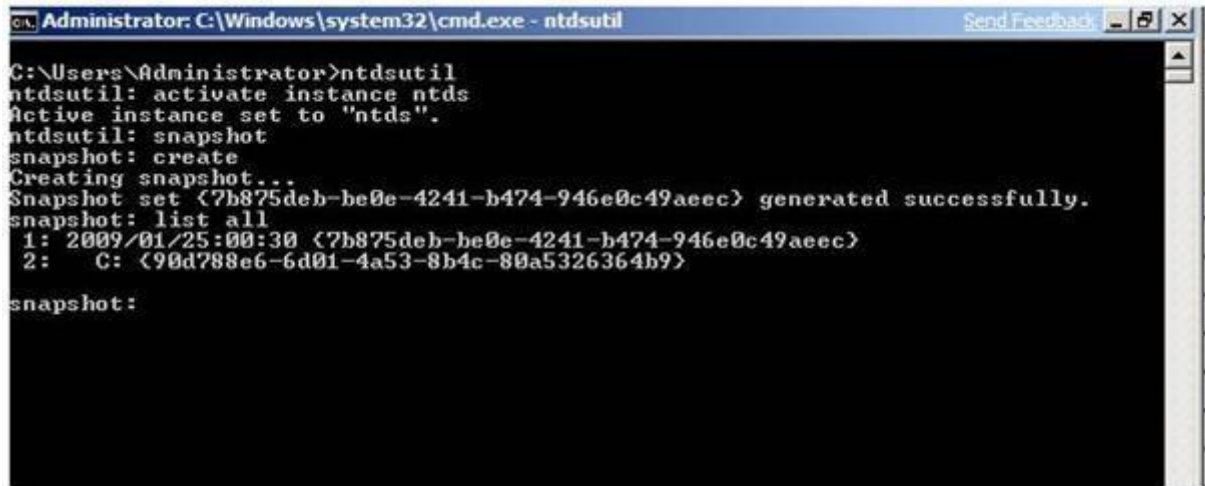
There are quite a few scenarios for using AD snapshots. For example, if someone has changed properties of AD objects and you need to revert to their previous values, you can mount a copy of a previous snapshot to an alternate port and easily export the required attributes for every object that was changed. These values can then be imported into the running instance of AD DS. You can also restore deleted objects or simply view objects for diagnostic purposes.

It does not allow you to move or copy items or information from the snapshot to the live database. In order to do that you will need to manually export the relevant objects or attributes from the snapshot, and manually import them back to the live AD database.

Steps for using Snapshot:

1. Create a snapshot:

open CMD.exe, Ntdsutil, activate instance ntds, snapshot, create, list all.



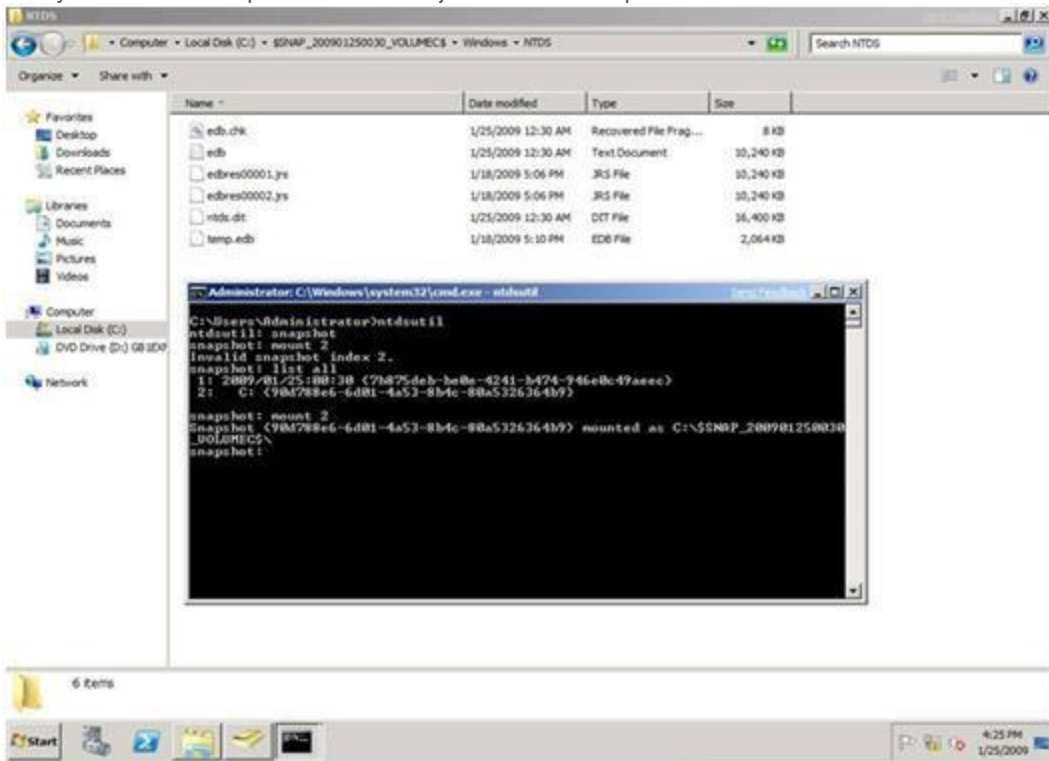
```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: snapshot
snapshot: create
Creating snapshot...
Snapshot set <7b875deb-be0e-4241-b474-946e0c49aee> generated successfully.
snapshot: list all
1: 2009/01/25:00:30 <7b875deb-be0e-4241-b474-946e0c49aee>
2: C: <90d788e6-6d01-4a53-8b4c-80a5326364b9>

snapshot:
```

2. Mounting an Active Directory snapshot:

Before connecting to the snapshot we need to mount it. By looking at the results of the List All command in above step, identify the snapshot that you wish to mount, and note the number next to it.

Type Ntdsutil, Snapshot, List all, Mount 2. The snapshot gets mounted to c:\\$SNAP_200901250030_VOLUMEC\$. Now you can refer this path to see the objects in these snapshots.

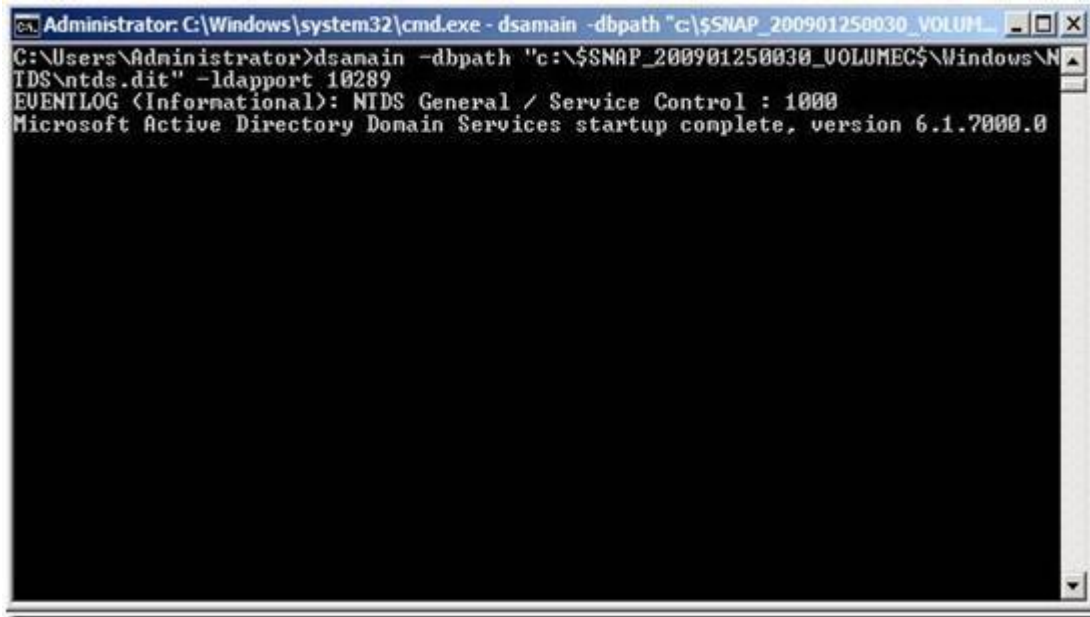


3. Connecting an Active Directory snapshot:

In order to connect to the AD snapshot you've mounted you will need to use the DSAMAIN command. DSAMAIN is a command-line tool that is built into Windows Server 2008. It is available if you have the Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS) server role installed.

After using DSAMAIN to expose the information inside the AD snapshot, you can use any GUI tool that can connect to the specified port, tools such as Active Directory Users and Computers (DSA.msc), ADSIEDIT.msc, LDP.exe or others. You can also connect to it by using command line tools such as LDIFDE or CSVDE, tools that allow you to export information from that database.

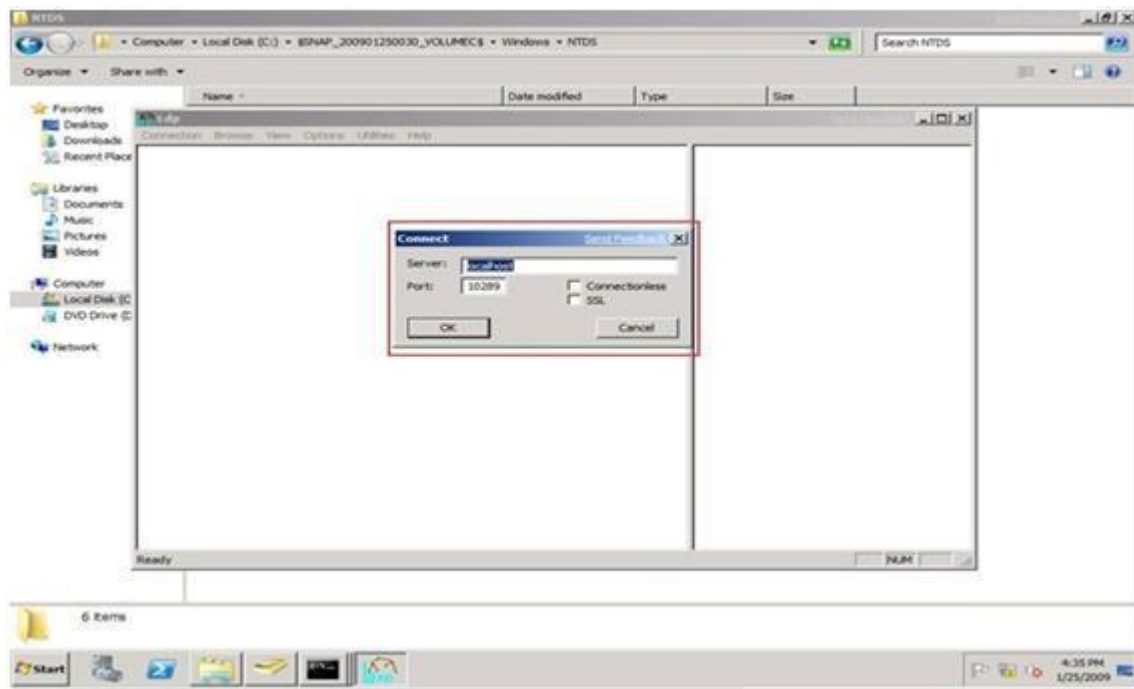
dsamain -dbpath "c:\\$SNAP_200901250030_VOLUMEC\$\Windows\NTDS\ntds.dit" -ldapport 10289



```
Administrator: C:\Windows\system32\cmd.exe - dsamain -dbpath "c:\$SNAP_200901250030_VOLUMEC$\Windows\NTDS\ntds.dit" -ldapport 10289
C:\Users\Administrator>dsamain -dbpath "c:\$SNAP_200901250030_VOLUMEC$\Windows\NTDS\ntds.dit" -ldapport 10289
EVENTLOG (Informational): NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete, version 6.1.7000.0
```

