## Skills required for Microsoft Server Administrator

Microsoft has specified more than twenty-five objectives for the 70-297 test, which are grouped under four topics. Following are the important areas in which an individual should possess good knowledge before taking the 70-297 test:

1. Analyzing business and technical requirements of an organization.
2. Analyzing the impact of Active Directory on the existing technical environment.
3. Analyzing existing and planned business models and organizational structure.
4. Analyzing the structure of IT management.
5. Evaluating the company's existing and planned technical environments.
6. Analyzing existing network operating system implementation.
7. Analyzing the impact of Active Directory on a planned environment.
8. Analyzing the business requirement for client computer desktop management.
9. Analyzing security requirements for the Active Directory directory service.
10. Designing an Active Directory and domain structure.
11. Designing an Active Directory naming strategy including planning of DNS.
12. Designing an organizational unit structure and a site structure. Designing a replication strategy.
13. Designing a user and computer authentication strategy.
14. Designing the placement of operations masters, global catalog servers, domain controllers, and DNS servers.
15. Identifying network topology and performance levels.

### What is Active Directory Migration Tool (ADMT) ?

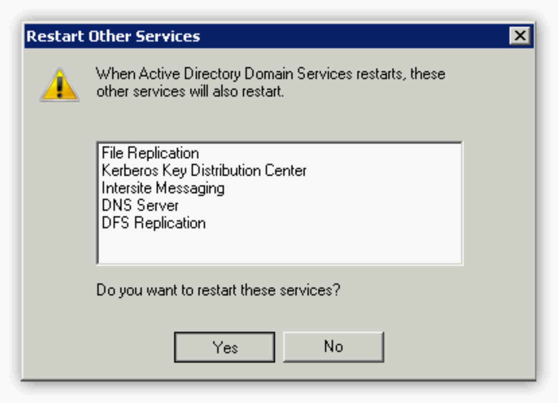
The Active Directory Migration Tool (ADMT) is used to migrate from an earlier implementation of Windows NT to Windows Server 2003 or Windows 2000 Server. ADMT supports not only migration from Windows NT 4.0 to Active Directory but also interforest and intraforest migrations. ADMT is designed to migrate an Active Directory schema from one forest to another, regardless of whether a change in operating systems is involved.

ADMT 2.0 has many new features such as a command-line interface and a better interface to work with Microsoft Exchange Server. ADMT also supports a user-account password migration.

### How to restart Active Directory Domain Services?

Take the following steps to restart Active Directory Domain Services:

Start the Services console through Start > Administrative Tools > Services.


Restart Other Services

When Active Directory Domain Services restarts, these other services will also restart.

File Replication
Kerberos Key Distribution Center
Intersite Messaging
DNS Server
DFS Replication

Do you want to restart these services?

### What is LDIFDE

LDIFDE is a command-line tool in the Windows Server 2003 operating system. It is used to create, modify, and delete objects on computers running on Windows Server 2003 and Windows XP Professional. LDIFDE is also used 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.

What is primary restore method?

The primary restore method is a type of backup restoration of the System State data. This method is used to restore Active Directory data on a stand-alone domain controller. This method of restoration is also used in a situation when a completely failed forest needs to be restored

**What is replication?**

Replication is a process through which the changes made to a replica on one domain controller are synchronized to replicas on all other domain controllers in the network. Each domain controller stores three types of replicas:

Schema partition: This partition stores definitions and attributes of objects that can be created in the forest. Changes made in this partition are replicated to all the domain controllers in all the domains in the forest.

**Configuration partition:** This partition stores the logical structure of the forest deployment. It includes the domain structure and replication topology. Changes made in this partition are replicated to all the domain controllers in all the domains in the forest.

**Domain partition**: This partition stores all the objects in a domain. Changes made in this partition are replicated to all the domain controllers within the domain.

Note: Windows supports a new type of directory partition named Application directory partition. This partition is available only to the Windows 2003 (or above) domain controllers. The applications and services use this partition to store application-specific data.

Creating, modifying, moving, or deleting an object triggers a replication between domain controllers. Replications are of two types:

**Intrasite**: In the intrasite (within a site) replication, the data is not compressed, as the replication mostly uses LAN connections. This saves the computer's CPU time of processing data. In the intrasite replication, the replication partners poll each other periodically and notify each other when changes need to be replicated, and then pull the information for processing. Active Directory uses the remote procedure call (RPC) transport protocol for intrasite replication.

**Intersite:** As intersite (between sites) replication uses WAN connections, a large amount of data is compressed to save bandwidth. For the same reason, the replication partners do not notify each other when changes need to be replicated. Instead, administrators configure the replication schedule to update the information. Active Directory uses the IP or SMTP protocol for intersite replication.

**What is NLB Manager?**

Network Load Balancing (NLB) Manager is a Windows Server 2008 GUI tool to manage NLB. NLB Manager is used to add or remove hosts from an NLB cluster, to configure a cluster, and to manage a cluster. NLB Manager can be installed by using Add Features within Server Manager

**Group Policy and Group Policy Object (GPO)**

**What are group policies?**

Group policies specify how programs, network resources, and the operating system work for users and computers in an organization. They are collections of user and computer configuration settings that are applied on the users and computers (not on groups). For better administration of group policies in the Windows environment, the group policy objects (GPOs) are used.

**What is GPO?**

Group policy object (GPO) is a collection of group policy settings. It can be created using a Windows utility known as the Group Policy snap-in. GPO affects the user and computer accounts located in sites, domains, and organizational units (OUs). The Windows 2000/2003 operating systems support two types of GPOs, local and non-local (Active Directory-based) GPOs.

**Local GPOs**

Local GPOs are used to control policies on a local server running Windows 2000/2003 Server. On each Windows 2000/2003 server, a local GPO is stored. The local GPO affects only the computer on which it is stored. By default, only Security Settings nodes are configured. The rest of the settings are either disabled or not enabled. The local GPO is stored in the %systemroot%SYSTEM32GROUPPOLICY folder.

**Non-local GPOs**

Non-local GPOs are used to control policies on an Active Directory-based network. A Windows 2000/2003 server needs to be configured as a domain controller on the network to use a non-local GPO. The non-local GPOs must be linked to a site, domain, or organizational unit (OU) to apply group policies to the user or computer objects. The non-local GPOs are stored in %systemroot%SYSVOL<domain name>POLICIES<GPO GUID>ADM, where <GPO GUID> is the GPO's globally unique identifier. Two non-local GPOs are created by default when the Active Directory is installed:

Default Domain Policy: This GPO is linked to the domain and it affects all users and computers in the domain.

Default Domain Controllers Policy: This GPO is linked to the Domain Controllers OU and it affects all domain controllers placed in this OU.

**What is ADS** Automated Deployment Services**?**

Microsoft Windows Server 2003 Automated Deployment Services (ADS) is used by administrators to build and manage very large and scaled out deployment of Windows servers. It includes a new set of imaging tools for rapidly deploying Windows 2000 Server and Windows Server 2003 remotely. ADS offers improved communication security and a reliable script execution framework. It uses the image-based deployment method

**Under what conditions should Administrators create multiple forests?**

Microsoft recommends the creation of multiple forests under the following conditions:

**If Administrators do not trust each other:** An Administrator can create a "denial of service" condition. One can create this condition by rapidly creating or deleting objects, hence causing a large amount of replication to the global catalog. This replication can waste network bandwidth and slow down global catalog servers, as they spend time in processing replication. This condition forces administrators to create multiple forests.

**Organizations cannot agree on a forest change policy:** Changes in schema, configuration, and the addition of new domains to a forest have forest-wide impact. If organizations in a forest cannot agree on a common policy, they cannot share the same forest, forcing administrators to create multiple forests.

**If one wants to limit the scope of a trust relationship:** All domains in a forest trust each other. In order to prevent certain users from being granted permissions to certain resources, those users must be placed in a forest different from the forest containing those resources. Administrators can use explicit trust relationships to allow those users to be granted access to resources in specific domains, if required

**What is GPMC tool?**

The Group Policy Management Console (GPMC) is a tool for managing group policies in Windows Server 2003. It provides administrators a single consolidated environment for working on group policy-related tasks. GPMC provides a single interface with drag-and-drop functionality to allow an administrator to manage group policy settings across multiple sites, domains, or even forests. GPMC is used to back up, restore, import, and copy group policy objects. It also provides a reporting interface on how group policy objects (GPOs) have been deployed.

