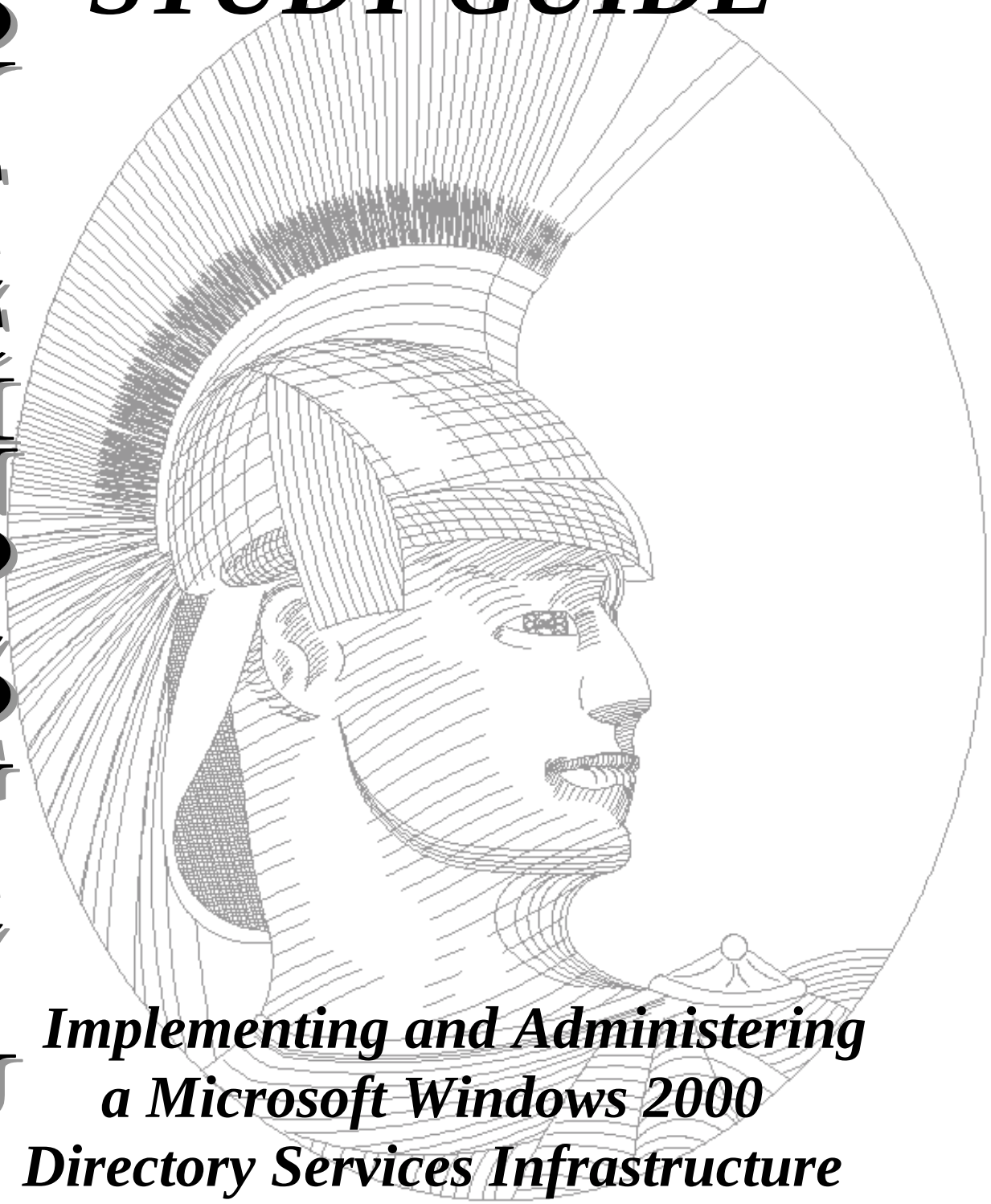
TROY TECHNOLOGIES USA

MCSE STUDY GUIDE



Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure Exam 70-217

Edition 1

Congratulations!!