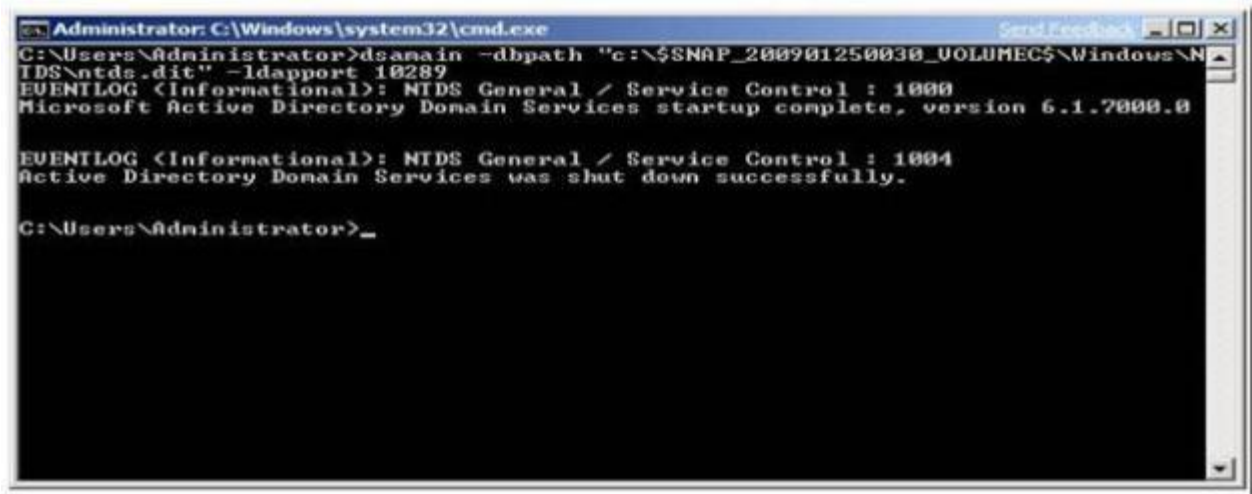
The above command will allow you to access the database using port 10289.

Now you can use LDP.exe tool to connect to this mounted instance.



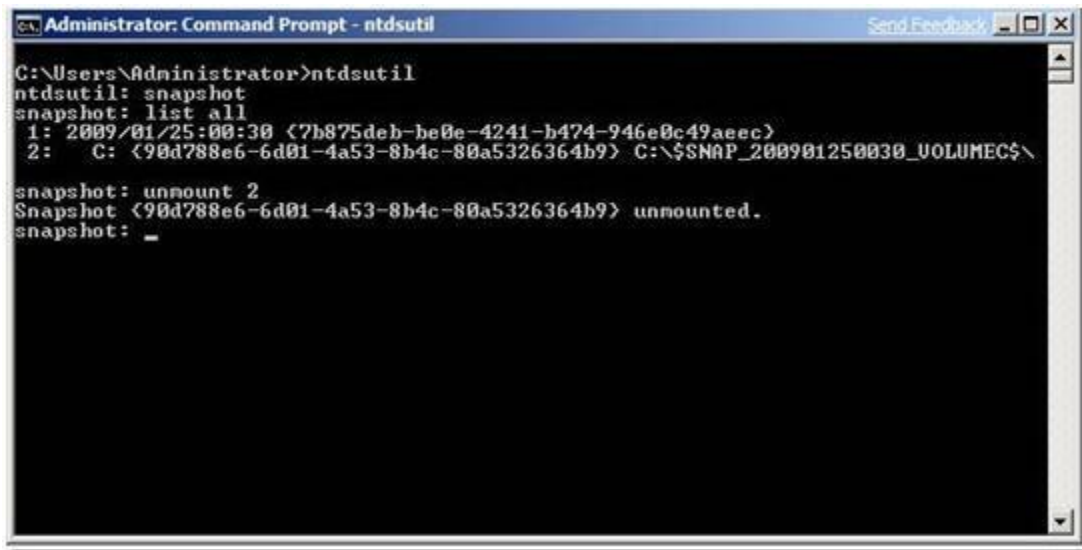
4. Disconnecting from the Active Directory snapshot:

In order to disconnect from the AD snapshot all you need to do is to type CTRL+C at the DSAMAIN command prompt window. You'll get a message indicating that the DS shut down successfully.



5. Unmounting the snapshot:

Run command, Ntfsutil, Snapshot, List all, Unmount 2.



```
Administrator: Command Prompt - ntdsutil
C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: list all
1: 2009/01/25:00:30 <7b875deb-be8e-4241-b474-946e8c49aee>
2: C: <90d788e6-6d01-4a53-8b4c-80a5326364b9> C:\$SNAP_200901250030_VOLUME$
snapshot: unmount 2
Snapshot <90d788e6-6d01-4a53-8b4c-80a5326364b9> unmounted.
snapshot: _
```

What is Offline Domain Join? How do you use it?

You can use offline domain join to join computers to a domain without contacting a domain controller over the network. You can join computers to the domain when they first start up after an operating system installation. No additional restart is necessary to complete the domain join. This helps reduce the time and effort required to complete a large-scale computer deployment in places such as datacenters.

For example, an organization might need to deploy many virtual machines within a datacenter. Offline domain join makes it possible for the virtual machines to be joined to the domain when they initially start following the operating system installation. No additional restart is required to complete the domain join. This can significantly reduce the overall time required for wide-scale virtual machine deployments.

A domain join establishes a trust relationship between a computer running a Windows operating system and an Active Directory domain. This operation requires state changes to AD DS and state changes on the computer that is joining the domain. To complete a domain join in the past using previous Windows operating systems, the computer that joined the domain had to be running and it had to have network connectivity to contact a domain controller. Offline domain join provides the following advantages over the previous requirements:

- The Active Directory state changes are completed without any network traffic to the computer.
- The computer state changes are completed without any network traffic to a domain controller.
- Each set of changes can be completed at a different time.

<http://technet.microsoft.com/en-us/library/offline-domain-join-djoin-step-by-step%28WS.10%29.aspx>

What are Fine-Grained Passwords? How do you use them?

You can use fine-grained password policies to specify multiple password policies within a single domain. You can use fine-grained password policies to apply different restrictions for password and account lockout policies to different sets of users in a domain.

For example, you can apply stricter settings to privileged accounts and less strict settings to the accounts of other users. In other cases, you might want to apply a special password policy for accounts whose passwords are synchronized with other data sources.

Talk about Restartable Active Directory Domain Services in Windows Server 2008/R2. What is this feature good for?

Restartable AD DS is a feature in Windows Server 2008 that you can use to perform routine maintenance tasks on a domain controller, such as applying updates or performing offline defragmentation, without restarting the server.

While AD DS is running, a domain controller running Windows Server 2008 behaves the same way as a domain controller running Microsoft® Windows® 2000 Server or Windows Server 2003.

While AD DS is stopped, you can continue to log on to the domain by using a domain account if other domain controllers are available to service the logon request. You can also log on to the domain with a domain account while the domain controller is started in Directory Services Restore Mode (DSRM) if other domain controllers are available to service the logon request.

If no other domain controller is available, you can log on to the domain controller where AD DS is stopped in Directory Services Restore Mode (DSRM) only by using the DSRM Administrator account and password by default, as in Windows 2000 Server Active Directory or Windows Server 2003 Active Directory.

Benefits of restartable AD DS

Restartable AD DS reduces the time that is required to perform offline operations such as offline defragmentation. It also improves the availability of other services that run on a domain controller by keeping them running when AD DS is stopped. In combination with the Server Core installation option of Windows Server 2008, restartable AD DS reduces the overall servicing requirements of a domain controller.

In Windows 2000 Server Active Directory and Windows Server 2003 Active Directory, you must restart the domain controller in DSRM when you perform offline defragmentation of the database or apply security updates. In contrast, you can stop Windows Server 2008 AD DS as you stop other services that are running locally on the server. This makes it possible to perform offline AD DS operations more quickly than you could with Windows 2000 Server and Windows Server 2003.

You can use Microsoft Management Console (MMC) snap-ins, or the Net.exe command-line tool, to stop or restart Active Directory® Domain Services (AD DS) in the Windows Server® 2008 operating system. You can stop AD DS to perform tasks, such as offline defragmentation of the AD DS database, without restarting the domain controller. Other services that run on the server, but that do not depend on AD DS to function, are available to service client requests while AD DS is stopped. An example of such a service is Dynamic Host Configuration Protocol (DHCP).

Windows 2008 Server Interview Questions Part II

OCTOBER 19, 2011 [4 COMMENTS](#)

1. What are the Important Windows port numbers:

RDP – 3389 – (windows rdp port number and remote desktop port number)
FTP – 21 – (file transfer protocol)
TFTP – 69 – (tftp port number)
Telnet – 23 – (telnet port number)
SMTP – 25 – (SMTP port number)
DNS – 53 – (dns port number and Domain Name System port number)
DHCP – 68 – (DHCP port number and Dynamic Host Configuration Protocol port number)
POP3 – 110 – (post office Protocol 3 port)
HTTP – 80 – (http port number)
HTTPS – 443 – (https port number)
NNTP – 119 – (Network News Transfer Protocol Port number)
NTP – 123 – (ntp port number and network Time Protocol and SNTP port number)
IMAP – 143 – (Internet Message Access Protocol port number)
SSMTP – 465 – (SMTP Over SSI)
SIMAP – 993 – (IMAP Over SSL)
SPOP3 – 995 – (POP# Over SS L)
Time – 123 – (ntp port number and network Time Protocol and SNTP port number)
NetBios – 137 – (Name Service)
NetBios – 139 – (Datagram Service)
DHCP Client – 546 – (DHCP Client port number)
DHCP Server – 547 – (DHCP Server port number)
Global Catalog – 3268 – (Global Catalog port number)
LDAP – 389 – (LDAP port number and Lightweight Directory Access Protocol port number)
RPC – 135 – (remote procedure call Port number)
Kerberos – 88 – (Kerberos Port Number)
SSH – 22 – (ssh port number and Secure Shell port number)

2. How to check tombstone lifetime value in your Forest

Tombstone lifetime value different from OS to OS, for windows server 2000/2003 it's 60 days, In Windows Server 2003 SP1, default tombstone lifetime (TSL) value has increased from 60 days to 180 days, again in Windows Server 2003 R2 TSL value has been decreased to 60 days, Windows Server 2003 R2 SP2 and windows server 2008 it's 180 days

If you migrating windows 2003 environment to windows 2008 then its 60 day's
you can use the below command to check/view the current tombstone lifetime value for your Domain/Forest
dsquery * "cn=directory service,cn=windows nt,cn=services,cn=configuration,dc=" –scope base –attr tombstonelifetime

Replace forestDN with your domain partition DN, for domainname.com the DN would be dc=domainname, dc=com

Source: [http://technet.microsoft.com/en-us/library/cc784932\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc784932(WS.10).aspx)

3. How to find the domain controller that contains the lingering object

If we enable Strict Replication Consistency

Lingering objects are not present on domain controllers that log Event ID 1988. The source domain controller contains the lingering object

If we doesn't enable Strict Replication Consistency

Lingering objects are not present on domain controllers that log Event ID 1388. Domain controller that doesn't log Event ID 1388 and that domain controller contain the lingering object

You have a 100 Domain controllers which doesn't enable Strict Replication Consistency, then you will get the Event ID 1388 on all the 99 Domain controllers except the one that contain the lingering object

Need to Remove Lingering Objects from the affected domain controller or decommission the domain controller

You can use Event Comb tool (Eventcombmt.exe) is a multi-threaded tool that can be used to gather specific events from the Event Viewer logs of different computers at the same time.