**What is Performance Monitor?**

Performance Monitor is used to get statistical information about the hardware and software components of a server. Performance Monitor is used for the following:

- Monitor objects on multiple computers.
- Log data pertaining to objects on multiple computers, over time.
- Analyze the effects of changes made to a computer.
- Launch programs and send notifications when thresholds are reached.
- Export data for analysis in spreadsheet or database applications.
- Save counter and object settings for repeated use.
- Create reports for use in analyzing performance, over time.

**What is System Monitor?**

System Monitor is a Windows graphical tool for measuring the performance of a host or remote computer. It is used to view reports on CPU load, memory usage, and interrupt rate, and the overall throughput of the traffic on a network. Using System Monitor, administrators can perform the following functions:

- Create charts and reports to measure a computer's efficiency.
- Identify and troubleshoot possible issues, such as unbalanced resource use, insufficient hardware, or poor program design.
- Plan for additional hardware needs.

System Monitor can also be used to monitor the resource use of specific components and program processes.

**What is the SQL Server: General Statistics: User Connections counter?**

The SQL Server: General Statistics: User Connections counter displays the number of user connections in SQL Server. Its maximum value is 255. An increase in the value of the counter causes performance problems and affects throughput. A Database Administrator should monitor this counter to resolve performance issues.

**What is Simple Mail Transfer Protocol (SMTP)?**

Simple Mail Transfer Protocol (SMTP) is a protocol used for sending e-mail messages between servers. It is mostly used to send messages from a mail client such as Microsoft Outlook to a mail server. Most of the e-mail systems that send mails over the Internet use SMTP to send messages from one server to another. Due to its limitations in queuing messages at the receiving end, it is generally used with either the POP3 or IMAP protocol, which enables a user to save and download messages from the server.

**What is bluescreen error?**

Bluescreen error, sometimes called Blue Screen of Death (BSOD), is the condition that occurs when a Windows computer fails to boot properly or quits unexpectedly. Microsoft refers these blue screens as "Stop errors". There are several causes of the blue screen popping up. It can be due to a poorly written device driver, bad memory, damaged registry, or usage of incompatible versions of DLLs. In Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista, a blue screen of death occurs when the kernel or a driver running in kernel mode encounters an error from which it cannot recover. This is usually caused by an illegal operation being performed. The only safe action to overcome such situations is to restart the computer.

### What is the netstat command?

The netstat command displays protocol-related statistics and the state of current TCP/IP connections. It is used to get information about the open connections on a computer, incoming and outgoing data, as well as the ports of remote computers to which the computer is connected. The netstat command gets all this networking information by reading the kernel routing tables in the memory.

### What is IIS?

Internet Information Services (IIS) is a software service that supports Web site creation, configuration, and management, along with other Internet functions. Microsoft Internet Information Services includes Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

### Clustering

A cluster is a group of two or more computers (servers) connected to provide fault tolerance and load balancing. It is dedicated to run a specific application. Each server in a cluster is known as a node. The failover and failback capabilities of a cluster bring the application downtime to zero.

Note: Server clustering is intended to provide high availability for applications and not for data.

#### Failover

In the cluster, each node or computer runs the same critical application. In case one computer fails, the other computers detect the failure and take charge immediately. This phenomenon is called failover.

#### Failback

When the failed node returns back to the network, other nodes take notice and the cluster begins to use the restored node again. This phenomenon is called failback.

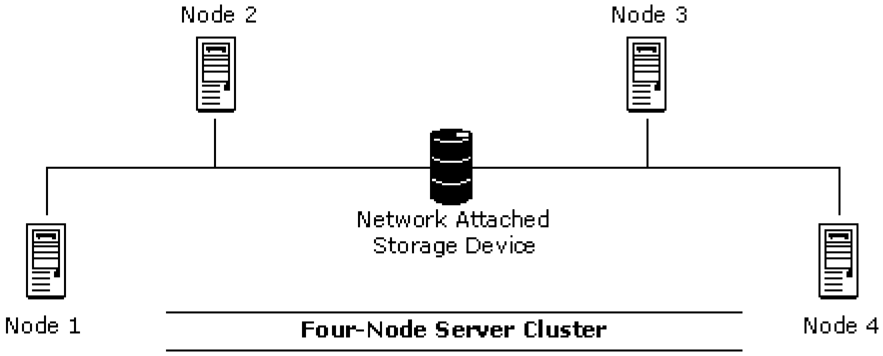
#### Types of Clusters

Windows Server 2003 supports two types of clusters:

- Server clusters
- Network Load Balancing (NLB)

**Server Clusters**

In server clusters, all nodes are connected to a common data set, such as a storage area network. All nodes have access to the same application data. Any of these nodes can process a request from a client at any time. Nodes can be configured as either active or passive. Only an active node can process requests from clients. In the event of a failure of the active node, the passive node takes charge and becomes active. Otherwise, the passive node remains idle.



Four-Node Server Cluster

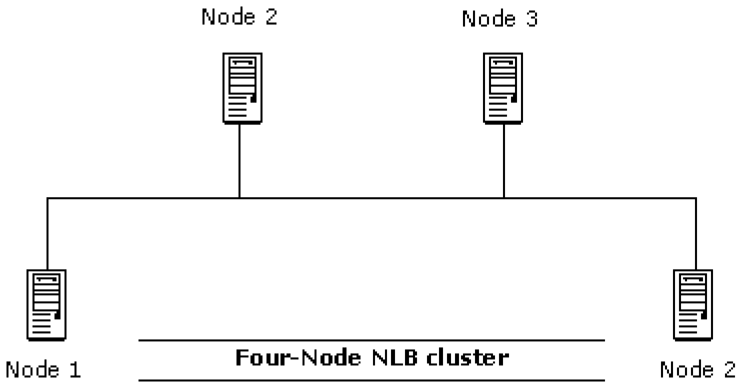
Server clusters are created for running applications that have frequently changing data sets and have long-running in-memory states. The applications such as database servers, e-mail and messaging servers, and file and print services can be included in server clusters.

A server cluster is treated as a single destination for a client. It has its own name and IP address. This address is different from the individual IP addresses of the servers in the cluster. Hence, when any server fails in the cluster, the passive server becomes active. Clients send their requests to the server cluster address. Therefore, this change over does not affect the functionality of the cluster.

Windows Server 2003 supports eight nodes in a cluster. However, Windows 2000 Server supports only two nodes in a cluster.

**Network Load Balancing**

Network Load Balancing (NLB) is a type of clustering. It is used to provide high availability and reliability of the application servers. NLB is configured for the applications that rarely change and that have very small data sets. Web servers, FTP servers, VPN servers are the areas where NLB can be used successfully.



In the NLB cluster, all nodes are active and have separate identical data sets. Multiple servers (or nodes) are used to distribute the load of processing data. Clients send the requests to the cluster, and then the clustering software distributes incoming client requests among the nodes. If a node fails, the clients' requests are served by other nodes. Network Load Balancing is highly scaleable. Both Windows 2003 and Windows 2000 operating systems support NLB clusters of up to thirty-two nodes.

**What is the Task Manager utility?**

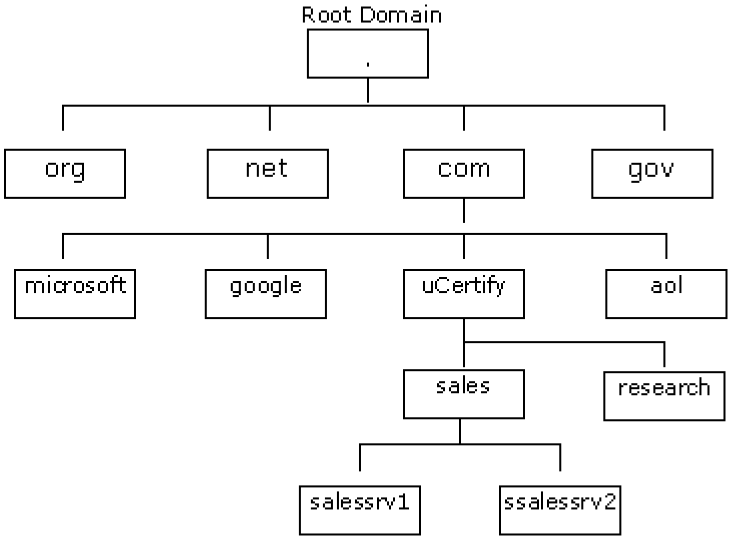
Task Manager is a utility that is used for managing applications, processes, and the general system performance and also for viewing the networking and user statistics. The Task Manager utility is used to run or end programs or applications. Administrators use this tool to quickly identify and terminate a rogue application.