You have purchased a ***Troy Technologies USA*** Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure MCSE exam. Study and memorize the following concepts, questions and answers for approximately 10 to 12 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 10 to 12 hours and then you are ready!!!

GOOD LUCK!

Guarantee

If you use this study guide correctly and still fail the exam, send your official score notice and mailing address to:

Troy Technologies USA
8200 Pat Booker Rd. #368
San Antonio, TX 78233

We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

Table of Contents

Microsoft Windows 2000
Directory Services Infrastructure Concepts

Active Directory Overview

The Microsoft Windows 2000 Active Directory (AD) is the central repository in which all objects in an enterprise and their respective attributes are stored. It is a hierarchical, multimaster enabled database, capable of storing millions of objects. Because it is multimaster, changes to the database can be processed at any given domain controller (DC) in the enterprise regardless of whether the domain controller is connected or disconnected from the network.

Windows 2000 Domain Hierarchy

Windows 2000 domains use a hierarchical model with a parent domain and child domains under it. A single domain tree consists of a parent domain and all of its child domains. Domains are named in accordance with the Internet's Domain Name System standard. If the parent (root) domain is called "troytec.com", a child may be called "support.troytec.com". In a Windows 2000 domain, trust relationships between domains are made automatically either by two-way, or transitive trusts. Domain A can trust Domain B, Domain A can trust Domain C, and Domain B can trust Domain C. In addition, you have the option of only having one way trusts, or no trust. The act of permissions flowing downward from parent to child is called inheritance. It is the default, but can be blocked for specific objects or classes of objects.

AD Database Overview

Forest and Trees

The AD database contains all information about objects in all the domains from logon authentication to objects in the directory. A hierarchical structure made up of multiple domains that trust each other is called a tree. A set of object definitions and their associated attributes is called a schema. All domains in a tree will share the same schema and will have a contiguous namespace. A namespace is a collection of domains that share a common root name. An example of this is support.troytec.com, marketing.troytec.com, and troytec.com. A disjointed namespace contains domains that are interrelated, but don't share common root name. This might occur when a company merges with another company. An example of this is troytec.com, and abc.com. A forest is one or more domain trees that have separate contiguous namespaces. All the trees in a forest share a common schema and trust one another because of transitive trusts. If you have multiple forests, you must set up an explicit trust between them.

Sites

Use the Active Directory Sites And Services Microsoft Management Console (MMC) snap-in to configure sites. To create a site, add the subnets the domain controllers are in to the site object. A site object is a collection of subnet addresses that usually share a geographic location. Sites can span domains, and domains can span sites. If the subnet address of a client or domain controller has not been included in any site, it is assigned to the initial site

container created by AD, named Default-First-Site. If a subnet requires fast access to the directory, it should be configured as a site. In every site, at least one global catalog server should be installed for fast directory access, and at least one domain controller should be installed.

Dynamic Domain Name System (DDNS)
AD requires Dynamic Domain Name System (DDNS) for name resolution of objects. The records in the DNS database are automatically updated instead of the normal DNS manual methods.

Organizational Units (OUs)
An Organizational Unit is a container object that can hold users, groups, printers, and other objects, as long as these objects are members of the same domain as the OU. You can organize the domain into logical administrative groups using OUs. OUs allow you to delegate the management of the objects in the OU to other users. You can assign separate sets of permissions over the objects in the OU, other than the permissions in your domain. The Active Directory Users And Computers MMC snap-in is used to create and manage OUs. To delegate the control of an OU, use the Delegation of Control Wizard.

Global Catalog
A global catalog contains all the objects in the AD, with only a subset of their attributes. This allows you to find object quickly even in a large multi-domain environment. The global catalog serves as an index to the entire structure of all domains and trees in a forest. It is also used for user authentication, so a user can log on at any location without having to perform a lookup back to the user's home domain. The first server installed in a tree is called the global catalog server. Additional global catalog servers will improve the response time of queries for AD objects. Use the Active Directory Sites And Services MMC snap-in to create additional global catalog servers.