You can download these tools from the following location:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en>

4. What are Active Directory ports:

List of Active Directory Ports for Active Directory replication and Active Directory authentication, this ports can be used to configure the Firewall

Active Directory replication- There is no defined port for Active Directory replication, Active Directory replication remote procedure calls (RPC) occur dynamically over an available port through RPCSS (RPC Endpoint Mapper) by using port 135

File Replication Services (FRS)- There is no defined port for FRS, FRS replication over remote procedure calls (RPCs) occurs dynamically over an available port by using RPCSS (RPC Endpoint Mapper) on port 135

Other required ports for Active Directory

TCP 53 – DSN (DNS Download)

UDP 53 – DSN (DNS Queries)

TCP 42- WINS

UDP 42- WINS

TCP 3389- RDP (Remote Desktop)

TCP 135 – MS-RPC

TCP 1025 & 1026 – AD Login & replication

TCP 389 – LDAP

TCP 639 – LDAP over SSL/TLS

TCP 3268 -Global Catalog

TCP 3268 – Global Catalog over SSL/TSL

UDP 137 & 138 – NetBIOS related

UDP 88 – Kerberos v5

TCP 445 – SMB , Microsoft-ds

TCP 139 – SMB

5. How to do active directory health checks?

As an administrator you have to check your active directory health daily to reduce the active directory related issues, if you are not monitoring the health of your active directory what will happen

Let's say one of the Domain Controller failed to replicate, first day you will not have any issue. If this will continue then you will have login issue and you will not find the object change and new object, that's created and changed in other Domain Controller this will lead to other issues

If the Domain Controller is not replicated more then 60 day's then it will lead to Lingering issue

Command to check the replication to all the DC's(through this we can check Active Directory Health)

Repadmin /replsum /bysrc /bydest /sort:delta

You can also save the command output to text file, by using the below command

Repadmin /replsum /bysrc /bydest /sort:delta >>c:\replication_report.txt

this will list the domain controllers that are failing to replicate with the delta value

You can daily run this to check your active directory health

6. GPRESULT failed with access denied error:

Unable to get the result from gpresult on windows 2003 server, gpresult return with the access denied errors, you can able to update the group policy without issue

Run the following commands to register the userenv.dll and recompile the rsop mof file

To resolve the access denied error while doing the gpresult.

1. Open a cmd

1. re-register the userenv.dll

Regsvr32 /n /l c:\winnt\system32\userenv.dll

2. CD c:\windows\system32\wbem

3. Mofcomp scersop.mof

4. Gpupdate /force

5. Gpresult

Now you able to run the gpresult without error and even server reboot not required for this procedure

7. What is the command to find out site name for given DC

dsquery server NYDC01 -site

domain controller name = NYDC01

8. Command to find all DCs in the given site

Command to find all the Domain Controllers in the "Default-First-Site-Name" site

dsquery server -o rdn -site Default-First-Site-Name

Site name = Default-First-Site-Name

9. How many types of queries DNS does?

Iterative Query

Recursive Query

Iterative Query

In this query the client ask the name server for the best possible answer, the name server check the cache and zone for which it's authoritative and returns the best possible answer to the client, which would be the full answer like IP address or try the other name server

Recursive Query

Client demands either a full answer or an error message (like record or domain name does not exist)

Client machine always send recursive query to the DNS server, if the DNS server does not have the requested information, DNS server send the iterative query to the other name server (through forwarders or secondary DNS server) until it gets the information, or until the name query fails.

System Administrator – Active Directory Interview Questions and Answers

[Uncategorized](#) March 14, 2012 [Comments: 29](#)

1) What is Active Directory?

ACTIVE DIRECTORY IS A CENTRALIZED DATABASE ...WHICH IS USED IN DOMAIN FOR ADMINISTRATIVE PURPOSES...

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. It is primarily used for online information and was originally created in 1996 and first used with Windows 2000.

An active directory (sometimes referred to as an AD) does a variety of functions including the ability to provide information on objects, helps organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.

An active directory can be defined as a hierarchical structure and this structure is usually broken up into three main categories, the resources which might include hardware such as printers, services for end users such as web email servers and objects which are the main functions of the domain and network.

It is interesting to note the framework for the objects. Remember that an object can be a piece of hardware such as a printer, end user or security settings set by the administrator. These objects can hold other objects within their file structure. All objects have an ID, usually an object name (folder name). In addition to these objects being able to hold other objects, every object has its own attributes which allows it to be characterized by the information which it contains. Most IT professionals call these setting or characterizations schemas.

Depending on the type of schema created for a folder, will ultimately determine how these objects are used. For instance, some objects with certain schemas can not be deleted, they can only be deactivated. Others types of schemas with certain attributes can be deleted entirely. For instance, a user object can be deleted, but the administrator object can not be deleted.

When understanding active directories, it is important to know the framework that objects can be viewed at. In fact, an active directory can be viewed at either one of three levels; these levels are called forests,

trees or domains. The highest structure is called the forest because you can see all objects included within the active directory.

Within the Forest structure are trees, these structures usually hold one or more domains, going further down the structure of an active directory are single domains. To put the forest, trees and domains into perspective, consider the following example.

A large organization has many dozens of users and processes. The forest might be the entire network of end users and specific computers at a set location. Within this forest directory are now trees that hold information on specific objects such as domain controllers, program data, system, etc. Within these objects are even more objects which can then be controlled and categorized

Another Answer

Active Directory in Windows Server 2003

The Active Directory is the one of the important part of Windows Server 2003 networking .First need to know and understand Active directory. How does it work? It makes information easy for the administrator and the users. You can use the Active Directory to design an organization's structure according to the requirement. If you are using the Active Directory then you can scale active directory from a single computer to a single network or too many networks. In active directory you can include every object server and domain in a network.

Logical Component

In the organization you set up in Windows Server 2003 and the organization you set up in Exchange Server 2003 are the same and the same is the case with Windows 2000 and Exchange 2000 as well. Now I am going to tell you its advantage one user administrator manage all aspects of user configuration. These logical constructs which are described in the following subsections allow you to define and group resources so that they can be located and administered by the name rather than by physical location.

Objects

Object is the basic unit in the Active Directory. It is an apocarpous named set of features that represents something adjective such as a user, printer and the application. A user is also an object. In Exchange a user's features include its name and location, surrounded by other things.

Organization Unit

Organization Unit is a persona in which you can keep objects such as user accounts, groups, computer, and printer. Applications and other (OU). In organization unit you can assign specific permission to the users. Organization unit can also be used to create departmental limitation.

Domains

Domains is a group of computers and other resources that are part of a network and share a common directory database. Once a server has been installed, you can use the Active Directory Wizard to install Active Directory in order to install Active directory on the first server on the network, that server must have the access to a server running DNS (Domain Name Service). If you don't have installed this service on your server then you will have to install this service during the Active Directory installation...

Active Directory in Windows Server 2003

The Active Directory is the one of the important part of Windows Server 2003 networking. First need to know and understand Active directory. How does it work? It makes information easy for the administrator and the users. You can use the Active Directory to design an organization's structure according to the requirement. If you are using the Active Directory then you can scale active directory from a single computer to a single network or too many networks. In active directory you can include every object server and domain in a network.

Logical Component

In the organization you set up in Windows Server 2003 and the organization you set up in Exchange Server 2003 are the same and the same is the case with Windows 2000 and Exchange 2000 as well. Now I am going to tell you its advantage one user administrator manage all aspects of user configuration. These logical constructs which are described in the following subsections allow you to define and group resources so that they can be located and administered by the name rather than by physical location.

Objects

Object is the basic unit in the Active Directory. It is an apocarpous named set of features that represents something adjective such as a user, printer and the application. A user is also an object. In Exchange a user's features include its name and location, surrounded by other things.

Organization Unit

Organization Unit is a persona in which you can keep objects such as user accounts, groups, computer, and printer. Applications and other (OU). In organization unit you can assign specific permission to the user's. Organization unit can also be used to create departmental limitation.

Domains

Domains is a group of computers and other resources that are part of a network and share a common directory database. Once a server has been installed, you can use the Active Directory Wizard to install Active Directory in order to install Active directory on the first server on the network, that server must have the access to a server running DNS (Domain Name Service). If you don't have installed this service on your server then you will have to install this service during the Active Directory installation...

Another Answer

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. It is primarily used for online information and was originally created in 1996 and first used with Windows 2000.

An active directory (sometimes referred to as an AD) does a variety of functions including the ability to provide information on objects, helps organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.

An active directory can be defined as a hierarchical structure and this structure is usually broken up into three main categories, the resources which might include hardware such as printers, services for end users such as web email servers and objects which are the main functions of the domain and network.

It is interesting to note the framework for the objects. Remember that an object can be a piece of hardware such as a printer, end user or security settings set by the administrator. These objects can hold other objects within their file structure. All objects have an ID, usually an object name (folder name). In addition to these objects being able to hold other objects, every object has its own attributes which allows it to be characterized by the information which it contains. Most IT professionals call these setting or characterizations schemas.

Depending on the type of schema created for a folder, will ultimately determine how these objects are used. For instance, some objects with certain schemas can not be deleted, they can only be deactivated.

Others types of schemas with certain attributes can be deleted entirely. For instance, a user object can be deleted, but the administrator object can not be deleted.

When understanding active directories, it is important to know the framework that objects can be viewed at. In fact, an active directory can be viewed at either one of three levels; these levels are called forests, trees or domains. The highest structure is called the forest because you can see all objects included within the active directory.

Within the Forest structure are trees, these structures usually hold one or more domains, going further down the structure of an active directory are single domains. To put the forest, trees and domains into perspective, consider the following example.

A large organization has many dozens of users and processes. The forest might be the entire network of end users and specific computers at a set location. Within this forest directory are now trees that hold information on specific objects such as domain controllers, program data, system, etc. Within these objects are even more objects which can then be controlled and categorized.

2) What is LDAP?

LDAP means Light-Weight Directory Access Protocol. It determines how an object in an Active directory should be named. LDAP (Lightweight Directory Access Protocol) is a proposed open standard for accessing global or local directory services over a network and/or the Internet. A directory, in this sense, is very much like a phone book. LDAP can handle other information, but at present it is typically used to associate names with phone numbers and email addresses. LDAP directories are designed to support a high volume of queries, but the data stored in the directory does not change very often. It works on port no. 389. LDAP is sometimes known as X.500 Lite. X.500 is an international standard for directories and full-featured, but it is also complex, requiring a lot of computing resources and the full OSI stack. LDAP, in contrast, can run easily on a PC and over TCP/IP. LDAP can access X.500 directories but does not support every capability of X.500

ANSWER B:

The Lightweight Directory Access Protocol or LDAP is an application protocol for querying and modifying directory services running over TCP/IP. [1]A directory is a set of objects with attributes organized in a logical and hierarchical manner. The most common example is the telephone directory, which consists of

a series of names (either of persons or organizations) organized alphabetically, with each name having an address and phone number attached.

An LDAP directory tree often reflects various political, geographic, and/or organizational boundaries, depending on the model chosen. LDAP deployments today tend to use Domain name system (DNS) names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else that represents a given tree entry (or multiple entries).

Its current version is LDAPv3, which is specified in a series of Internet Engineering Task Force (IETF) Standard Track Requests for comments (RFCs) as detailed in RFC 4510.

3) Can you connect Active Directory to other 3rd-party Directory Services? Name a few options.

Yes, you can use dirXML or LDAP to connect to other directories (ie. E-directory from Novell). Novell eDirectory, formerly called Novell Directory Services (NDS)

4) Where is the AD database held? What other folders are related to AD?

AD Database is saved in/ntds. You can see other files also in this folder. These are the main files controlling the AD structure •ntds.dit

- edb.log

- res1.log

- res2.log

- edb.chk

- SysVOL folder is also created which is used for replication

When a change is made to the Win2K database, triggering a write operation, Win2K records the transaction in the log file (edb.log). Once written to the log file, the change is then written to the AD database. System performance determines how fast the system writes the data to the AD database from the log file. Any time the system is shut down; all transactions are saved to the database.

During the installation of AD, Windows creates two files: res1.log and res2.log. The initial size of each is 10MB. These files are used to ensure that changes can be written to disk should the system run out of free disk space. The checkpoint file (edb.chk) records transactions committed to the AD database (ntds.dit). During shutdown, a "shutdown" statement is written to the edb.chk file. Then, during a reboot, AD determines that all transactions in the edb.log file have been committed to the AD database. If, for some reason, the edb.chk file doesn't exist on reboot or the shutdown statement isn't present, AD will use the edb.log file to update the AD database.