**What is Task Manager utility?**

The Task Manager utility provides information about programs and processes running on a computer. By using Task Manager, a user can end or run programs, end processes, and display a dynamic overview of his computer's performance. Task Manager provides an immediate overview of system activity and performance.

**What is DNS namespace?**

DNS namespace is the hierarchical structure of the domain name tree. It is defined such that the names of all similar components must be similarly structured, but similarly identifiable. The full DNS name must point to a particular address. Consider the following image of DNS namespace of the Internet:



The salessrv1 and salessrv2 are host names of the hosts configured in the sales.ucertify.com domain. The fully qualified domain name (FQDN) of the host salessrv1 is salessrv1.sales.ucertify.com. No two hosts can have the same FQDN.

**What is 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

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

**What are group scopes?**

The scope of a group defines two characteristics:

- It determines the level of security applying to a group.
- It determines which users can be added to a group.

Windows Server 2003 supports the following scopes:

Domain Local: Domain local groups are used to assign permissions to local resources such as files and printers. Members can come from any domain.

Global: Members of this group can access resources in any domain. Members can only come from the local domain.

Universal: Members can be added from any domain in the forest. Members can access resources from any domain. Universal groups are used for managing the security across domains. Universal groups can also contain global groups. Universal groups are only available in the domains having functional level Windows 2000 native or Windows Server 2003.

**What is IPv6?**

IP addressing version 6 (IPv6) is the latest version of IP addressing. IPv6 is designed to solve many of the problems that were faced by IPv4, such as address depletion, security, auto-configuration, and extensibility. With the fast increasing number of networks and the expansion of the World Wide Web, the allotted IP addresses are depleting rapidly, and the need for more network addresses is arising. IPv6 solves this problem, as it uses a 128-bit address that can produce a lot more IP addresses. These addresses are hexadecimal numbers, made up of eight octet pairs. An example of an IPv6 address is 45CF: 6D53: 12CD: AFC7: E654: BB32: 543C: FACE.

**What is DSMOD?**

DSMOD is a command-line utility that is used to modify existing objects, such as users, computers, groups, servers, OUs etc., in Active Directory

**What is NTDSUTIL utility?**

NTDSUTIL.EXE is a command-line tool that is used to manage Active Directory. This utility is used to perform the following tasks:

- Performing database maintenance of Active Directory.
- Managing and controlling operations master roles.
- Removing metadata left behind by domain controllers.

Note:The NTDSUTIL utility is supposed to be used by experienced administrators.

**What is System File Checker utility?**

The System File Checker utility is used to verify the integrity of the operating system files, to restore them if they are corrupt, and to extract compressed files (such as drivers) from installation disks. It can also be used to backup the existing files before restoring the original files.

**What is SCHTASKS tool?**

The SCHTASKS tool is used to schedule commands and programs to run periodically or at a specific time. It adds and removes tasks from the schedule, starts and stops tasks on demand, and displays and changes scheduled tasks.

**What is CHKDSK?**

CHKDSK is a command-line tool used to scan and repair volumes on the hard disk for physical problems such as bad blocks. It also repairs volumes for logical structure errors such as lost clusters, cross-linked files, or directory errors.

**Network Configuration and Management Utilities**

Administrators use various utilities to configure and manage networks. Following are some commonly used utilities:

WINIPCFG: WINIPCFG is a Windows 9x Internet Protocol (IP) configuration utility used to display all current TCP/IP network configuration values for a computer running Microsoft TCP/IP. Network configuration values include the current IP address allocated to the computer and other useful data about TCP/IP allocation. This utility is of particular use on networks using Dynamic Host Configuration Protocol (DHCP), allowing users to determine which TCP/IP configuration values have been configured by DHCP.

**IPCONFIG:** IPCONFIG is a command-line utility used to display current TCP/IP network configuration values, and to update or release the Dynamic Host Configuration Protocol (DHCP) allocated leases. It is also used to display, register, or flush Domain Name System (DNS) names.

**NSLOOKUP**: NSLOOKUP is a utility for diagnosing and troubleshooting Domain Name System (DNS) problems. It performs its function by sending queries to the DNS server and obtaining detailed responses at the command prompt. This information can be useful for diagnosing and resolving name resolution issues, verifying whether or not the resource records are added or updated correctly in a zone, and debugging other server-related problems. This utility is installed along with the TCP/IP protocol through the Control Panel.

**PING:** PING is a command-line utility used to test connectivity with a host on a TCP/IP-based network. This is achieved by sending out a series of packets to a specified destination host. On receiving the packets, the destination host responds with a series of replies. These replies can be used to determine if the network is working properly.

**TRACERT:** TRACERT is a route-tracing Windows utility that displays the path an IP packet takes to reach its destination. It shows the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.

**PATHPING:** PATHPING is a command-line utility that pings each hop along the route for a set period of time and shows the delay and packet loss along with the tracing functionality of TRACERT, which helps determine a weak link in the path.

**NBTSTAT:** NBTSTAT is a Windows utility used to check the state of current NetBIOS over TCP/IP connections, update the NetBIOS name cache, and determine the registered names and scope IDs.

**NETSTAT:** NETSTAT is a command-line utility that displays protocol related statistics and the state of current TCP/IP connections. It is used to obtain information about the open connections on a computer, incoming and outgoing data, and also the ports of remote computers to which the computer is connected.

The NETSTAT command gets all this networking information by reading the kernel routing tables in the memory.

**TELNET:** TELNET is a command-line connectivity utility that starts terminal emulation with a remote host running the Telnet Server service. TELNET allows users to communicate with a remote computer, offers the ability to run programs remotely, and facilitates remote administration. The TELNET utility uses the Telnet protocol for connecting to a remote computer running the Telnet server software, to access files. It uses TCP port 23 by default.

## What is a certificate?

A certificate is a digital representation of information that identifies authorized users on the Internet and intranets. It can be used with applications and security services to provide authentication. Certificates are issued by certification authorities (CAs).

## What is a nonclustered index?

A nonclustered index has the same B-tree structure as the clustered index. The index consists of a root page, intermediate levels, and a leaf level. The leaf level of a nonclustered index does not contain the actual data. It contains pointers to the data that is stored in the data pages. A nonclustered index does not physically rearrange the data.

## Monitoring Physical Server Performance

SQL Server 2005 can be installed on a Windows 2000 or Windows 2003 server computer. A database administrator is always concerned about the performance of the SQL Server database engine and the server computer. Database Administrators monitor the performance of the server using various tools to analyze performance and resolve performance issues.

System Monitor: System Monitor is a tool used to monitor the performance of the server. It gives information about the resources that are under pressure. The values of various counters in System Monitor indicate which resource is under pressure. Performance deterioration can be diagnosed by setting performance alerts. These alerts show the increase or decrease in a counter value with respect to the pre-defined value. Normally the counters are monitored for a period of 24-hours. If an error occurs, a message regarding the error can either be sent to the administrator or written to the Application log. Log files can be saved in various formats such as text file, binary file, or SQL database file.

The counters that are to be measured in order to resolve performance issues are as follows:

- Memory: Pages/sec
- Memory: Available Bytes
- SQL Server: Buffer Manager: Buffer Cache Hit Ratio
- Physical Disk: Disk Reads/sec
- Physical Disk: Disk Writes/sec
- Physical Disk: %Disk Time
- Physical Disk: Avg: Disk Queue Length
- Physical Disk: % Free Space
- Logical Disk: %Free Space
- Processor: %Processor Time

- System: Processor Queue Length
- Network Interface: Bytes Received/sec
- Network Interface: Bytes Sent/sec
- Network Interface: Bytes/sec
- Network Interface: Output Queue Length
- SQL Server: General: User Connection

## Tip for server roles.

There are eight server roles. These roles are as follows:

- sysadmin
- dbcreator
- bulkadmin
- diskadmin
- processadmin
- serveradmin
- setupadmin
- securityadmin

## What is virus?

A virus is a malicious program. A computer virus passes from one computer to another in the same way as a biological virus passes from one person to another. Most viruses are written with a malicious intent, so that they can cause damage to programs and data in addition to spreading themselves. Viruses infect existing programs to alter the behavior of programs, actively destroy data, and perform actions on storage devices that render their stored data inaccessible.

Computer viruses attack the software of a computer such as operating systems, data files, application software, and e-mails. However, viruses do not affect the computer hardware

**Network Protocols**

Protocol is a set of rules and conventions by which two computers pass messages across a network. Sets of standard protocols facilitate communication between the computers in a network having different types of hardware and software. Both the sender and the receiver computers must use exactly the same set of protocols in order to communicate with each other. A protocol can lay down the rules for the message format, timing, sequencing, and error handling.