Domain Controllers
All domain controllers in a Windows 2000 domain have a writeable copy of the AD database. All changes performed on any domain controller are replicated to all the other domain controllers within the domain via multimaster replication. Multimaster replication occurs when there is no master domain controllers, and all domain controls are considered equal. Domain controllers are not required to replicate directly with each other. Domain controllers that are in close proximity to each other can replicate with each other, and then one of them can send all the changes to a remote domain controller.

Replication
A connection object is a connection that AD uses for replication. Connection objects are fault tolerant. When a communication fails, AD will automatically reconfigure itself to use another route to continue replication. The process that creates connection objects is called Knowledge Consistency Checker (KCC). It runs on all domain controllers every 15 minutes by default. It creates connection objects that provide the most favorable route for replication at the time of replication. KCC uses the network model that has been defined to determine

connectivity between sites, but it will configure the links between domain controllers in the same site without assistance. Changes that need to be replicated are based on the update sequence number (USN). Each domain controller maintains a table of its own USNs, which is updated whenever it makes a change to an AD object. The USN is written to the AD database with the attribute that has changed. Other domain controllers use this USN to determine whether a change has occurred on a replication partner. To reduce network traffic, only the changed attribute will be transferred. After a domain controller fails, it attempts to replicate with all of the domain controllers when brought back online. It only requests updates with USNs greater than the last USN that was applied.

Sites
AD uses sites to control replication traffic over a WAN. A site is a group of domain controllers joined by a fast connection. Intrasite replication traffic can consume a large amount of bandwidth. Intersite traffic is compressed at a rate of 10:1.

Site Links
Site links are created using either Remote Procedure Call (RPC), or Simple Mail Transfer Protocol (SMTP) after sites are created. These links facilitate the replication between sites. If not created, domain controllers will not be able to send or receive directory updates. Replication availability, cost, and replication frequency can be configured for greater efficiency. The KCC uses settings from the site links to determine which connection objects to create to replicate directory data. SMTP transport is generally used for connections that are intermittent, such as dial-up links. Replication can be set up for a specific schedule by specifying when replication over that site link cannot take place, or by default, which allows replication to occur at any time. The default replication time is every three hours. Cost value determines which link to use when there are multiple links between sites. AD always uses the lowest cost path available. You can designate a domain controller as a bridgehead server to act as a replication gateway. It accepts all replication data from other sites via slow links and distributes it to other domain controllers in the site via fast links. Bridgehead servers are commonly used when sites are separated by firewalls, proxy servers, or Virtual Private Networks (VPNs).

Site Link Bridge
A site link bridge specifies a preferred route for replication traffic. It is the process of building a connection between two links. It is not needed in a fully routed IP network. If you set up site link bridges, you must turn off the default option to bridge all site links automatically.

Installing, Configuring, and Troubleshooting Active Directory

Microsoft Management Console (MMC)
MMC is a framework in which you can add custom utilities called snap-ins to administer system components. Preconfigured MMCs that are used to work with AD are:

Snap-in	Description

AD Domains And Trusts	Configures and manages trust relationships.
AD Sites And Services	Creates and manages sites, site links, site link bridges, replications and OUs.
AD Users And Computers	Creates and Manages user accounts, resource objects and security groups.
DNS	Manages DNS.
Domain Security Policy	Manages security policy for domains.

Active Directory

Installing Active Directory

Servers install as member servers (standalone) by default. Active Directory services can be only installed on a Windows 2000 Server, an Advanced Server or a Datacenter Server. You must have at least 256 MB of memory available, and at least one NTFS 5.0 partition. The Directory Services database is installed to %systemroot%\ntds\ntds.dit by default. AD depends on DNS, and as such, cannot be installed without it. During the installation program, if DNS is not found, you are given the choice of aborting the installation or installing DNS on the server you're upgrading to a domain controller.