The last file in our list of files to know is the AD database itself, ntds.dit. By default, the file is located in \NTDS, along with the other files we've discussed

5) What is the SYSVOL folder?

All active directory data base security related information store in SYSVOL folder and it's only created on NTFS partition.

B:

The Sysvol folder on a Windows domain controller is used to replicate file-based data among domain controllers. Because junctions are used within the Sysvol folder structure, Windows NT file system (NTFS) version 5.0 is required on domain controllers throughout a Windows distributed file system (DFS) forest.

This is a quote from Microsoft themselves; basically the domain controller info stored in files like your group policy stuff is replicated through this folder structure

6) Name the AD NCs and replication issues for each NC

*Schema NC, *Configuration NC, * DomainNC

Schema NC This NC is replicated to every other domain controller in the forest. It contains information about the Active Directory schema, which in turn defines the different object classes and attributes within Active Directory.

Configuration NC Also replicated to every other DC in the forest, this NC contains forest-wide configuration information pertaining to the physical layout of Active Directory, as well as information about display specifics and forest-wide Active Directory quotas.

Domain NC This NC is replicated to every other DC within a single Active Directory domain. This is the NC that contains the most commonly-accessed Active Directory data: the actual users, groups, computers, and other objects that reside within a particular Active Directory domain.

7) What are application partitions? When do I use them?

Application directory partitions: These are specific to Windows Server 2003 domains.

An application directory partition is a directory partition that is replicated only to specific domain controllers. A domain controller that participates in the replication of a particular application directory partition hosts a replica of that partition. Only Domain controllers running Windows Server 2003 can host a replica of an application directory partition.

8) How do you create a new application partition?

When you create an application directory partition, you are creating the first instance of this partition. You can create an application directory partition by using the create nc option in the domain management menu of Ntdsutil. When creating an application directory partition using LDP or ADSI, provide a description in the description attribute of the domain DNS object that indicates the specific application that will use the partition. For example, if the application directory partition will be used to store data for a Microsoft accounting program, the description could be Microsoft accounting application. Ntdsutil does not facilitate the creation of a description.

To create or delete an application directory partition

1. Open Command Prompt.

2. Type:

Ntdsutil

3. At the Ntdsutil command prompt, type:

Domain management

4. At the domain management command prompt, do one of the following:

· To create an application directory partition, type:

Create ncApplicationDirectoryPartitionDomainController

Answer:

Start >> RUN>> CMD >> type there "NTDSUTIL" Press Enter

Ntdsutil: domain management Press Enter

Domain Management: Create NC dc=, dc=, dc=com <>

ANSWER B

Create an application directory partition by using the DnsCmd command

Use the DnsCmd command to create an application directory partition. To do this, use the following syntax:

DnsCmd ServerName /CreateDirectoryPartition FQDN of partition

To create an application directory partition that is named CustomDNSPartition on a domain controller that is named DC-1, follow these steps:

1. Click Start, click Run, type cmd, and then click OK.
2. Type the following command, and then press ENTER:dnscmd DC-1 /createdirectorypartition CustomDNSPartition.contoso.com

When the application directory partition has been successfully created, the following information appears:

DNS Server DC-1 created directory partition: CustomDNSPartition.contoso.com Command completed successfully.

Configure an additional domain controller DNS server to host the application directory partition

Configure an additional domain controller that is acting as a DNS server to host the new application directory partition that you created. To do this, use the following syntax with the DnsCmd command:

DnsCmd ServerName /EnlistDirectoryPartition FQDN of partition

To configure the example domain controller that is named DC-2 to host this custom application directory partition, follow these steps:

1. Click Start, click Run, type cmd, and then click OK.

2. Type the following command, and then press ENTER: `dnscmd DC-2 /enlistdirectorypartition CustomDNSPartition.contoso.com`

The following information appears:

DNS Server DC-2 enlisted directory partition: CustomDNSPartition.contoso.com Command completed successfully.

9) How do you view replication properties for AD partitions and DCs?

By using replication monitor

go to start > run > type **repadmin**

go to start > run > type **replmon**

10) What is the Global Catalog?

The global catalog contains a complete replica of all objects in Active Directory for its Host domain, and contains a partial replica of all objects in Active Directory for every other domain in the forest.

ANSWER B:

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

In addition to configuration and schema directory partition replicas, every domain controller in a Windows 2000 Server or Windows Server 2003 forest stores a full, writable replica of a single domain directory partition. Therefore, a domain controller can locate only the objects in its domain. Locating an object in a different domain would require the user or application to provide the domain of the requested object.

The global catalog provides the ability to locate objects from any domain without having to know the domain name. A global catalog server is a domain controller that, in addition to its full, writable domain directory partition replica, also stores a partial, read-only replica of all other domain directory partitions in the forest. The additional domain directory partitions are partial because only a limited set of attributes is

included for each object. By including only the attributes that are most used for searching, every object in every domain in even the largest forest can be represented in the database of a single global catalog server.

11) How do you view all the GCs in the forest?

```
C:\>repadmin /showreps  
domain_controller
```

OR

You can use Replmon.exe for the same purpose.

OR

AD Sites and Services and nslookup gc._msdcs.

To find the in GC from the command line you can try using DSQUERY command.

dsquery server -isgc to find all the GC's in the forest

you can try dsquery server -forest -isgc.

12) Why not make all DCs in a large forest as GCs?

The reason that all DCs are not GCs to start is that in large (or even Giant) forests the DCs would all have to hold a reference to every object in the entire forest which could be quite large and quite a replication burden.

For a few hundred, or a few thousand users even, this not likely to matter unless you have really poor WAN lines.

13) Trying to look at the Active Directory Schema, how can I do that?

Option to view the schema

Register schmmgmt.dll using this command

```
c:\windows\system32>regsvr32 schmmgmt.dll
```

Open mmc -> add snapin -> add Active directory schema

name it as schema.msc

Open administrative tool -> schema.msc

14) What are the Support Tools? Why do I need them?

Support Tools are the tools that are used for performing the complicated tasks easily. These can also be the third party tools. Some of the Support tools include DebugViewer, DependencyViewer, RegistryMonitor, etc.

-edit by Casquehead

I believe this question is referring to the Windows Server 2003 Support Tools, which are included with Microsoft Windows Server 2003 Service Pack 2. They are also available for download here:

<http://www.Microsoft.com/downloads/details.aspx?familyid=96A35011-FD83-419D-939B-9A772EA2DF90&displaylang=en>

you need them because you cannot properly manage an Active Directory network without them. Here they are, it would do you well to familiarize yourself with all of them.

Acldiag.exe

Adsiedit.msc

Bitsadmin.exe

Dcdiag.exe

Dfsutil.exe

Dnslint.exe

Dsacis.exe

Iadstools.dll

Ktpass.exe

Ldp.exe

Netdiag.exe

Netdom.exe

Ntfrsutl.exe

Portqry.exe

Repadmin.exe

Replmon.exe

Setspn.exe

15) What is LDP? What is REPLMON? What is ADSIEDIT? What is NETDOM? What is REPADMIN?

What is LDP?

A:

The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP.[1]

A directory is a set of objects with attributes organized in a logical and hierarchical manner. The most common example is the telephone directory, which consists of a series of names (either of persons or organizations) organized alphabetically, with each name having an address and phone number attached. An LDAP directory tree often reflects various political, geographic, and/or organizational boundaries, depending on the model chosen. LDAP deployments today tend to use Domain name system (DNS) names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else that represents a given tree entry (or multiple entries).

Its current version is LDAPv3, which is specified in a series of Internet Engineering Task Force (IETF) Standard Track Requests for comments (RFCs) as detailed in RFC 4510.

LDAP means Light-Weight Directory Access Protocol. It determines how an object in an Active directory should be named. LDAP (Lightweight Directory Access Protocol) is a proposed open standard for accessing global or local directory services over a network and/or the Internet. A directory, in this sense, is very much like a phone book. LDAP can handle other information, but at present it is typically used to associate names with phone numbers and email addresses. LDAP directories are designed to support a high volume of queries, but the data stored in the directory does not change very often. It works on port no. 389. LDAP is sometimes known as X.500 Lite. X.500 is an international standard for directories and full-featured, but it is also complex, requiring a lot of computing resources and the full OSI stack. LDAP, in contrast, can run easily on a PC and over TCP/IP. LDAP can access X.500 directories but does not support every capability of X.500

What is REPLMON?

A: Replmon is the first tool you should use when troubleshooting Active Directory replication issues. As it is a graphical tool, replication issues are easy to see and somewhat easier to diagnose than using its command line counterparts. The purpose of this document is to guide you in how to use it, list some

common replication errors and show some examples of when replication issues can stop other network installation actions.

For more go to http://www.techtutorials.net/articles/replmon_howto_a.html

What is ADSIEDIT?

A: Adsiedit.msc is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for Active Directory. It is a Graphical User Interface (GUI) tool. Network administrators can use it for common administrative tasks such as adding, deleting, and moving objects with a directory service. The attributes for each object can be edited or deleted by using this tool.

Adsiedit.msc uses the ADSI application programming interfaces (APIs) to access Active Directory. The following are the required files for using this tool:

- ADSIEDIT.DLL
- ADSIEDIT.MSC

Regarding system requirements, a connection to an Active Directory environment and Microsoft Management Console (MMC) is necessary

What is NETDOM?

A: NETDOM is a command-line tool that allows management of Windows domains and trust relationships. It is used for batch management of trusts, joining computers to domains, verifying trusts, and secure channels

A:

Enables administrators to manage Active Directory domains and trust relationships from the command prompt.

Netdom is a command-line tool that is built into Windows Server 2008. It is available if you have the Active Directory Domain Services (AD DS) server role installed. To use Netdom, you must run the Netdom command from an elevated command prompt. To open an elevated command prompt, click Start, right-click Command Prompt, and then click Run as administrator.

You can use Netdom to:

Join a computer that runs Windows XP Professional or Windows Vista to a Windows Server 2008 or Windows Server 2003 or Windows 2000 or Windows NT 4.0 domain.

Provide an option to specify the organizational unit (OU) for the computer account.

Generate a random computer password for an initial Join operation.

Manage computer accounts for domain member workstations and member servers. Management operations include:

Add, Remove, Query.

An option to specify the OU for the computer account.

An option to move an existing computer account for a member workstation from one domain to another while maintaining the security descriptor on the computer account.

Establish one-way or two-way trust relationships between domains, including the following kinds of trust relationships:

From a Windows 2000 or Windows Server 2003 or Windows Server 2008 domain to a Windows NT 4.0 domain.

From a Windows 2000 or Windows Server 2003 or Windows Server 2008 domain to a Windows 2000 or Windows Server 2003 or Windows Server 2008 domain in another enterprise.

Between two Windows 2000 or Windows Server 2003 or Windows Server 2008 domains in an enterprise (a shortcut trust).

The Windows Server 2008 or Windows Server 2003 or Windows 2000 Server half of an interoperable Kerberos protocol realm.

Verify or reset the secure channel for the following configurations:

Member workstations and servers.

Backup domain controllers (BDCs) in a Windows NT 4.0 domain.

Specific Windows Server 2008 or Windows Server 2003 or Windows 2000 replicas.

Manage trust relationships between domains, including the following operations:

Enumerate trust relationships (direct and indirect).

View and change some attributes on a trust.

16) What are sites? What are they used for?

One or more well-connected (highly reliable and fast) TCP/IP subnets. A site allows administrators to configure Active Directory access and replication topology to take advantage of the physical network.

B: A Site object in Active Directory represents a physical geographic location that hosts networks. Sites contain objects called Subnets. [3] Sites can be used to Assign Group Policy Objects, facilitate the discovery of resources, manage active directory replication, and manage network link traffic. Sites can be linked to other Sites. Site-linked objects may be assigned a cost value that represents the speed,

reliability, availability, or other real property of a physical resource. Site Links may also be assigned a schedule

17) What's the difference between a site link's schedule and interval?