The description of the primary protocols in the suite is as follows:

| Protocol Name | Description |
|---|---|
| IP | Internet Protocol (IP) is a connectionless network-layer protocol that is the primary carrier of data on a TCP/IP network. |
| TCP | Transmission Control Protocol (TCP) is a reliable, connection-oriented protocol operating at the transport layer. This protocol can transmit large amounts of data. Application-layer protocols, such as HTTP and FTP, utilize the services of TCP to transfer files between clients and servers. |
| UDP | User Datagram Protocol (UDP) is a connectionless, unreliable transport-layer protocol. UDP is used primarily for brief exchange |

| | |
|---|---|
| | of requests and replies. |
| Telnet | Telnet is a protocol that enables an Internet user to log onto and enter commands on a remote computer linked to the Internet, as if the user were using a text-based terminal directly attached to that computer. |
| FTP | File Transfer Protocol (FTP) is a primary protocol of the TCP/IP protocol suite, used to transfer text and binary files between computers over a TCP/IP network. |
| SMTP | Simple Mail Transfer Protocol (SMTP) is used for transferring or sending e-mail messages between servers. |

**PPP:** Point-to-Point Protocol (PPP) is a set of industry-standard framing and authentication protocols included with Windows remote access to ensure interoperability with third-party remote access software. It is a data link-layer protocol designed to create a direct connection between two computers, typically using telephone lines.

**POP3**: Post Office Protocol version 3 (POP3) is a protocol used for retrieving e-mail messages. The POP3 servers allow access to a single Inbox in contrast to IMAP servers that provide access to multiple server-side folders.

IMAP: Internet Message Access Protocol (IMAP) is a protocol for receiving e-mail messages. It allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer. It is used mainly by the users who want to read their e-mails from remote locations.

**PPTP:** Point-to-Point Tunneling Protocol (PPTP) is an encryption protocol used to provide secure, low-cost remote access to corporate networks through public networks such as the Internet. Using PPTP, remote users can use PPP-enabled client computers to dial a local ISP and connect securely to the corporate network through the Internet.

**HTTP:** Hypertext Transfer Protocol (HTTP) is a client/server TCP/IP protocol used on the World Wide Web (WWW) to display Hypertext Markup Language (HTML) pages. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when a client application or browser sends a request to the server using HTTP commands, the server responds with a message containing the protocol version, success or failure code, server information, and body content, depending on the request. HTTP uses TCP port 80 as the default port.

**HTTPS**: Hypertext Transfer Protocol Secure (HTTPS) protocol is a protocol used in the Uniform Resource Locator (URL) address line to connect to a secure site. If a site has been made secure by using the Secure Sockets Layer (SSL), HTTPS (instead of HTTP protocol) should be used as a protocol type in the URL.

**ARP**: Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.

**ICMP:** Internet Control Message Protocol (ICMP) is a maintenance protocol and is normally considered a part of the IP layer. ICMP messages are encapsulated within IP datagrams, so that they can be routed throughout an internetwork.

Internet Message Access Protocol 4 (IMAP4): It is an e-mail message retrieval protocol that allows e-mail clients to retrieve e-mail messages from e-mail servers. IMAP4 has the following advantages over the POP3 protocol:

- IMAP4 can be used to download only specific mails from the mail server, while POP3 downloads all the mails from the mail server at a time.
- IMAP4 can download only a part of the message (e.g., the header) initially. Then depending upon the user, the entire message can be downloaded afterwards. However, POP3 downloads the entire message at a time.
- IMAP4 only marks a message as deleted as soon as it is being read. The message will then be deleted as soon as the user logs off, or sends the EXPUNGE command to the mail server.
- IMAP4 supports server side storage. Hence, the location of the user is insignificant. However, POP3 uses a local client application to read the mails.
- Since IMAP4 stores messages on the server side, the user does not have to bother about fault tolerance and system crashes. When the POP3 protocol is used, the messages once downloaded from the server are stored locally and can be lost if the local system crashes.
- IMAP4 allows a user to create multiple mailboxes on multiple servers under the same user name. The user can personalize these mailboxes for receiving specific kinds of mails in each mailbox. However, POP3 allows only a single user account to be configured.

- Changes made to a mail are propagated to the IMAP4 server. This feature is not available under POP3 protocol.

**However, there are some disadvantages of IMAP4 over the POP3 protocol, which are as follows:**

- If the connection with the mail server drops while reading a mail, it has to be re-established. On the other hand, POP3 downloads the entire mail at a time. Hence, if the connection with the mail server is dropped at the time of reading a mail, it does not affect the reading.
- The POP3 protocol is mostly supported by the commercially available mail servers.
- Since the mails in IMAP4 are stored on the server, the space storage management is a primary concern on such mail servers.

### IP Addressing

IP Addresses are used to uniquely identify the computers in a network, so each computer must have its own unique IP address. An IP address consists of two parts: a network identifier and a host identifier. The network identifier denotes the type of network, and the host identifier is a unique number of a particular computer. So in a particular type of network, each node has the same network id and a host id, which are unique.

The type of IP address also depends on the subnet mask, which is used to determine which part of the IP address denotes the network id and which part is the host id. For example, if the IP address is 192.168.1.200 and the subnet mask is 255.255.255.0, the network id will be 192.168.1 and the host id will be 200. In the same way, if the subnet mask is 255.255.0.0, the network id will be 192.168 and the host id will be 1.200. If the subnet mask is 255.0.0.0, the network id will be 192 and the host id will be 168.1.200.

There are two versions of IP addressing, the commonly used IPv4 and the latest version known as IPv6. They have been discussed in detail in the following paragraphs.

### IPv4

### IP Address

In this version of IP addressing, an IP address is of 32 bits in length, and is divided into four 8 bit decimal values known as octets. In these types of IP addresses, the leftmost bit has the value of 128, which is followed by 64, 32, 16, 8, 4, 2, and 1. An IP address can have values from 0 to 255 because each bit can be either a 0 or a 1. So if all the bits are 1, the value will be 255; and if all the bits are 0, the value will be 0.

### Subnet Mask

A subnet mask determines which part of the IP address denotes the network id and which part is the host id. It is also a 32-bit number, which is expressed in decimal format. The subnet mask is assigned according to the class of IP address used.

### IP Address Classes

The Internet Assigned Number Authority registers the IP addresses used in the networks to ensure their uniqueness. IP addresses have been divided into five groups or classes known as IP Address classes. Each class of IP address has a particular subnet mask associated with it. The five classes of IP addresses are class A, B, C, D and E, in which class D is reserved for multicast addressing and class E is reserved for future use. So only classes A through C are used for assigning IP addresses to client computers.

- In class A addresses, only the first octet is used to define the network id, and the rest are used for the host id. It has the address range from 1 to 126 and so it can have only 126 numbers of networks. The number of hosts possible in these types of networks is 16,777,214. It uses the subnet mask 255.0.0.0.

- In class B networks, the first two octets represent the network id and the rest are the host id. It has a range of 128-191 and can have 16384 networks with 65,534 hosts. The standard subnet mask assigned to these IP addresses is 255.255.0.0.

- In class C addresses, the first three octets are used to represent the network id. It has a range of 192-223 and can have 2,097,152 networks with 253 hosts. The subnet mask associated with it is 255.255.255.0.

- Class D addresses have an address range of 224-239, and class E addresses have an address range of 240-255.

**Default Gateway**

Default gateway is a TCP/IP configuration option, used to communicate with TCP/IP nodes on remote network segments. At least one interface must be configured with the IP address of a default gateway.

**IPv6**

The current version of IP addressing (i.e., IPv4) has its limitations. With the fast increasing number of the networks and the expansion of the World Wide Web, the IP addresses allotted are finishing fast and the need for more network addresses has arisen. IPv6 can solve this problem, as it uses a 128-bit address that can produce a lot more IP addresses. These addresses are hexadecimal numbers, made up of eight octet pairs. An example of an IPv6 address can be 45CF: 6D53: 12CD: AFC7: E654: BB32: 543C.

**Subnetting**

Subnets are subdivisions of an IP address network, used for creating smaller broadcast domains and for better utilization of the bits in the host ID. Through subnetting, the host id portion of an IP address can be used to create more networks than by using the **default subnet mask.**

Suppose that a company has been assigned a Class C IP address 200.1.1.0, and the standard subnet mask is 255.255.255.0. This means that the network id will be 200.1.1 and the total number of hosts will be 254. The company has two departments: production and sales. Members of the production department do not need to access the computers of the sales department. So it is better to have separate networks for both the departments for better security and manageability. Through subnetting, the bits from the host id portion can be used to create more networks, which will work as separate networks.