You do not have to reinstall the operating system to create a domain controller. A member server can be promoted to a domain controller or demoted to a member server at any time by using dcpromo. The answer file contains only the [DCInstall] section. Use the /answer**:**<answer_file> switch to specify the answer file. To remove AD and demote a domain controller to a member server, log on as an Administrator, then supply Enterprise Administrator credentials during the demotion process.

Use mixed mode (installed by default) if your domain consists of both AD and pre-Windows 2000 domain controllers. If Windows 2000 is being installed into an infrastructure where all domain controllers will be running Windows 2000, then domain controllers should utilize native mode.

Creating Sites

By default, all domain controllers are placed in the default site, Default-First-Site-Name, and the KCC handles all replication. To create a site go to Start | Programs | Administrative Tools | AD Sites And Services. Right-click Sites, and choose New Site. Type the name of your site and select a site link. If the IP address of a newly installed domain controller matches an existing subnet in a defined site, it is automatically added to that site. Otherwise, it is added to the site of the source domain controller.

Creating Subnets

Subnets are the objects used by AD to determine the boundaries of sites. Workstations use subnets to determine the closest domain controller for logons. AD uses IP subnets to find a domain controller in the same site as the system that is being authenticated during a logon and to determine the best routes between domain controllers. To create a subnet go to Start | Programs | Administrative Tools | AD Sites And Services | Sites. Right-click Subnets, and

choose New Subnet. Enter the subnet address and subnet mask. Associate the subnet with a site.

Creating Site Links

Creating a site link between two or more sites influences replication. In creating a site link, you can specify what connections are available, which ones are preferred, and how much bandwidth is available. AD can use this information to choose the most efficient times and connections for replication. Site links are not created automatically, they must be manually created. Computers in different sites cannot communicate with each other or replicate data until a site link has been established between them. To create a new site link go to Start | Programs | Administrative Tools | AD Sites And Services Right-click the Inter-Site Transports folder (IP or SMTP), then click New Site Link. Provide a link name and choose the sites you want to connect. The DEFAULTIPSITELINK object is created in the IP container when AD is installed on the first domain controller in a site. Default site link cost is 100. The slower a connection, the more it should cost. The replication interval must be at least 15 minutes and cannot exceed 10,080 minutes.

Replication protocols over site links:

Protocol	Description
SMTP Replication	Only used for intersite replication. Is synchronous and ignores all schedules. Requires installation of a Certificate Authority (CA).
IP Replication	Uses Remote Procedure Calls (RPCs) for both intersite and intrasite replication. Intersite IP replication uses schedules by default. Does not require a CA.

Creating Site Link Bridges

In a fully routed network, it is not necessary to create site link bridges as all site links using the same protocol are bridged by default. When a network is not fully routed it is necessary to disable the default site link bridging. To create a new site link bridge, go to Start | Programs | Administrative Tools | AD Sites And Services. Right-click the Inter-Site Transports folder (IP or SMTP), then click New Site Link Bridge. Provide a site link bridge name and choose the site links you want to connect. To disable default site link bridging, go to Start | Programs | Administrative Tools | AD Sites And Services. Right-click the Inter-Site Transports folder (IP or SMTP), then click Properties. Uncheck the Bridge All Site Links check box.

Creating Connection Objects

Connection objects are automatically created by the Knowledge Consistency Checker (KCC). Manually adding connection objects may increase replication performance. To create a connection object, go to Start | Programs | Administrative Tools | AD Sites And Services. Open the Site folder. Next, open the Servers folder, then expand the server object to get to the NTDS Settings. Right-click NTDS Settings, and choose New Active Directory

Connection. In the Find Domain Controllers box, select the desired domain controller. In the New Object – Connection window, name the new connection.

Creating Global Catalog Servers

There should be at least one global catalog server located in every site. If your network has multiple sites, you may wish to create additional global catalog servers to prevent queries from being performed across slow Wide Area Network (WAN) links. AD creates one global catalog server per forest by default. To create a global catalog server, go to Start | Programs | Administrative Tools | AD Sites And Services. Open the Site folder, and open the Servers folder, then expand the server object to get to the NTDS Settings. Right-click NTDS Settings, and choose Properties. Select the Global Catalog Server checkbox on the General tab.