Schedule enables you to list weekdays or hours when the site link is available for replication to happen in the give interval. Interval is the re occurrence of the inter site replication in given minutes. It ranges from 15 – 10,080 mins. The default interval is 180 mins.

18) What is the KCC?

Knowledge consistency checker- it generates the replication topology by specifying what domain controllers will replicate to which other domain controllers in the site. The KCC maintains a list of connections, called a **replication topology**, to other domain controllers in the site. The KCC ensures that changes to any object are replicated to all site domain controllers and updates go through no more than three connections. Also an administrator can configure connection objects.

19) What is the ISTG? Who has that role by default?

Intersite Topology Generator (ISTG), which is responsible for the connections among the sites. By default Windows 2003 Forestlevel functionality has this role.

By Default the first Server has this role. If that server can no longer perform this role then the next server with the highest GUID then takes over the role of ISTG.

20) What are the requirements for installing AD on a new server?

- An NTFS partition with enough free space (250MB minimum)
- An Administrator's username and password
- The correct operating system version
- A NIC
- Properly configured TCP/IP (IP address, subnet mask and – optional – default gateway)
- A network connection (to a hub or to another computer via a crossover cable)
- An operational DNS server (which can be installed on the DC itself)

- A Domain name that you want to use
- The Windows 2000 or Windows Server 2003 CD media (or at least the i386 folder)

20) What can you do to promote a server to DC if you're in a remote location with slow WAN link?

First available in Windows 2003, you will create a copy of the system state from an existing DC and copy it to the new remote server. Run "Dcpromo /adv". You will be prompted for the location of the system state files

=====

Answer B:

Backup system state as;

1. Click **Start**, click **Run**, type ntbackup, and then click **OK**. (If the Backup utility starts in wizard mode, click the **Advanced Mode** hyperlink.)
2. From the **Backup** tab, click to select the **System State** check box in the left pane. Do not back up the file system part of the SYSVOL tree separately from the system state backup.
3. In the **Backup media or file name** box, specify the drive, path, and file name of the system state backup.

Name the file .bak (recommended and general)

Restore system stat as below on the target computer;

1. Log on to the Windows Server 2003-based computer that you want to promote. You must be a member of the local administrators group on this computer.
2. Click **Start**, click **Run**, type ntbackup, and then click **OK**. (If the Backup utility starts in wizard mode, click the **Advanced Mode** hyperlink.)
3. In the Backup utility, click the **Restore and Manage Media** tab. In the **Tools** menu, click **Catalog a backup file...**, and then locate the .bkf file that you created earlier. Click **OK**.
4. Expand the contents of the .bkf file, and then click to select the **System State** check box.
5. In **Restore files to:** click **Alternate Location**. To restore the system state, type the logical drive and the path. We suggest that you type X:\Ntdsrestore. In this

command, *X* is the logical drive that will ultimately host the Active Directory database when the member computer is promoted. The final location for the Active Directory database is selected when you run the Active Directory Installation Wizard. This folder must be different from the folder that contains the restored system state.

Now Last stage is Promoting an additional domain controller

1. Verify that the domain controller that is to be promoted has DNS name resolution and network connectivity to existing domain controllers in the domain controller's target domain.
2. Click **Start**, click **Run**, type `dcpromo /adv`, and then click **OK**.
3. Click **Next** to bypass the **Welcome to the Active Directory Installation Wizard** and **Operating System Compatibility** dialog boxes.
4. On the **Domain Controller Type** page, click **Additional domain controller for an existing domain**, and then click **next**.
5. On the **Copying Domain Information** page, click **from these restored backup files**: and then type the logical drive and the path of the alternative location where the system state backup was restored. Click **Next**.
6. In **Network Credentials**, type the user name, the password, and the domain name of an account that is a member of the domain administrators group for the domain that you are promoting in.
7. Continue with the remainder of the Active Directory Installation Wizard pages as you would with the standard promotion of an additional domain controller.
8. After the SYSVOL tree has replicated in, and the SYSVOL share exists, delete any remaining restored system files and folders.

21) How can you forcibly remove AD from a server, and what do you do later? • Can I get user passwords from the AD database?

Demote the server using `dcpromo /forceremoval`, and then remove the metadata from Active directory using `Ntdsutil`. There is no way to get user passwords from AD that I am aware of, but you should still be able to change them.

Another way out too

Restart the DC in DSRM mode

a. Locate the following registry subkey:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions`

b. In the right-pane, double-click **ProductType**.

c. Type **ServerNT** in the **Value data** box, and then click **OK**.

Restart the server in normal mode

it's a member server now but AD entries are still there. Promote the server to a fake domain say ABC.com and then remove gracefully using Dcpromo. Else after restart you can also use Ntdsutil to do metadata as told in the earlier post

22) Name some OU design considerations

OU design requires balancing requirements for delegating administrative rights – independent of Group Policy needs – and the need to scope the application of Group Policy. The following OU design recommendations address delegation and scope issues:

Applying Group Policy An OU is the lowest-level Active Directory container to which you can assign Group Policy settings.

Delegating administrative authority

Usually don't go more than 3 OU levels

23) What is tombstone lifetime attribute?

The number of days before a deleted object is removed from the directory services. This assists in removing objects from replicated servers and preventing restores from reintroducing a deleted object. This value is in the Directory Service object in the configuration NIC

By default 2000 (60 days)

2003 (180 days)

24) How would you find all users that have not logged on since last month?

Using only native commands, **JSILLD.bat** produces a sorted/formated report of Users who have not logged on since YYYYMMDD.

The report is sorted by UserName and list the user's full name and last logon date.

The syntax for using **JSILLD.bat** is:

JSILLD \Folder\OutputFile.Ext YYYYMMDD [/N]

where:

YYYYMMDD will report all users who have not logged on since this date.

/N is an optional parameter that will bypass users who have never logged on.

JSILLD.bat contains:

```
@echo off
setlocal
if {%2}=={} goto syntax
if "%3"==" " goto begin
if /i "%3"==" /n" goto begin
:syntax
@echo Syntax: JSILLD File yyyyymmdd [/N]
endlocal
goto :EOF
:begin
if /i "%2"==" /n" goto syntax
set dte=%2
set XX=%dte:~0,4%
if "%XX%" LSS "1993" goto syntax
set XX=%dte:~4,2%
if "%XX%" LSS "01" goto syntax
if "%XX%" GTR "12" goto syntax
set XX=%dte:~6,2%
if "%XX%" LSS "01" goto syntax
if "%XX%" GTR "31" goto syntax
set never=X
if /i "%3"==" /n" set never=/n
set file=%1
if exist %file% del /q %file%
for /f "Skip=4 Tokens=*" %%i in (`net user /domain^|findstr /v /c:"—" ^|findstr /v /i /c:"The command
completed"`) do (
```

```

do call :parse "%%i"
)
endlocal
goto :EOF
:parse
set str=%1#
set str=%str:="#"=%
set str=%str:"#=%
set substr=%str:~0,25%#
set substr=%substr: =%
set substr=%substr: #=%
set substr=%substr: #=%
if "%substr%"==" goto :EOF
for /f "Skip=1 Tokens=*" %%i in ('net user "%substr%" /domain') do call :parse1 "%%i"
set substr=%str:~25,25%#
set substr=%substr: =%
set substr=%substr: #=%
set substr=%substr: #=%
if "%substr%"==" goto :EOF
for /f "Skip=1 Tokens=*" %%i in ('net user "%substr%" /domain') do call :parse1 "%%i"
set substr=%str:~50,25%#
set substr=%substr: =%
set substr=%substr: #=%
set substr=%substr: #=%
if "%substr%"==" goto :EOF
for /f "Skip=1 Tokens=*" %%i in ('net user "%substr%" /domain') do call :parse1 "%%i"
goto :EOF
:parse1
set ustr=%1
if %ustr%=="The command completed successfully." goto :EOF
set ustr=%ustr:=%
if /i "%ustr:~0,9%"=="Full Name" set fullname=%ustr:~29,99%
if /i not "%ustr:~0,10%"=="Last logon" goto :EOF

```



```

set txt=%ustr:~29,99%
for /f "Tokens=1,2,3 Delims=/ " %i in ('@echo %txt%') do set MM=%i&set DD=%j&set YY=%k
if /i "%MM%"=="Never" goto tstnvr
goto year
:tstnvr
if /i "%never%"==" /n" goto :EOF
goto report
:year
if "%YY%" GTR "1000" goto mmm
if "%YY%" GTR "92" goto Y19
set /a YY=100%YY%%100
set YY=%YY% + 2000
goto mmm
:Y19
set YY=19%YY%
:mmm
set /a XX=100%MM%%100
if %XX% LSS 10 set MM=0%XX%
set /a XX=100%DD%%100
if %XX% LSS 10 set DD=0%XX%
set YMD=%YY%%MM%%DD%
if "%YMD%" GEQ "%dte%" goto :EOF
:report
set fullname=%fullname% #
set fullname=%fullname:~0,35%
set substr=%substr% #
set substr=%substr:~0,30%
@echo %substr% %fullname% %txt% >> %file%

```

25) What are the DS commands?

New **DS** (Directory Service) Family of built-in **command** line utilities for Windows Server 2003 Active Directory

A:

New DS built-in tools for Windows Server 2003

The DS (Directory Service) group of commands are split into two families. In one branch are DSadd, DSmod, DSrm and DSMove and in the other branch are DSQuery and DSGet.

When it comes to choosing a scripting tool for Active Directory objects, you really are spoilt for choice. The DS family of built-in command line executables offers alternative strategies to CSVDE, LDIFDE and VBScript.

Let me introduce you to the members of the DS family:

DSadd – add Active Directory users and groups

DSmod – modify Active Directory objects

DSrm – to delete Active Directory objects

DSmove – to relocate objects

DSQuery – to find objects that match your query attributes

DSget – list the properties of an object

DS Syntax

These DS tools have their own command structure which you can split into five parts:

1 2 3 4 5

Tool object "DN" (as in LDAP distinguished name) -switch value For example:

DSadd user "cn=billy, ou=managers, dc=cp, dc=com" -pwd cX49pQba

This will add a user called Billy to the Managers OU and set the password to cx49Qba

Here are some of the common DS switches which work with DSadd and DSmod

-pwd (password) -upn (userPrincipalName) -fn (FirstName) -samid (Sam account name).

The best way to learn about this DS family is to logon at a domain controller and experiment from the command line. I have prepared examples of the two most common programs. Try some sample commands for DSadd.°

Two most useful Tools: DSQuery and DSGet

The DSQuery and DSGet remind me of UNIX commands in that they operate at the command line, use

powerful verbs, and produce plenty of action. One pre-requisite for getting the most from this DS family is a working knowledge of LDAP.

If you need to query users or computers from a range of OU's and then return information, for example, office, department manager. Then DSQuery and DSGet would be your tools of choice. Moreover, you can export the information into a text file

26) What is the difference between ldifde and csvde usage considerations?

Ldifde

Ldifde creates, modifies, and deletes directory objects on computers running Windows Server 2003 operating systems or Windows XP Professional. You can also use Ldifde to extend the schema, export Active Directory user and group information to other applications or services, and populate Active Directory with data from other directory services.

The LDAP Data Interchange Format (LDIF) is a draft Internet standard for a file format that may be used for performing batch operations against directories that conform to the LDAP standards. LDIF can be used to export and import data, allowing batch operations such as add, create, and modify to be performed against the Active Directory. A utility program called LDIFDE is included in Windows 2000 to support batch operations based on the LDIF file format standard. This article is designed to help you better understand how the LDIFDE utility can be used to migrate directories.

<http://support.microsoft.com/kb/237677>

Csvde

Imports and exports data from Active Directory Domain Services (AD DS) using files that store data in the comma-separated value (CSV) format. You can also support batch operations based on the CSV file format standard.