**Public and Private Networks**

Network can be differentiated as private and public. A public network is a network, which can be accessed by anyone from the general public, an example being the Internet. In contrast, a private network is accessible only by those people who have special permissions on that particular network. An example of a private network is a network within an organization such as a company, a hospital, or a college.

Public and private networks have different types of IP addressing schemes. Addresses on the Internet are assigned by the IANA (Internet Assigned Numbers Authority), which assigns them to the Internet Service Providers (ISPs), who then distribute them to the users. Apart from the public address, some addresses have been reserved for the private networks. These are not available for general public and are used in private networks.

Some addresses from each of the classes A, B, and C have been assigned for use by private networks. The address range for class A addresses is from 10.0.0.0 to 255.255.255, for class B addresses it is from 172.6.0.0 to 172.31.255.255, and for class C addresses, it is from 192.168.0.0 to 192.168.255.255.

**IP Addressing Methods:**

**Static Addressing**

In static addressing, every computer is assigned an IP address manually. It is not preferred in large networks, which have lots of hosts, because the chance of assigning duplicate addresses will be more. This will result in a conflict of IP addresses and deterioration of the speed. Also it is time consuming, as every system is configured manually and if some changes are to be made afterwards, it will consume a lot of time doing it manually for every computer.

**Dynamic Addressing**

In this type of addressing scheme, the IP addresses are assigned automatically by the use of Dynamic Host Configuration Protocol (DHCP) to all the computers in the network. This results in much less burden on the network administrator and faster configuration of the network. This type of addressing needs a DHCP server, to which a range of IP addresses is allotted. The

DHCP server automatically assigns any address from the range of IP addresses defined to the workstations on the network.

**APIPA**

Automatic private IP addressing (APIPA) is a feature of Windows XP TCP/IP that configures a unique IP address for each computer on a network when the TCP/IP protocol is configured for dynamic addressing and a DHCP server is not available or offline. The key function of APIPA is to allow resources to be available even if the DHCP server is offline. APIPA addresses are always in the range of 169.254.0.1 and 169.254.255.254 and use a subnet mask of 255.255.0.0.

When a user configures a TCP/IP connection to obtain an IP address automatically, by default the computer tries to find a DHCP server for obtaining the address. The user obtains the address if the computer finds the DHCP server. If it does not find the DHCP server, the computer uses APIPA to configure a unique IP address for the computers of a network. Since APIPA does not offer a gateway address, it can never be used on the Internet, and the clients using APIPA cannot access resources outside the local subnet.

**TCP/UDP Ports**

The default TCP/UDP ports associated with TCP/IP protocol or applications are as under:

| Protocol | Port |
|---|---|
| HTTP | 80 |
| HTTPS | 443 |
| POP3 | 110 |
| FTP | 20 |
| FTP | 21 |
| IMAP4 | 143 |
| SMTP | 25 |
| NNTP | 119 |
| NTP | 123 |
| DNS | 53 |
| TFTP | 69 |
| Telnet | 23 |
| SSH | 22 |

## What are cluster configurations?

Server clusters using the Cluster service can be set up as one of the following three different cluster configurations:

1. **Single Node server clusters:** They can be configured with or without external cluster storage devices. For Single Node server clusters without an external cluster storage device, the local disk is configured as the cluster storage device.
2. **Single Quorum Device server clusters**: They can have two or more nodes and are so configured as to attach every node to one or more shared storage devices, such as an external array of Small Computer System Interface (SCSI) disks. The cluster configuration data is stored on a single cluster storage device, also known as the quorum disk.
3. **Majority Node Set server clusters:** They can have two or more nodes, but nodes might not be attached to one or more cluster storage devices. The cluster configuration data is stored on multiple disks across the cluster, and the Cluster service guarantees that this data is kept consistent across the disks.

However, server clusters using the Cluster service are set up depending on the specific needs for failovers, in which application services are moved to another node in the cluster.

## What is N+I Hot Standby Server?

N+I Hot Standby Server is one of the failover models. It is commonly referred to as an Active/Passive mode. In an active/passive mode, the active nodes handle all client requests, whereas the passive nodes monitor the active nodes. In N+I Hot Standby Server, N denotes the number of active nodes, and I refers to the number of passive nodes. This model has a drawback that the server resources remain idle for a long time and are utilized only when another server fails. However, it is the most scalable and reliable model.

## What is failover?

Failover is a term associated with cluster services. It refers to the ability of a server to immediately start servicing the requests if a primary server fails. If the application services in a cluster-node fail, the Cluster Service generally tries to restart them on the same node. If the services do not start, then it moves the services to another node in the cluster and restarts them on that node.

## Windows Server 2003 Active Directory and Network Infrastructure

Windows Server 2003 Active Directory is a centralized database that stores the collection of information about all the resources available on the Windows Server 2003 domain. It is a hierarchical representation of all the objects and their attributes available on the network. It enables administrators to manage the network resources, i.e., computers, users, printers, shared folders, etc., in an easy way. The logical structure represented by Active Directory consists of forests, trees, domains, organizational units, and individual objects. This structure is completely independent from the physical structure of the network, and allows administrators to manage domains according to the organizational needs without bothering about the physical network structure.

Following is the description of all logical components of the Active Directory structure:

1. **Forest:** A forest is the outermost boundary of an Active Directory structure. It is a group of multiple domain trees that share a common schema but do not form a contiguous namespace. It is created when the first Active Directory-based computer is installed on a network. There is at least one forest on a network. The first domain in a forest is called a root domain. It controls the schema and domain naming for the entire forest. It can be separately removed from the forest. Administrators can create multiple forests and then create trust relationships between specific domains in those forests, depending upon the organizational needs.

2. **Trees:** A hierarchical structure of multiple domains organized in the Active Directory forest is referred to as a tree. It consists of a root domain and several child domains. The first domain created in a tree becomes the root domain. Any domain added to the root domain becomes its child, and the root domain becomes its parent. The parent-child hierarchy continues until the terminal node is reached. All domains in a tree share a common schema, which is defined at the forest level. Depending upon the organizational needs, multiple domain trees can be included in a forest.

3. **Domains:** A domain is the basic organizational structure of a Windows Server 2003 networking model. It logically organizes the resources on a network and defines a security boundary in Active Directory. The directory may contain more than one domain, and each domain follows its own security policy and trust relationships with other domains. Almost all the organizations having a large network use domain type of networking model to enhance network security and enable administrators to efficiently manage the entire network.

4. **Objects:** Active Directory stores all network resources in the form of objects in a hierarchical structure of containers and subcontainers, thereby making them easily accessible and manageable. Each object class consists of several attributes. Whenever a new object is created for a particular class, it automatically inherits all attributes from its member class. Although the Windows Server 2003 Active Directory defines its default set of objects, administrators can modify it according to the organizational needs.

5. **Organizational Unit (OU):** It is the least abstract component of the Windows Server 2003 Active Directory. It works as a container into which resources of a domain can be placed. Its logical structure is similar to an organization's functional structure. It allows creating administrative boundaries in a domain by delegating separate administrative tasks to the administrators on the domain. Administrators can create multiple Organizational Units in the network. They can also create nesting of OUs, which means that other OUs can be created within an OU.

In a large complex network, the Active Directory service provides a single point of management for the administrators by placing all the network resources at a single place. It allows administrators to effectively delegate administrative tasks as well as facilitate fast searching of network resources. It is easily scalable, i.e., administrators can add a large number of resources to it without having additional administrative burden. It is accomplished by partitioning the directory database, distributing it across other domains, and establishing trust relationships, thereby providing users with benefits of decentralization, and at the same time, maintaining the centralized administration.

The physical network infrastructure of Active Directory is far too simple as compared to its logical structure. The physical components are domain controllers and sites.

1. **Domain Controller:** A Windows 2003 server on which Active Directory services are installed and run is called a domain controller. A domain controller locally resolves queries for information about objects in its domain. A domain can have multiple domain controllers. Each domain controller in a domain follows the multimaster model by having a complete replica of the domain's directory partition. In this model, every domain controller holds a master copy of its directory partition. Administrators can use any of the domain controllers to modify the Active Directory database. The changes performed by the administrators are automatically replicated to other domain controllers in the domain.

   However, there are some operations that do not follow the multimaster model. Active Directory handles these operations and assigns them to a single domain controller to be accomplished. Such a domain controller is referred to as operations master. The operations master performs several roles, which can be forest-wide as well as domain-wide.