Moving Server Objects between Sites

When a server is created, it becomes a member of the site in which it's installed. To move server objects between sites go to Start | Programs | Administrative Tools | AD Sites And Services. Open the Site folder, and open the Servers folder where the server is currently located. Right-click the server to be moved, and select Move. Select the site you want to move the server object to then click OK.

Operations Master Roles

AD uses multimaster replication of the directory to make all domain controllers equal. Some operations are impractical to perform in a multimaster environment. In a single-master model, only one DC in the entire directory is allowed to process updates. The Windows 2000 Active Directory has the ability to transfer roles to any domain controller (DC) in the enterprise. Because an Active Directory role is not bound to a single DC, it is referred to as operations masters roles. There are five operations masters roles:

Role	Description
Domain naming master	Forest-level master that controls adding/deleting of domains to the forest. Responsible for domain name uniqueness.
Infrastructure daemon	Domain-level master that maintains inter-domain consistency.
PDC emulator	Domain-level master that provides support for non-AD compatible clients. Handles the replication of data to Windows NT BDCs.
Relative Identifier (RID) pool operations master	Domain-level master that allocates relative IDs to domain controllers.
Schema master	Forest-level master responsible for write updates and changes to the schema.

Transferring Operations Master Roles
In transferring operations master roles, you are moving the role from one domain controller to another. This may occur when one of the domain controllers hosting the master role should fail. Depending on the role, you must transfer the role using one of three AD snap-ins:

Role	Snap-in
Domain naming master	Active Directory Domains And Trusts
Infrastructure daemon	Active Directory Users And Computers
PDC emulator	Active Directory Users And Computers
Relative Identifier pool operations master	Active Directory Users And Computers
Schema master	Active Directory Schema

Verifying Active Directory Installation
You can verify promotion of a server to a domain controller by checking for the following items after an upgrade:

Item	Description
Default containers	Created automatically when the first domain is created.
Default domain controllers OU	Contains the first domain controller.
Default-First-Site-Name	First site is automatically created when you install the first domain controller.
Directory services database	The file Ntds.dit is installed in the %systemroot%\ntds directory.
Global catalog server	First domain controller becomes a global catalog server by default.
Root domain	Forest root is created when the first domain controller is installed.
Shared system volume	Default location is %systemroot%\Sysvol directory. Exists on all Windows 2000 domain controllers.
SRV resource records	Check the Netlogon.dns file for the LDAP SRV entry.

Implementing an Organizational Unit Structure
OUs are AD containers into which users, groups, resources, and other OUs are placed. The objects must be members of the same domain as the OU. OUs allow you to assign separate sets of permissions over the objects in the OU, and allow you to delegate administrative rights to objects. To create OUs, go to Start | Programs | Administrative Tools | AD Users And Computers. Select the domain name or in another OU. Right-click it, then choose New from the Action menu then select Organizational Unit. Enter the name of the new OU, then click OK.

OU Properties:

Property	Description
General	Description, street address, city, state or province, zip or postal code, and country or region.
Managed By	OU manager's name, office location, street address, city, state or province, country or region, phone number, and fax number.
Group Policy	OU's group policy links.

Backing Up and Restoring Active Directory

The data in AD that is backed up is called System State data. It contains the Registry, system boot file, the AD database, the SYSVOL directory, and the COM+ Class Registration database. To use the Windows 2000 Backup utility to back up the System State data, you must be a member of the Administrators or the Backup Operators group.

Performing a Nonauthoritative Restore of Active Directory

By default, when restoring System State data to a domain controller, you are performing a nonauthoritative restore. All System State components that are older than the replicated components on the other domain controllers will be brought up to date by replication after the data is restored. If you do not want this information to be updated by replication, you must perform an Authoritative Restore. Nonauthoritative restore is used for restoring System State data on a local computer only. If you do not specify an alternate location for the restored data, Backup will erase your current System State data. Only the registry files, SYSVOL directory files, and system boot files are restored to the alternate location. The AD database, Certificate Services database, and COM+ are not restored when an alternate location is selected. To restore System State data, you must first start the system in safe mode.