Csvde is a command-line tool that is built into Windows Server 2008 in the/system32 folder. It is available if you have the AD DS or Active Directory Lightweight Directory Services (AD LDS) server role installed. To use **csvde**, you must run the **csvde** command from an elevated command prompt. To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

<http://technet.microsoft.com/en-us/library/cc732101.aspx>

DIFFERENCE USAGE WISE

Csvde.exe is a Microsoft Windows 2000 command-line utility that is located in the SystemRoot\System32 folder after you install Windows 2000. Csvde.exe is similar to Ldifde.exe, but it extracts information in a comma-separated value (CSV) format. You can use Csvde to import and export Active Directory data that uses the comma-separated value format. Use a spreadsheet program such as Microsoft Excel to open this .csv file and view the header and value information. See Microsoft Excel Help for information about functions such as **Concatenate** that can simplify the process of building a .csv file.

Note Although Csvde is similar to Ldifde, Csvde has a significant limitation: it can only import and export Active Directory data by using a comma-separated format (.csv). Microsoft recommends that you use the Ldifde utility for Modify or Delete operations. Additionally, the distinguished name (also known as DN) of the item that you are trying to import must be in the first column of the .csv file or the import will not work.

The source .csv file can come from an Exchange Server directory export. However, because of the difference in attribute mappings between the Exchange Server directory and Active Directory, you must make some modifications to the .csv file. For example, a directory export from Exchange Server has a column that is named "obj-class" that you must rename to "objectClass." You must also rename "DisplayName" to "displayName."

<http://support.microsoft.com/kb/327620>

27) What are the FSMO roles that have them by default what happens when each one fails?

FSMO stands for the Flexible single Master Operation

It has 5 Roles: -

- **Schema Master:**

The schema master domain controller controls all updates and modifications to the schema. Once the Schema update is complete, it is replicated from the schema master to all other DCs in the directory. To update the schema of a forest, you must have access to the schema master. There can be only one schema master in the whole forest.

- **Domain naming master:**

The domain naming master domain controller controls the addition or removal of domains in the forest. This DC is the only one that can add or remove a domain from the directory. It can also add or remove cross references to domains in external directories. There can be only one domain naming master in the whole forest.

- **Infrastructure Master:**

When an object in one domain is referenced by another object in another domain, it represents the reference by the GUID, the SID (for references to security principals), and the DN of the object being referenced. The infrastructure FSMO role holder is the DC responsible for updating an object's SID and distinguished name in a cross-domain object reference. At any one time, there can be only one domain controller acting as the infrastructure master in each domain.

Note: The Infrastructure Master (IM) role should be held by a domain controller that is not a Global Catalog server (GC). If the Infrastructure Master runs on a Global Catalog server it will stop updating object information because it does not contain any references to objects that it does not hold. This is because a Global Catalog server holds a partial replica of every object in the forest. As a result, cross-domain object references in that domain will not be updated and a warning to that effect will be logged on that DC's event log. If all the domain controllers in a domain also host the global catalog, all the domain controllers have the current data, and it is not important which domain controller holds the infrastructure master role.

- **Relative ID (RID) Master:**

The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain. When a DC creates a security principal object such as a user or group, it attaches a unique Security ID (SID) to the object. This SID consists of a domain SID (the same for all SIDs created in a domain), and a relative ID (RID) that is unique for each security principal SID created in a domain. Each DC in a domain is allocated a pool of RIDs that it is allowed to assign to the security principals it creates. When a DC's allocated RID pool falls below a threshold, that DC issues a request for additional RIDs to the domain's RID master. The domain RID master responds to the request by retrieving RIDs from the domain's unallocated RID pool and assigns them to the pool of the requesting DC. At any one time, there can be only one domain controller acting as the RID master in the domain.

- **PDC Emulator:**

The PDC emulator is necessary to synchronize time in an enterprise. Windows 2000/2003 includes the W32Time (Windows Time) time service that is required by the Kerberos authentication protocol. All Windows 2000/2003-based computers within an enterprise use a common time. The purpose of the time service is to ensure that the Windows Time service uses a hierarchical relationship that controls authority and does not permit loops to ensure appropriate common time usage.

The PDC emulator of a domain is authoritative for the domain. The PDC emulator at the root of the forest becomes authoritative for the enterprise, and should be configured to gather the time from an external source. All PDC FSMO role holders follow the hierarchy of domains in the selection of their in-bound time partner.

:: In a Windows 2000/2003 domain, the PDC emulator role holder retains the following functions:

:: Password changes performed by other DCs in the domain are replicated preferentially to the PDC emulator.

Authentication failures that occur at a given DC in a domain because of an incorrect password are forwarded to the PDC emulator before a bad password failure message is reported to the user.

Account lockout is processed on the PDC emulator.

Editing or creation of Group Policy Objects (GPO) is always done from the GPO copy found in the PDC Emulator's SYSVOL share, unless configured not to do so by the administrator.

The PDC emulator performs all of the functionality that a Microsoft Windows NT 4.0 Server-based PDC or earlier PDC performs for Windows NT 4.0-based or earlier clients.

This part of the PDC emulator role becomes unnecessary when all workstations, member servers, and domain controllers that are running Windows NT 4.0 or earlier are all upgraded to Windows 2000/2003. The PDC emulator still performs the other functions as described in a Windows 2000/2003 environment.

28) What FSMO placement considerations do you know of?

Windows 2000/2003 Active Directory domains utilize a Single Operation Master method called FSMO (Flexible Single Master Operation), as described in Understanding FSMO Roles in Active Directory.

In most cases an administrator can keep the FSMO role holders (all 5 of them) in the same spot (or actually, on the same DC) as has been configured by the Active Directory installation process. However,

there are scenarios where an administrator would want to move one or more of the FSMO roles from the default holder DC to a different DC.

Windows Server 2003 Active Directory is a bit different than the Windows 2000 version when dealing with FSMO placement. In this article I will only deal with Windows Server 2003 Active Directory, but you should bear in mind that most considerations are also true when planning Windows 2000 AD FSMO roles

29) I want to look at the RID allocation table for a DC. What do I do?

1.install support tools from OS disk(OS Inst: Disk=>support=>tools=>suptools.msi)

2.In Command prompt type dcdiag /test:ridmanager /s:system1 /v (system1 is the name of our DC)

30) What's the difference between transferring a FSMO role and seizing one? Which one should you NOT seize? Why?

Seizing an FSMO can be a destructive process and should only be attempted if the existing server with the FSMO is no longer available.

If the domain controller that is the Schema Master FSMO role holder is temporarily unavailable, **DO NOT seize the Schema Master role.**

If you are going to seize the Schema Master, you must permanently disconnect the current Schema Master from the network.

If you seize the Schema Master role, the boot drive on the original Schema Master must be completely reformatted and the operating system must be cleanly installed, if you intend to return this computer to the network.

NOTE: The Boot Partition contains the system files (\System32). The System Partition is the partition that contains the startup files, NTDetect.com, NTLDR, Boot.ini, and possibly Ntbootdd.sys.

The Active Directory Installation Wizard (Dcpromo.exe) assigns all 5 FSMO roles to the first domain controller in the forest root domain. The first domain controller in each new child or tree domain is assigned the three domain-wide roles.

31) How do you configure a "stand-by operation master" for any of the roles?

1. Open **Active Directory Sites and Services**.
2. Expand the site name in which the standby operations master is located to display the **Servers** folder.

3. Expand the **Servers** folder to see a list of the servers in that site.
4. Expand the name of the server that you want to be the standby operations master to display its NTDS Settings.
5. Right-click **NTDS Settings**, click **New**, and then click **Connection**.
6. In the **Find Domain Controllers** dialog box, select the name of the current role holder, and then click **OK**.
7. In the **New Object-Connection** dialog box, enter an appropriate name for the Connection object or accept the default name, and click **OK**.

32) How do you backup & restore AD.

Backing up Active Directory is essential to maintain an Active Directory database. You can back up Active Directory by using the Graphical User Interface (GUI) and command-line tools that the Windows Server 2003 family provides.

You frequently backup the system state data on domain controllers so that you can restore the most current data. By establishing a regular backup schedule, you have a better chance of recovering data when necessary.

To ensure a good backup includes at least the system state data and contents of the system disk, you must be aware of the tombstone lifetime. By default, the tombstone is 60 days. Any backup older than 60 days is not a good backup. Plan to backup at least two domain controllers in each domain, one of at least one backup to enable an authoritative restore of the data when necessary.

SystemStateData

Several features in the windows server 2003 family make it easy to backup Active Directory. You can backup Active Directory while the server is online and other network function can continue to function.

System state data on a domain controller includes the following components:

Active Directory system state data does not contain Active Directory unless the server, on which you are backing up the system state data, is a domain controller. Active Directory is present only on domain controllers.

The SYSVOL shared folder: This shared folder contains Group policy templates and logon scripts. The SYSVOL shared folder is present only on domain controllers.

The Registry: This database repository contains information about the computer's configuration.

System startup files: Windows Server 2003 requires these files during its initial startup phase. They

include the boot and system files that are under windows file protection and used by windows to load, configure, and run the operating system.

The COM+ Class Registration database: The Class registration is a database of information about Component Services applications.

The Certificate Services database: This database contains certificates that a server running Windows server 2003 uses to authenticate users. The Certificate Services database is present only if the server is operating as a certificate server.

System state data contains most elements of a system's configuration, but it may not include all of the information that you require recovering data from a system failure. Therefore, be sure to backup all boot and system volumes, including theSystemState, when you back up your server.

Restoring Active Directory

In Windows Server 2003 family, you can restore the Active Directory database if it becomes corrupted or is destroyed because of hardware or software failures. You must restore the Active Directory database when objects in Active Directory are changed or deleted.

Active Directory restore can be performed in several ways. Replication synchronizes the latest changes from every other replication partner. Once the replication is finished each partner has an updated version of Active Directory. There is another way to get these latest updates by Backup utility to restore replicated data from a backup copy. For this restore you don't need to configure again your domain controller or no need to install the operating system from scratch.

Active Directory Restore Methods

You can use one of the three methods to restore Active Directory from backup media: primary restore, normal (non authoritative) restore, and authoritative restore.

Primary restore: This method rebuilds the first domain controller in a domain when there is no other way to rebuild the domain. Perform a primary restore only when all the domain controllers in the domain are lost, and you want to rebuild the domain from the backup.

Members of Administrators group can perform the primary restore on local computer, or user should have been delegated with this responsibility to perform restore. On a domain controller only Domain Admins can perform this restore.

Normal restore: This method reinstates the Active Directory data to the state before the backup, and then updates the data through the normal replication process. Perform a normal restore for a single domain controller to a previously known good state.

Authoritative restore: You perform this method in tandem with a normal restore. An authoritative restore marks specific data as current and prevents the replication from overwriting that data. The authoritative data is then replicated through the domain.

Perform an authoritative restore individual object in a domain that has multiple domain controllers. When you perform an authoritative restore, you lose all changes to the restore object that occurred after the backup. Ntdsutil is a command line utility to perform an authoritative restore along with windows server 2003 system utilities. The Ntdsutil command-line tool is an executable file that you use to mark Active Directory objects as authoritative so that they receive a higher version recently changed data on other domain controllers does not overwrite system state data during replication.

33) Why can't you restore a DC that was backed up 4 months ago?

Because of the tombstone life which is set to only 60 days

34) What are GPOs?

Group Policy Objects

35) What is the order in which GPOs are applied?

Local, Site, Domain, OU

Group Policy settings are processed in the following order:

1:- Local Group Policy object-each computer has exactly one Group Policy object that is stored locally. This processes for both computer and user Group Policy processing.

2:- Site-Any GPOs that have been linked to the site that the computer belongs to are processed next. Processing is in the order that is specified by the administrator, on the Linked Group Policy Objects tab for the site in Group Policy Management Console (GPMC). The GPO with the lowest link order is processed last, and therefore has the highest precedence.

3:- Domain-processing of multiple domain-linked GPOs is in the order specified by the administrator, on the Linked Group Policy Objects tab for the domain in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.