   ○ Forest-wide roles: There are two types of forest-wide roles:

   Schema Master and Domain Naming Master. The Schema Master is responsible for maintaining the schema and distributing it to the entire forest. The Domain Naming Master is responsible for maintaining the integrity of the forest by recording additions of domains to and deletions of domains from the forest. When new domains are to be added to a forest, the Domain Naming Master role is queried. In the absence of this role, new domains cannot be added.

   ○ Domain-wide roles: There are three types of domain-wide roles: RID Master, PDC Emulator, and Infrastructure Master.

   Domain controllers can also be assigned the role of a Global Catalog server. A Global Catalog is a special Active Directory database that stores a full replica of the directory for its host domain and the partial replica of the directories of other domains in a forest. It is created by default on the initial domain controller in the forest. It performs the following primary functions regarding logon capabilities and queries within Active Directory:

   1. It enables network logon by providing universal group membership information to a domain controller when a logon request is initiated.
   2. It enables finding directory information about all the domains in an Active Directory forest.

   A Global Catalog is required to log on to a network within a multidomain environment. By providing universal group membership information, it greatly improves the response time for queries. In its absence, a user will be allowed to log on only to his local domain if his user account is external to the local domain.

2. **Site**: A site is a group of domain controllers that exist on different IP subnets and are connected via a fast and reliable network connection. A network may contain multiple sites connected by a WAN link. Sites are used to control replication traffic, which may occur within a site or between sites. Replication within a site is referred to as intrasite replication, and that between sites is referred to as intersite replication. Since all domain controllers within a site are generally connected by a fast LAN connection, the intrasite replication is always in uncompressed form. Any changes made in the domain are quickly replicated to the other domain controllers. Since sites are connected to each other via a WAN connection, the intersite replication always occurs in compressed form. Therefore, it is slower than the intrasite replication.

## What are domain functional levels?

The domain functional levels are the various states of a domain, which enable domain-wide Active Directory features within a network environment. Domain levels are the same as domain modes in Windows 2000. Windows supports four types of functional levels:

1. **Windows 2000 Mixed:** This is the default domain functional level. When a first domain controller is installed or upgraded to Windows 2003, the domain controller is configured to run in the Windows 2000 mixed functional level. In this mode, domain controllers running the following operating systems are supported:
   - Windows NT Server 4.0
   - Windows 2000 Server
   - Windows Server 2003
2. **Windows 2000 Native:** In this level, domain controllers running Windows 2000 and Windows 2003 can interact with each other. No domain controller running a pre-Windows 2000 version is supported in this functional level of the domain.

3. **Windows Server 2003 Interim**: This functional level allows a Windows Server 2003 domain controller to interact with domain controllers in the domain running Windows NT 4.0 or Windows Server 2003. This functional level is used to upgrade the first Windows NT domain to a new forest.

   Note: Windows Server 2003 interim functional level does not support domain controllers running Windows 2000.

4. **Windows Server 2003**:This functional level of domain allows a Windows Server 2003 domain controller to interact only with the domain controllers running Windows 2003 in the domain. A domain level can be raised to Windows Server 2003 only when all the domain controllers in the domain are running Windows Server 2003

## What is site?

A site is a collection of one or more well-connected (usually a local area network) TCP/IP subnets. The network between the subnets must be highly reliable and fast (512 Kbps and higher). Although the sites are defined on the basis of location, they can be spanned over more than one location. A site structure corresponds to the physical environment, whereas a domain is the logical environment of the network. A site can contain single or multiple domains, and a domain can contain single or multiple sites.

Sites are created to physically group the computers and resources for optimizing the network traffic. Administrators can configure Active Directory access and replication technology to take advantage of the physical network by configuring sites. When a user logs on to a network, the authentication request searches for the domain controllers in the same site where the user is located. A site prevents the network traffic from traveling on wide area network (WAN) links that are slow.

## What is DCDIAG tool? AD Trubleshooting tool.

Domain Controller Diagnostic (DCDIAG) is a diagnostic tool that is used to analyze the domain controllers in a forest to report problems or issues. The scope of this tool covers the functions of the domain controllers and interactions across an entire enterprise. The DCDIAG tool is used to diagnose the domain controller status for the following issues:

- Connectivity
- Replication
- Integrity of topology
- Permissions on directory partition heads
- Permissions of users
- Functionality of the domain controller locator
- Consistency among domain controllers in the site
- Verification of trusts
- Diagnosis of replication latencies
- Replication of trust objects
- Verification of File Replication service
- Verification of critical services

Note: DCDIAG is an analyzing tool, which is mostly used for the reporting purposes. Although this tool allows specific tests to be run individually, it is not intended as a general toolbox of commands for performing specific tasks.

## What is 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

## Windows 2003 system services?

Windows Server 2003 comes with many system services that have different functionalities in the operating system. When Windows Server 2003 is first installed, the default system services are created and are configured to run when the system starts

Example :

Following are some important system services of Windows Server 2003:

Alerter
Automatic Updates
Cluster Service
DHCP
Distributed File System
DNS Client service
DNS Server service
Event Log service
Remote Installation
Remote Procedure Call (RPC)
Routing and Remote Access

## What is a paging file?

A paging file is a hidden file on the hard disk used by Windows operating systems to hold parts of programs and data that do not fit in the computer's memory. The paging file and the physical memory, or random access memory (RAM), comprise the virtual memory. Windows operating systems move data from the paging file to the memory as required and move data from the memory to the paging file to make room for new data. A paging file is also known as a swap file.

## What are authoritative and non-authoritative Active Directory restores?

There are two general methods of restoring Active Directory from the backup media: authoritative and non-authoritative.

Authoritative restore makes the computer authoritative over other domain controllers. Data restored authoritatively in a computer takes precedence over other domain controllers' data, despite the fact that the restored data is older than the current replicas. Authoritative restore is typically used to restore a system to a previously known state. The NTDSUTIL command-line tool allows authoritatively restoring the entire directory, a subtree, or individual objects, provided they are leaf objects.

A non-authoritative restore results in the restored data (which may be outdated) becoming synchronized with the data on other domain controllers through replication.

## What is ADPREP tool?

The ADPREP tool is used to prepare Windows 2000 domains and forests for an upgrade to Windows Server 2003. It extends the schema, updates default security descriptors of selected objects, and adds new directory objects as required by some applications.

Syntax:

**ADPREP {/forestprep | /domainprep}**

| Parameter | Description |
|---|---|
| /forestprep | Prepares a Windows 2000 forest for an upgrade to a Windows Server 2003 forest. |
| /domainprep | Prepares a Windows 2000 domain for an upgrade to a Windows Server 2003 domain. |
| /? | Displays help for the command. |

To run ADPREP /forestprep, the administrator must be a member of the Enterprise Admins group and the Schema Admins group in Active Directory. The ADPREP /forestprep command must be run on the schema master.

To run ADPREP /domainprep, the administrator must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory. The ADPREP /domainprep command must be run on each infrastructure master.

## Which files are included in the System State data?

Following are the files included in the System State data:

- Boot files, including the system files and all files protected by Windows File Protection (WFP)
- Active Directory (on domain controller only)
- SYSVOL (on domain controller only)
- Certificate Services (on certification authority only)
- Cluster database (on cluster node only)
- Registry
- IIS metabase
- Performance counter configuration information
- Component Services Class registration database

## What is RENDOM utility?

RENDOM is a Windows 2003 utility used to rename and restructure a domain in the forest. It can perform the following tasks:

- Change the DNS and NetBIOS names of the forest-root domain.
- Change the DNS and NetBIOS names of any tree-root domain.
- Change the DNS and NetBIOS names of the parent and child domains.
- Restructure a domain's position in the forest.

The utility is supplied by Microsoft and is placed in the ValueaddMsftMgmtDomren directory on the Windows Server 2003 CD-ROM.

Note: Renaming a domain is a thorough multi-step process that requires a detailed understanding of the operation. It affects every domain controller in the forest.

## What is volume shadow copy?

The Windows Backup provides a feature of taking a backup of files that are opened by a user or system. This feature is known as volume shadow copy. Volume shadow copy makes a duplicate copy of all files at the start of the backup process. In this way, files that have changed during the backup process are copied correctly. Volume shadow copy ensures the following:

- Applications continue to write data to the volume during a backup
- Backups are scheduled at any time without locking out users.