Performing an Authoritative Restore of Active Directory

An authoritative restore is performed immediately after a nonauthoritative restore and designates the information that is authoritative. A value of 100,000 is added to the Property Version number of every object on the domain controller. This ensures the objects on this domain controller will overwrite the copies of these objects on other domain controllers. To perform an authoritative restore, perform the standard restore procedure, but do not allow the domain controller to reboot at the end of the procedure. Click No to bypass the restart option, then close Backup. From a command prompt, type Ntdsutil. From the Ntdsutil: prompt, type Authoritative Restore. Then type Restore Database.

Startup and Recovery Settings

The paging file must be on the system partition and the pagefile itself must be at least 1 MB larger than the amount of RAM installed for the Write debugging information option to work. Use dumpchk.exe to examine contents of memory.dmp. A small memory dump needs 64K of space. Found in %systemroot%\minidump. Memory dumps are saved with the filename memory.dmp. Startup and recovery settings are accessed through Control Panel | System. Choose the Advanced tab, Startup and Recovery.

DNS for Active Directory

Installing, Configuring and Troubleshooting DNS for Active Directory

Integrating Active Directory DNS Zones With Non-Active Directory DNS Zones

The Domain Name System (DNS) is the Active Directory locator in Windows 2000. Active Directory clients and client tools use DNS to locate domain controllers for administration and logon. You must have a DNS server installed and configured for Active Directory and the associated client software to function correctly. Non-Microsoft DNS servers can be used with AD if they support SRV records and dynamic updates. The DNS server in Windows NT Server 4.0 cannot be used with AD, but BIND versions 8.1.2 and later can. Active Directory Integrated DNS uses the directory for the storage and replication of DNS zone databases. If you use Active Directory Integrated DNS, DNS runs on one or more domain controllers and you do not need to set up a separate DNS replication topology.

Configuring Zones for Dynamic DNS (DDNS) Updates

Zones can be configured for dynamic updates. Resource records will then be updated by the DHCP clients and or server without administrator intervention. The Only Secure Updates option is only available in Active Directory integrated zones. To configure DDNS, from the DNS console, select the server you want to administer and then select Forward Lookup Zones. Right-click the domain name and choose Properties. Check the Allow Dynamic Updates box on the General tab. You must do the same for the Reverse Lookup Zones. Root or "." zones cannot be configured for dynamic updates.

Managing Replication of DNS Data

Zone Transfer is the duplication of data between DNS servers that do not participate in AD. Zone Replication is the replication of data between DNS servers (on domain controllers) that participate in AD. Zone Replication DNS servers poll AD every 15 minutes for updates. Zone Transfer uses DNS Notification. There are two zone transfer types, full zone transfer (AXFR) and incremental zone transfer (IXFR):

- AXFR*:* When the refresh interval expires on a secondary server it queries its primary using an AXFR query. If serial numbers have changed since the last copy, a new copy of the entire zone database is transferred to the secondary.
- IXFR: Uses serial numbers, but transfers only information that has changed. The server will only transfer the full database if the sum of the changes is larger than the entire zone, the client serial number is lower than the serial number of the old version of the zone on the server or the server responding to the IXFR request doesn't recognize that type of query.

Troubleshooting

Dcpromo creates an installation log during the installation procedure that records every step, including success or failures. The file created is Dcpromo.log, and is stored in the %systemroot%\Debug directory Dns.log can be enabled for debugging purposes. It is stored in the %systemroot%\system32\dns folder. All debugging options are disabled by default because they can be resource-intensive. Use nslookup to troubleshoot problems with DNS.