4:- Organizational units-GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

At the level of each organizational unit in the Active Directory hierarchy, one, many, or no GPOs can be linked. If several GPOs are linked to an organizational unit, their processing is in the order that is specified by the administrator, on the Linked Group Policy Objects tab for the organizational unit in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.

This order means that the local GPO is processed first, and GPOs that are linked to the organizational unit of which the computer or user is a direct member are processed last, which overwrites settings in the earlier GPOs if there are conflicts. (If there are no conflicts, then the earlier and later settings are merely aggregated.)

36) Name a few benefits of using GPMC.

- Easy administration of all GPOs across the entire Active Directory Forest
- View of all GPOs in one single list
- Reporting of GPO settings, security, filters, delegation, etc.
- Control of GPO inheritance with Block Inheritance, Enforce, and Security Filtering
- Delegation model
- Backup and restore of GPOs
- Migration of GPOs across different domains and forests

With all of these benefits, there are still negatives in using the GPMC alone. Granted, the GPMC is needed and should be used by everyone for what it is ideal for. However, it does fall a bit short when you want to protect the GPOs from the following:

- Role based delegation of GPO management
- Being edited in production, potentially causing damage to desktops and servers
- Forgetting to back up a GPO after it has been modified
- Change management of each modification to every GPO

37) What are the GPC and the GPT? Where can I find them?

A GPO is a collection of Group Policy settings, stored at the domain level as a virtual object consisting of a Group Policy container (GPC) and a Group Policy template (GPT).

The GPC, which contains information on the properties of a GPO, is stored in Active Directory on each domain controller in the domain. The GPT contains the data in a GPO and is stored in the Sysvol in the /Policies sub-directory.

38) What are GPO links? What special things can I do to them?

Linking GPOs

To apply the settings of a GPO to the users and computers of a domain, site, or OU, you need to add a link to that GPO. You can add one or more GPO links to each domain, site, or OU by using GPMC. Keep in mind that creating and linking GPOs is a sensitive privilege that should be delegated only to administrators who are trusted and understand Group Policy.

Linking GPOs to the Site

If you have a number of policy settings to apply to computers in a particular physical location only – certain network or proxy configuration settings, for example – these settings might be appropriate for inclusion in a site-based policy. Because domains and sites are independent, it is possible that computers in the site might need to cross domains to link the GPO to the site. In this case, make sure there is good connectivity.

If, however, the settings do not clearly correspond to computers in a single site, it is better to assign the GPO to the domain or OU structure rather than to the site.

Linking GPOs to the Domain

Link GPOs to the domain if you want them to apply to all users and computers in the domain. For example, security administrators often implement domain-based GPOs to enforce corporate standards. They might want to create these GPOs with the GPMC **Enforce** option enabled to guarantee that no other administrator can override these settings.

Important

- If you need to modify some of the settings contained in the **Default Domain Policy GPO**, it is recommended that you create a new GPO for this purpose, link it to the domain, and set the **Enforce** option. In general, do not modify this or the **Default Domain Controller Policy GPO**. If you do, be sure to back up these and any other GPOs in your network by using GPMC to ensure you can restore them.

As the name suggests, the **Default Domain Policy GPO** is also linked to the domain. The **Default Domain Policy GPO** is created when the first domain controller in the domain is installed and the administrator logs on for the first time. This GPO contains the domain-wide account policy settings, Password Policy, Account Lockout Policy, and Kerberos Policy, which is enforced by the domain controller computers in the domain. All domain controllers retrieve the values of these account policy settings from the **Default Domain Policy GPO**. In order to apply account policies to domain accounts, these policy settings must be deployed in a GPO linked to the domain, and it is recommended that you set these settings in the Default Domain Policy. If you set account policies at a lower level, such as an OU, the settings only affect local accounts (non-domain accounts) on computers in that OU and its children.

Before making any changes to the default GPOs, be sure to back up the GPO using GPMC. If for some reason there is a problem with the changes to the default GPOs and you cannot revert back to the previous or initial states, you can use the Dcgpofix.exe tool to recreate the default policies in their initial state.

Dcgpofix.exe is a command-line tool that completely restores the Default Domain Policy GPO and Default Domain Controller GPO to their original states in the event of a disaster where you cannot use GPMC. Dcgpofix.exe restores only the policy settings that are contained in the default GPOs at the time they are generated. The only Group Policy extensions that include policy settings in the default GPOs are RIS, Security, and EFS. Dcgpofix.exe does not restore other GPOs that administrators create; it is only intended for disaster recovery of the default GPOs.

Note that Dcgpofix.exe does not save any information created through applications, such as SMS or Exchange. The Dcgpofix.exe tool is included with Windows Server 2003 and only works in a Windows Server 2003 domain.

Dcgpofix.exe is located in the C:\Windows\Repair folder. The syntax for Dcgpofix.exe is as follows:

Copy Code

DCGPOFix [/Target: Domain | DC | BOTH]

Table 2.1 describes the options you can use with the command line parameter /Target: when using the Dcgpofix.exe tool.

Table 2.1 Dcgpofix.exe Options for Using the /Target Parameter

	DOMAIN	Specifies that the Default Domain Policy should be recreated.
	DC	Specifies that the Default Domain Controllers Policy should be recreated.
	BOTH	Specifies that both the Default Domain Policy and the Default Domain Controllers Policy should be recreated.
/Target option:	Description of option	For more information about Dcgpofix.exe, in Help and Support Center for Windows Server 2003 click Tools , and then click Command-line reference A-Z

Linking GPOs to the OU Structure

Most GPOs are normally linked to the OU structure because this provides the most flexibility and manageability:

- You can move users and computers into and out of OUs.
- OUs can be rearranged if necessary.
- You can work with smaller groups of users who have common administrative requirements.
- You can organize users and computers based on which administrators manage them.

Organizing GPOs into user- and computer-oriented GPOs can help make your Group Policy environment easier to understand and can simplify troubleshooting. However, separating the user and computer components into separate GPOs might require more GPOs. You can compensate for this by adjusting the **GPO Status** to disable the user or computer configuration portions of the GPO that do not apply and to reduce the time required to apply a given GPO.

Changing the GPO Link Order

Within each domain, site, and OU, the link order controls the order in which GPOs are applied. To change the precedence of a link, you can change the link order, moving each link up or down in the list to the

appropriate location. Links with the lowest number have higher precedence for a given site, domain, or OU. For example, if you add six GPO links and later decide that you want the last one that you added to have the highest precedence, you can adjust the link order of the GPO link so it has link order of 1. To change the link order for GPO links for a domain, OU, or site, use GPMC

<http://technet.microsoft.com/en-us/library/cc736813.aspx>

<http://technet.microsoft.com/en-us/library/cc757050.aspx>

39) What can I do to prevent inheritance from above?

You can block policy inheritance for a domain or organizational unit. Using block inheritance prevents GPOs linked to higher sites, domains, or organizational units from being automatically inherited by the child-level. By default, children inherit all GPOs from the parent, but it is sometimes useful to block inheritance. For example, if you want to apply a single set of policies to an entire domain except for one organizational unit, you can link the required GPOs at the domain level (from which all organizational units inherit policies by default), and then block inheritance only on the organizational unit to which the policies should not be applied.

40) How can I override blocking of inheritance?

A. Group Policies can be applied at multiple levels (Sites, domains, organizational Units) and multiple GP's for each level. Obviously it may be that some policy settings conflict hence the application order of Site – Domain – Organization Unit and within each layer you set order for all defined policies but you may want to force some policies to never be overridden (No Override) and you may want some containers to not inherit settings from a parent container (Block Inheritance).

A good definition of each is as follows:

No Override – This prevents child containers from overriding policies set at higher levels

Block Inheritance – Stops containers inheriting policies from parent containers

No Override takes precedence over Block Inheritance so if a child container has Block Inheritance set but on the parent a group policy has No Override set then it will get applied.

Also the highest No Override takes precedence over lower No Override's set.

To block inheritance perform the following:

1. Start the Active Directory Users and Computer snap-in (Start – Programs – Administrative Tools – Active Directory Users and Computers)
2. Right click on the container you wish to stop inheriting settings from its parent and select Properties
3. Select the 'Group Policy' tab
4. Check the 'Block Policy inheritance' option
[Click here to view image](#)
5. Click Apply then OK

To set a policy to never be overridden performs the following:

1. Start the Active Directory Users and Computer snap-in (Start – Programs – Administrative Tools – Active Directory Users and Computers)
2. Right click on the container you wish to set a Group Policy to not be overridden and select Properties
3. Select the 'Group Policy' tab
4. Click Options
5. Check the 'No Override' option
6. Click OK
7. Click Apply then OK

41) How can you determine what GPO was and was not applied for a user? Name a few ways to do that.

1. **Group Policy Management Console (GPMC)** can provide assistance when you need to troubleshoot GPO behavior. It allows you to examine the settings of a specific GPO, and is can also be used to determine how your GPOs are linked to sites, domains, and OUs. The **Group Policy Results report** collects information on a computer and user, to list the policy settings which are enabled. To create a Group Policy Results report, right-click Group Policy Results, and select Group Policy Results Wizard on the shortcut menu. This launches the Group Policy Results Wizard, which guides you through various pages to set parameters for the information that should be displayed in the Group Policy Results report.
2. **Gpresult.exe** Click **Start > RUN > CMD > gpresult**, this will also give you information of applied group policies.

1. 3. RSOP.MSC

42) A user claims he did not receive a GPO, yet his user and computer accounts are in the right OU, and everyone else there gets the GPO. What will you look for?

Here interviewer want to know the troubleshooting steps

what GPOs is applying?

If it applying in all user and computer?

What GPOs are implemented on ou?

Make sure user not is member of loopback policy as in loopback policy it doesn't affect user settings only computer policy will applicable.

If he is member of GPOs filter grp or not?

You may also want to check the computers event logs. If you find event ID 1085 then you may want to download the patch to fix this and reboot the computer.

=====

Answer 2: Start troubleshooting by running RSOP.MSC (Resultant Set of Policy) or gpresult /z to verify whether relevant GPO actually applies to that user?

This also can be a reason of slow network; you can change the default setting by using the Group Policy MMC snap-in. This feature is enabled by default, but you can disable it by using the following policy: Administrative Templates\System\Logon**Always wait for the network at computer startup and logon.**

Identify which GPOs they correspond to; verify that they are applicable to the computer/user (based on the output of RSOP.MSC/gpresult)

43) What are administrative templates?

The GPO settings are divided between the Computer settings and the User settings. In both parts of the GPO you can clearly see a large section called Administrative Templates.

Administrative Templates are a large repository of registry-based changes (in fact, over 1300 individual settings) that can be found in any GPO on Windows 2000, Windows XP, and Windows Server 2003.

By using the Administrative Template sections of the GPO you can deploy modifications to machine (called HKEY_LOCAL_MACHINE in the registry) and user (called HKEY_CURRENT_USER in the registry) portions of the Registry of computers that are influenced by the GPO.

The Administrative Templates are Unicode-formatted text files with the extension .ADM and are used to create the Administrative Templates portion of the user interface for the GPO Editor.

44) What's the difference between software publishing and assigning?

An administrator can either assign or publish software applications.

Assign Users

the software application is advertised when the user logs on. It is installed when the user clicks on the software application icon via the start menu, or accesses a file that has been associated with the software application.

Assign Computers

The software application is advertised and installed when it is safe to do so, such as when the computer is next restarted.

Publish to users

the software application does not appear on the start menu or desktop. This means the user may not know that the software is available. The software application is made available via the Add/Remove Programs option in control panel, or by clicking on a file that has been associated with the application. Published applications do not reinstall themselves in the event of accidental deletion, and it is not possible to publish to computers.

45) You want to standardize the desktop environments (wallpaper, My Documents, Start menu, printers etc.) on the computers in one department. How would you do that?

Yes... Through Group Policy

Windows Server 2008 Questions and Answers:



1 :: What are some of the new tools and features provided by Windows Server 2008?