## What is Performance Logs and Alerts?

Performance Logs and Alerts is an MMC snap-in that is used to establish performance baselines, diagnose system problems, and anticipate increased system resource demands. It is used to obtain useful data for detecting system bottlenecks and changes in system performance. The alerting functionality of this tool is extremely useful for troubleshooting intermittent and difficult-to-reproduce problems. It uses the same performance counters as the System Monitor for capturing information to log files over a period of time. The prime benefit of this tool is the ability to capture performance counter information for further analysis. Performance Logs and Alerts runs as a service and loads during computer startup. It does not require a user to log on to a computer.

**Network Interface Card**

A network interface card (NIC) is a computer circuit board or card installed in a computer. It provides a physical connection between a computer and the network. Network interface cards provide a dedicated, full-time connection to a network. Each network Interface card has a unique Media Access Control (MAC) address.

Media Access Control (MAC) address is a numerical identifier that is unique for each network interface card (NIC). MAC addresses are 48-bit values expressed as twelve hexadecimal digits, usually divided into hyphen-separated pairs, for example, FF-00-F8-32-13-19. MAC addresses are also referred to as hardware addresses, Ethernet addresses, and universally administered addresses (UAAs).

**Hub**

A hub is a device used to link computers in a network. It connects computers that have a common architecture, such as Ethernet, ARCnet, FDDI, or Token Ring. All hub-computer connections for a particular network use the same type of cable, which can be twisted-pair, coaxial, or fiber-optic. Hubs are generally used in star topology networks. Token Ring hubs are also known as Multistation Access Units (MSAUs). A hub works on the physical layer of the OSI model. Two types of hubs are available as follows:

1. Active hub is a central device used to connect computers in a star network. It regenerates and retransmits deteriorated signals on the network.

2. Passive hub is a central device used to connect computers in a star network. It receives information through one of its ports and sends it to the computers connected to every other port. Therefore, although the information is broadcasted to the network, only the destination computer reads it. A passive hub does not regenerate signals.

**Repeater**
A repeater is a basic LAN connection device. It allows a network cabling system to extend beyond its maximum allowed length and reduces distortion by amplifying or regenerating network signals. Repeaters can also be used to connect network segments composed of different media, such as connecting a twisted pair cable segment to a fiber-optic cable segment. A repeater works at the physical layer of the OSI model.

**Switch**
A switch is a network connectivity device that brings media segments together in a central location. It reads the destination's MAC address or hardware address from each incoming data packet and forwards the data packet to its destination. This reduces the network traffic. Switches operate at the data-link layer of the OSI model.

**Router**
A router is a device that routes data packets between computers in different networks. It is used to connect multiple networks, and it determines the path to be taken by each data packet to its destination computer. A router maintains a routing table of the available routes and their conditions. By using this information, along with distance and cost algorithms, the router determines the best path to be taken by the data packets to the destination computer. A router can connect dissimilar networks, such as Ethernet, FDDI, and Token Ring, and route data packets among them. Routers operate at the network layer (layer 3) of the Open Systems Interconnection (OSI) model.

**Brouter**
A brouter is a combination of a bridge and a router. It is used to connect dissimilar network segments, and it routes only a specific transport protocol such as TCP/IP. A brouter also works as a bridge for all types of packets, passing them on as long as they are not local to the LAN segment from which they have originated.

**Bridge**
A bridge is an interconnectivity device that connects two local area networks (LANs) or two segments of the same LAN using the same communication protocols and provides address filtering between them. Users can use this device to divide busy networks into segments and reduce network traffic. A bridge broadcasts data packets to all the possible destinations within a specific segment. Bridges operate at the data-link layer of the OSI model.

**Gateway**
A gateway is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies. It provides greater functionality than a router or bridge because a gateway functions both as a translator and a router. Gateways are slower than bridges and routers. A gateway is an application layer device.

**Modem**
Modem stands for Modulator-Demodulator. It is a device that enables a computer to transmit information over standard telephone lines. Since a computer stores information digitally and a telephone line is analog, a modem converts digital signals to analog and vice versa. The conversion of a digital signal to analog is known as modulation and that of an analog signal to digital is known as demodulation.

**Normal Backups**

When an administrator chooses to use a normal backup, all selected files and folders are backed up and the archive attribute of all files are cleared. A normal backup does not use the archive attribute to determine which files to back up. A normal backup is used as the first step of any backup plan. It is used with the combination of other backup types for planning a backup strategy of an organization. Normal backups are the most time-consuming and are resource hungry. Restoration from a normal backup is more efficient than other types of backups.

**Incremental Backups**

An incremental backup backs up files that are created or changed since the last normal or incremental backup. It takes the backup of files of which the archive attribute is set. After taking a backup, it clears the archive attribute of files. An incremental backup is the fastest backup process. Restoring data from an incremental backup requires the last normal backup and all subsequent incremental backups. Incremental backups must be restored in the same order as they were created.

Note: If any media in the incremental backup set is damaged or data becomes corrupt, the data backed up after corruption cannot be restored.

**Differential Backups**

Differential backup backs up files that are created or changed since the last normal backup. It does not clear the archive attribute of files after taking a backup. The restoration of files from a differential backup is more efficient than an incremental backup.

**Copy Backups**

A copy backup copies all selected files and folders. It neither uses nor clears the archive attribute of the files. It is generally not a part of a planned scheduled backup.

**Daily Backups**

A daily backup backs up all selected files and folders that have changed during the day. It backs up data by using the modified date of the files. It neither uses nor clears the archive attribute of the files.

**Combining backup types**

The easiest backup plan is to take a normal backup every night. A normal backup every night ensures that the data is restored from a single job the next day. Although the restoration of data from a normal backup is easy, taking a backup is time consuming. Hence, an administrator is required to make an optimal backup plan. An administrator must consider the following points before creating a backup plan:

- The time involved in taking the backup.
- The size of the backup job.
- The time required to restore a system in the event of a system failure.

The most common solutions for the needs of different organizations include the combination of normal, differential, and incremental backups.

**Combination of Normal and Differential Backups**

An administrator can use a combination of a normal backup and a differential backup to save time in taking a backup as well as for a restoration of data. In this plan, a normal backup can be taken on Sunday, and differential backups can be taken on Monday through Friday every night. If data becomes corrupt at any time, only a normal and last differential backup are required to be restored. Although this combination is easier and takes lesser time for restoration, it takes more time to take backup if data changes frequently.

**Combination of Normal and Incremental Backups**

A combination of normal and incremental backups can be used to save more time for taking backups. In this plan, a normal backup is taken on Sunday and incremental backups on Monday through Friday every night. If data becomes corrupt at any time, a normal and all incremental backups till date are required to be restored.

**Backing up a System State Data**

**System State Data**

System State data contains critical elements of the Windows 2000 and Windows Server 2003 operating systems. Following are the files included in the System State data:

- Boot files, including the system files and all files protected by Windows File Protection (WFP)
- Active Directory (on domain controller only)
- SYSVOL (on domain controller only)
- Certificate Services (on certification authority only)
- Cluster database (on cluster node only)
- Registry
- IIS metabase
- Performance counter configuration information
- Component Services Class registration database

## What is Internet Security and Acceleration (ISA) Server 2000?

Internet Security and Acceleration Server 2000 is a Microsoft product that is used to provide powerful security and network acceleration while accessing the Internet. It works as a firewall as well as a Web cache server. It integrates with the Microsoft Windows 2000 operating system for policy-based security, acceleration, and management of internetworking.

Features of ISA Server

- It provides an additional level of security.
- It offers industry-leading Web cache performance.
- It integrates with Microsoft Windows 2000.
- It enables administrators to use bandwidth efficiently.
- It provides increased manageability.
- It provides enhanced usability.
- It provides integrated services.
- It provides increased extensibility.
- It provides improved interoperability.
- It provides enhanced scalability.

## Site and Replication

**What is a Site?**

A site is a collection of one or more well-connected (usually a local area network) TCP/IP subnets. The network between the subnets must be highly reliable and fast (512 Kbps and higher). Although the sites are generally defined on the basis of location, they can be spanned over more than one location. A site structure corresponds to the physical environment, whereas a domain is the logical environment of the network. A site can contain single or multiple domains, and a domain can contain single or multiple sites.

The sites are created to physically group the computers and resources to optimize network traffic. Administrators can configure Active Directory access and replication technology to take advantage of the physical network by configuring sites. When a user logs on to the network, the authentication request searches for the domain controllers in the same site as the user. A site prevents the network traffic from traveling on slow wide area network (WAN) links.

**What are Directory Tree, Directory Partition, and Replica?**

Directory tree is a hierarchy of objects and containers of Active Directory, which represents all the objects in the forest. Each domain controller stores a copy of a specific part of the directory tree, called a directory partition (sometimes called naming context). The copy of the directory partition is called a replica. A replica contains all attributes for each directory partition object. Each domain controller in the forest stores a replica.