Windows Server 2008 now provides a desktop environment similar to Microsoft Windows Vista and includes tools also found in Vista, such as the new backup snap-in and the BitLocker drive encryption feature. Windows Server 2008 also provides the new IIS7 web server and the Windows Deployment Service.

2 :: What are the different editions of Windows Server 2008?

The entry-level version of Windows Server 2008 is the Standard Edition. The Enterprise Edition provides a platform for large enterprisewide networks. The Datacenter Edition provides support for unlimited Hyper-V virtualization and advanced clustering services. The Web Edition is a scaled-down version of Windows Server 2008 intended for use as a dedicated web server. The Standard, Enterprise, and Datacenter Editions can be purchased with or without the Hyper-V virtualization technology.

3 :: What two hardware considerations should be an important part of the planning process for a Windows Server 2008 deployment?

Any server on which you will install Windows Server 2008 should have at least the minimum hardware requirement for running the network operating system. Server hardware should also be on the Windows Server 2008 Hardware Compatibility List to avoid the possibility of hardware and network operating system incompatibility.

4 :: How does the activation process differ on Windows Server 2008 as compared to Windows Server 2003?

You can select to have activation happen automatically when the Windows Server 2008 installation is complete. Make sure that the Automatically Activate Windows When I'm Online check box is selected on the Product Key page.

5 :: What are the options for installing Windows Server 2008?

You can install Windows Server 2008 on a server not currently configured with NOS, or you can upgrade existing servers running Windows 2000 Server and Windows Server 2003.

Windows Server 2008 Questions and Answers:



6 :: How do you configure and manage a Windows Server 2008 core installation?

This stripped-down version of Windows Server 2008 is managed from the command line.

7 :: Which Control Panel tool enables you to automate the running of server utilities and other applications?

The Task Scheduler enables you to schedule the launching of tools such as Windows Backup and Disk Defragmenter.

8 :: What are some of the items that can be accessed via the System Properties dialog box?

You can access virtual memory settings and the Device Manager via the System Properties dialog box.

9 :: Which Windows Server utility provides a common interface for tools and utilities and provides access to server roles, services, and monitoring and drive utilities?

The Server Manager provides both the interface and access to a large number of the utilities and tools that you will use as you manage your Windows server.

10 :: How are local user accounts and groups created?

Local user accounts and groups are managed in the Local Users and Groups node in the Server Manager. Local user accounts and groups are used to provide local access to a server.

11 :: When a child domain is created in the domain tree, what type of trust relationship exists between the new child domain and the trees root domain?

Child domains and the root domain of a tree are assigned transitive trusts. This means that the root domain and child domain trust each other and allow resources in any domain in the tree to be accessed by users in any domain in the tree.

12 :: What is the primary function of domain controllers?

The primary function of domain controllers is to validate users to the network. However, domain controllers also provide the catalog of Active Directory objects to users on the network.

13 :: What are some of the other roles that a server running Windows Server 2008 could fill on the network?

A server running Windows Server 2008 can be configured as a domain controller, a file server, a print server, a web server, or an application server. Windows servers can also have roles and features that provide services such as DNS, DHCP, and Routing and Remote Access.

14 :: Which Windows Server 2008 tools make it easy to manage and configure a servers roles and features?

The Server Manager window enables you to view the roles and features installed on a server and also to quickly access the tools used to manage these various roles and features. The Server Manager can be used to add and remove roles and features as needed.

15 :: What Windows Server 2008 service is used to install client operating systems over the network?

Windows Deployment Services (WDS) enables you to install client and server operating systems over the network to any computer with a PXE-enabled network interface.

16 :: What domain services are necessary for you to deploy the Windows Deployment Services on your network?

Windows Deployment Services requires that a DHCP server and a DNS server be installed in the domain.

17 :: How is WDS configured and managed on a server running Windows Server 2008?

The Windows Deployment Services snap-in enables you to configure the WDS server and add boot and install images to the server.

18 :: What utility is provided by Windows Server 2008 for managing disk drives, partitions, and volumes?

The Disk Manager provides all the tools for formatting, creating, and managing drive volumes and partitions.

19 :: What is the difference between a basic and dynamic drive in the Windows Server 2008 environment?

A basic disk embraces the MS-DOS disk structure; a basic disk can be divided into partitions (simple volumes).

Dynamic disks consist of a single partition that can be divided into any number of volumes. Dynamic disks also support Windows Server 2008 RAID implementations.

20 :: What is RAID in Windows Server 2008?

RAID, or Redundant Array of Independent Disks, is a strategy for building fault tolerance into your file servers. RAID enables you to combine one or more volumes on separate drives so that they are accessed by a single drive letter. Windows Server 2008 enables you to configure RAID 0 (a striped set), RAID 1 (a mirror set), and RAID 5 (disk striping with parity).

Windows Server 2008 Questions and Answers:



21 :: What is the most foolproof strategy for protecting data on the network?

Regular backups of network data provides the best method of protecting you from data loss.

22 :: What conceptual model helps provide an understanding of how network protocol stacks such as TCP/IP work?

The OSI model, consisting of the application, presentation, session, transport, network, data link, and physical layers, helps describe how data is sent and received on the network by protocol stacks.

23 :: What protocol stack is installed by default when you install Windows Server 2008 on a network server?

TCP/IP (v4 and v6) is the default protocol for Windows Server 2008. It is required for Active Directory implementations and provides for connectivity on heterogeneous networks.

24 :: When TCP/IP is configured on a Windows server (or domain client), what information is required?

You must provide at least the IP address and the subnet mask to configure a TCP/IP client for an IPv4 client, unless that client obtains this information from a DHCP server. For IPv6 clients, the interface ID is generated automatically from the MAC hardware address on the network adapter. IPv6 can also use DHCP as a method to configure IP clients on the network.

25 :: What are two command-line utilities that can be used to check TCP/IP configurations and IP connectivity, respectively?

The ipconfig command can be used to check a computer's IP configuration and also renew the client's IP address if it is provided by a DHCP server. ping can be used to check the connection between the local computer and any computer on the network, using the destination computer's IP address.

Windows Server 2008 Questions and Answers:



26 :: What term is used to refer to the first domain created in a new Active Directory tree?

The first domain created in a tree is referred to as the root domain. Child domains created in the tree share the same namespace as the root domain.

27 :: How is a server running Windows Server 2008 configured as a domain controller, such as the domain controller for the root domain or a child domain?

Installing the Active Directory on a server running Windows Server 2008 provides you with the option of creating a root domain for a domain tree or of creating child domains in an existing tree. Installing Active Directory on the server makes the server a domain controller.

28 :: What are some of the tools used to manage Active Directory objects in a Windows Server 2008 domain?

When the Active Directory is installed on a server (making it a domain controller), a set of Active Directory snap-ins is provided. The Active Directory Users and Computers snap-in is used to manage Active Directory objects such as user accounts, computers, and groups. The Active Directory Domains and Trusts snap-in enables you to manage the trusts that are defined between domains. The Active Directory Sites and Services snap-in provides for the management of domain sites and subnets.

29 :: How are domain user accounts created and managed?

The Active Directory Users and Computers snap-in provides the tools necessary for creating user accounts and managing account properties. Properties for user accounts include settings related to logon hours, the computers to which a user can log on, and the settings related to the user's password.

30 :: What type of Active Directory objects can be contained in a group?

A group can contain users, computers, contacts, and other nested groups.

Windows Server 2008 Questions and Answers:



31 :: What type of group is not available in a domain that is running at the mixed-mode functional level?

Universal groups are not available in a mixed-mode domain. The functional level must be raised to Windows 2003 or Windows 2008 to make these groups available.

32 :: What types of Active Directory objects can be contained in an Organizational Unit?

Organizational Units can hold users, groups, computers, contacts, and other OUs. The Organizational Unit provides you with a container directly below the domain level that enables you to refine the logical hierarchy of how your users and other resources are arranged in the Active Directory.

33 :: What are Active Directory sites in Windows Server 2008?

Active Directory sites are physical locations on the network's physical topology. Each regional domain that you create is assigned to a site. Sites typically represent one or more IP subnets that are connected by IP routers. Because sites are separated from each other by a router, the domain controllers on each site periodically replicate the Active Directory to update the Global Catalog on each site segment.

34 :: How can client computer accounts be added to the Active Directory?

Client computer accounts can be added through the Active Directory Users and Computers snap-in. You can also create client computer accounts via the client computer by joining it to the domain via the System Properties dialog box. This requires a user account that has administrative privileges, such as members of the Domain Administrator or Enterprise Administrator groups.

35 :: What firewall setting is required to manage client computers such as Vista clients and Windows 2008 member servers?

The Windows Firewall must allow remote administration for a computer to be managed remotely.

36 :: Can servers running Windows Server 2008 provide services to clients when they are not part of a domain?

Servers running Windows Server 2008 can be configured to participate in a workgroup. The server can provide some services to the workgroup peers but does not provide the security and management tools provided to domain controllers.

37 :: What does the use of Group Policy provide you as a network administrator?

Group Policy provides a method of controlling user and computer configuration settings for Active Directory containers such as sites, domains, and OUs. GPOs are linked to a particular container, and then individual policies and administrative templates are enabled to control the environment for the users or computers within that particular container.

38 :: What tools are involved in managing and deploying Group Policy?

GPOs and their settings, links, and other information such as permissions can be viewed in the Group Policy Management snap-in.

39 :: How do you deal with Group Policy inheritance issues?

GPOs are inherited down through the Active Directory tree by default. You can block the inheritance of settings from upline GPOs (for a particular container such as an OU or a local computer) by selecting Block Inheritance for that particular object. If you want to enforce a higher-level GPO so that it overrides directly linked GPOs, you can use the Enforce command on the inherited (or upline) GPO.

40 :: How can you make sure that network clients have the most recent Windows updates installed and have other important security features such as the Windows Firewall enabled before they can gain full network access?

You can configure a Network Policy Server (a service available in the Network Policy and Access Services role). The Network Policy Server can be configured to compare desktop client settings with health validators to determine the level of network access afforded to the client.

41 :: What is the purpose of deploying local DNS servers?

A domain DNS server provides for the local mapping of fully qualified domain names to IP addresses. Because the DNS is a distributed database, the local DNS servers can provide record information to remote DNS servers to help resolve remote requests related to fully qualified domain names on your network.

42 :: What types of zones would you want to create on your DNS server so that both queries to resolve hostnames to IP addresses and queries to resolve IP addresses to hostnames are handled successfully?

You would create both a forward lookup zone and a reverse lookup zone on your Windows Server 2008 DNS server.

43 :: What tool enables you to manage your Windows Server 2008 DNS server?

The DNS snap-in enables you to add or remove zones and to view the records in your DNS zones. You can also use the snap-in to create records such as a DNS resource record.

44 :: In terms of DNS, what is a caching-only server?

A caching-only DNS server supplies information related to queries based on the data it contains in its DNS cache. Caching-only servers are often used as DNS forwarders. Because they are not configured with any zones, they do not generate network traffic related to zone transfers.

45 :: How is the range of IP addresses defined for a Windows Server 2008 DHCP server?

The IP addresses supplied by the DHCP server are held in a scope. A scope that contains more than one subnet of IP addresses is called a superscope. IP addresses in a scope that you do not want to lease can be included in an exclusion range.

46 :: What TCP/IP configuration parameters can be provided to a DHCP client?

The DHCP server can supply a DHCP client an IP address and subnet mask. It also can optionally include the default gateway address, the DNS server address, and the WINS server address to the client.

47 :: How can you configure the DHCP server so that it provides certain devices with the same IP address each time the address is renewed?

You can create a reservation for the device (or create reservations for a number of devices). To create a reservation, you need to know the MAC hardware address of the device. You can use the ipconfig or nbstat command-line utilities to determine the MAC address for a network device such as a computer or printer.

48 :: To negate rogue DHCP servers from running with a domain, what is required for your DHCP server to function?

The DHCP server must be authorized in the Active Directory before it can function in the domain.