**What is replication?**

Replication is a process through which the changes made to a replica on one domain controller are synchronized to replicas on all the other domain controllers in the network. Each domain controller stores three types of replicas:

- **Schema partition:** This partition stores definitions and attributes of objects that can be created in the forest. The changes made in this partition are replicated to all the domain controllers in all the domains in the forest.
- **Configuration partition:** This partition stores the logical structure of the forest deployment. It includes the domain structure and the replication topology. The changes made in this partition are replicated to all the domain controllers in all the domains in the forest.
- **Domain partition:** This partition stores all the objects in a domain. Changes made in this partition are replicated to all the domain controllers within the domain.

Note: Windows Server 2003 supports a new type of directory partition named Application directory partition. This partition is available only to Windows 2003 domain controllers. The applications and services use this partition to store application-specific data.

Creating, modifying, moving, and deleting an object trigger a replication between domain controllers. Replications are of two types:

- **Intrasite:** An intrasite (within a site) replication mostly uses LAN connections. As intrasite replication does not compress data, it saves a computer's CPU time. In an intrasite replication, the replication partners poll each other periodically and notify each other when changes need to be replicated, and then pull the information for processing. Active Directory uses a remote procedure call (RPC) transport protocol for intrasite replication.
- **Intersite:** As an intersite (between sites) replication uses WAN connections, a large amount of data is compressed to save WAN bandwidth. For the same reason, the replication partners do not notify each other when changes need to be replicated. Instead, administrators configure the replication schedule to update the information. Active Directory uses an IP or SMTP protocol for intersite replication.

For intrasite replication to take place, connection objects are required. The Active Directory automatically creates and deletes connection objects as and when required. Connection objects can be created manually to force replication.

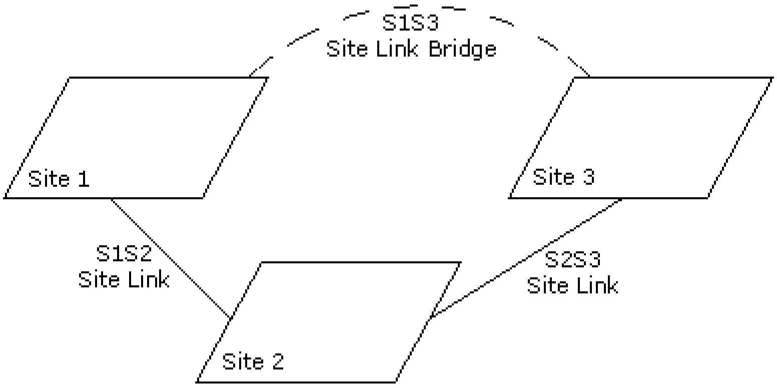
### What are Site Links?

Site links are logical, transitive connections between two or more sites. For intersite replication to take place, site links are required to be configured. Once a site link has been configured, the knowledge consistency checker (KCC) then automatically generates the replication topology by creating the appropriate connection objects. Site links are used to determine the paths between two sites. They must be created manually.

Site links are transitive in nature. For example, if Site 1 is linked with Site 2 and Site 2 is linked with Site 3, then Site 1 and Site 3 are linked transitively. The administrators can control transitivity of the site link. By default, transitivity is enabled. Site link transitivity can be enabled or disabled through a bridge.

### What is Site Link Bridge?

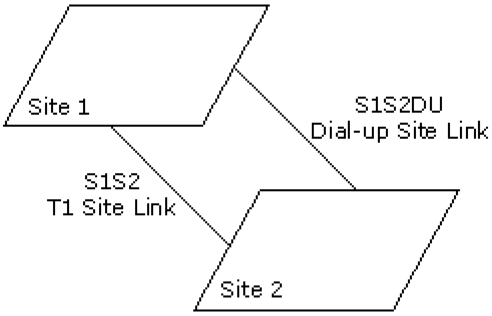
A site link bridge is created to build a transitive and logical link between two sites that do not have an explicit site link. The site link bridge is created only when the transitivity of the site link is disabled.



**What is Site Link Cost?**

Site link cost is an attribute of a site link. Each site link has been assigned a default cost of 100. The knowledge consistency checker (KCC) uses the site link cost to determine which site links should be preferred for replication. It should be remembered that the lower the site link cost, the more preferred is the link.

For example, an administrator has to configure the site link cost of links between Site 1 and Site 2. There are two site links available as shown in the image below:



S1S2 is a T1 site link that uses T1 lines for replication, whereas S1S2DU uses a dial-up connection for replication. If the administrator requires that the KCC should prefer the S1S2 site link to the S1S2DU site link for replication, he will have to configure the SIS2 link with a lower cost than that of the S1S2DU link. Any site link configured with the site link cost of one (1) will always get preference over the other site links with a higher cost.

**What is Bridgehead Server?**

A bridgehead server is a domain controller in each site, which is used as a contact point to receive and replicate data between sites. For intersite replication, KCC designates one of the domain controllers as a bridgehead server. In case the server is down, KCC designates another one from the domain controller. When a bridgehead server receives replication updates from another site, it replicates the data to the other domain controllers within its site.

**What is Preferred Bridgehead Server?**

A preferred bridgehead server is a domain controller in a site, specified by an administrator, to act as a bridgehead server. Administrators can specify more than one preferred bridgehead server, but only one server is active at a time in a site. A preferred bridgehead server is designated to take advantage of a certain domain controller having the appropriate bandwidth to transmit and receive information

## What is Performance Logs and Alerts?

Performance Logs and Alerts is an MMC snap-in that is used to establish performance baselines, diagnose system problems, and anticipate increased system resource demands. It is used to obtain useful data for detecting system bottlenecks and changes in system performance. The alerting functionality of this tool is extremely useful for troubleshooting intermittent and difficult-to-reproduce problems. It uses the same performance counters as the System Monitor for capturing information to log files over a period of time. The prime benefit of this tool is the ability to capture performance counter information for further analysis. Performance Logs and Alerts runs as a service and loads during computer startup. It does not require a user to log on to a computer

## What is WLBS.EXE?

WLBS.EXE is a command-line tool, which is used as a Network Load Balancing control program. WLBS.EXE is used to start, stop, and administer Network Load Balancing, as well as to enable and disable ports and to query cluster status.
Note: WLBS.EXE cannot be used to change the registry parameters of Network Load Balancing.

## What is buffer overflow?

Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application

## What is DMZ?

Demilitarized zone (DMZ) or perimeter network is a small network that lies in between the Internet and a private network. It is the boundary between the Internet and an internal network, usually a combination of firewalls and bastion hosts that are gateways between inside networks and outside networks. DMZ provides a large enterprise network or corporate network the ability to use the Internet while still maintaining its security

## What is Kerberos v5?

Kerberos v5 is an authentication method used by Windows operating systems to authenticate users and network services. Windows 2000/2003 and XP clients and servers use Kerberos v5 as the default authentication method. Kerberos has replaced the NT LAN Manager (NTLM) authentication method, which was less secure. Kerberos uses mutual authentication to verify both the identity of the user and network services. The Kerberos authentication process is transparent to the users.

Note: Kerberos v5 is not supported on Windows XP Home clients or on any clients that are not members of an Active Directory domain.

## What is Software Update Services (SUS)?

Software Update Services (SUS) is a tool used to acquire and distribute critical Windows patches to computers running Windows operating systems. Administrators use SUS to download and test the patches, and then deploy the patches to the appropriate computers running the Automatic Updates clients. SUS consists of three components:

1. Software Update Services (SUS) that runs on the server.
2. Automatic Updates (AU) that runs on client computers.
3. Group Policy settings that control AU clients from Active Directory.

SUS does not support Microsoft Office or Microsoft BackOffice products. It updates the operating systems (except Windows NT or Windows 9x), Microsoft IIS, and Microsoft Internet Explorer (IE) only.

## Which installation modes are available with ISA Server?

The following modes are available as a part of the ISA Server setup process:

- Firewall: In Firewall mode, network configuration can be secured by configuring rules that control communication between a corporate network and the Internet. In this mode, internal servers can also be published to share data with Internet users.
- Cache: In Cache mode, network performance can be improved and bandwidth can be saved by storing commonly accessed Internet objects locally. Requests can be routed from the Internet users to an appropriate internal Web server.
- Integrated: Integrated mode is a combination of Firewall and Cache modes. It supports all the features available in Firewall and Cache modes of ISA Server