Change and Configuration Management

Implementing and Troubleshooting Group Policy

Group policies are collections of computer and user configuration settings that are linked to domains, sites, computers, and organizational units. When applied, a Group Policy affects all users and computers within a container. Group Policy settings define what controls, freedoms, or restrictions are placed over an OU. Group Policy Objects can contain seven types of settings:

Setting	Description
Administrative Templates	Defines application and desktop configurations via Registry controls.
Security	Controls access and security (account policies, lockout policies, audit policies, user rights, etc.)
Software Installation	Controls installation, update, and removal of software.
Scripts	Controls when Windows 2000 will execute specific scripts.
Remote Installation Services	Controls options when Client Installation Wizard is used by RIS.
Internet Explorer Maintenance	Manages and customizes Internet Explorer.
Folder Redirection	Defines folder redirection for user profile home directories and folders.

User configuration settings apply group policies to users, regardless of what computer they have logged on to. Settings are only applied at time of logon and removed when the user logs off. Computer configuration settings apply group policies to computers, regardless of what user logs on to them. Settings are applied when Windows initializes.

Creating a Group Policy Object (GPO)

A GPO is stored in two locations; a Group Policy template (GPT), and a Group Policy container (GPC). Local GPOs are created using the Group Policy snap-in for the MMC. Site GPOs are created by Start | Programs | Administrative Tools | AD Sites And Services. Right-click the Site folder, and choose Properties, Group Policy tab. Each Windows 2000 computer can have one local GPO. Local GPOs can have their settings overridden by non-local GPOs when used in conjunction with AD. In a peer-to-peer environment, local GPOs are not overwritten by non-local GPOs. Domain/OU GPOs are created by Start | Programs | Administrative Tools | AD Users And Computers. Right-click domain or OU, and choose Properties, Group Policy tab.

Linking an Existing GPO

GPOs are linked with a container. It's through the container that GPOs are applied to individual users and computers. GPOs cannot be tied directly to users or computers. A single GPO can be linked to multiple OUs, or multiple GPOs can be linked to a single OU. Only Domain Admins and Enterprise Admins have the ability to link GPOs to domains, OUs, or

sites. To link a GPO to an existing, domain or OU, use Administrative Tools | AD Users And Computers | Right-click domain or OU, and choose Properties, Group Policy tab. Click Add then choose the policy and click OK. To link a GPO to an existing, site use Administrative Tools | AD Sites And Services | Right-click domain or OU, and choose Properties, Group Policy tab. Click Add then choose the policy and click OK.

Delegating Administrative Control of Group Policy
Delegating a GPO to a user grants that user control over the GPO, not the container to which the GPO applies. GPO management delegation includes; GPO links to sites, domains and OUs, creating GPOs, and editing GPOs. The default permissions are:

Security Group	Default Settings
Authenticated users	Read, Apply Group Policy, Special Permissions
Creator Owner	Special Permissions
Domain Admins	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions
Enterprise Admins	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions
System	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions

Modifying Group Policy Inheritance
When multiple Group Polices apply to an object, the inheritance rules (order in which applied) of Group Policy apply. The order is Local GPO, Site GPO, Domain GPO, and OU GPO. Each previous GPO is overwritten by the next in line. When several GPOs are linked to a single OU, they are processed synchronously, in the order specified by the administrator.

Exceptions to Inheritance Order
Any site, domain or OU can block inheritance of group policy from above, except when an administrator has set No Override to the GPO link. No override can be set so that none of its policies will be overridden by a child container it is linked to. Loopback setting is used to merge or replace modes.

Filtering Group Policy Settings by Associating Security Groups to GPOs
By default, a GPO is applied to all members of its linked container. Filtering grants or restricts Read access to the GPO. If a user/group has Read access, the GPO can be applied; if not, it has been filtered. To apply the GPO to specific uses, modify the GPO's Access Control List (ACL). To prevent a GPO from applying to a listed group, remove the Allow setting for the Apply Group Policy setting from the Security tab. To prevent a GPO from applying to a specific user within a listed group, add the user to the list of names and then select the Deny setting for the Apply Group Policy setting.

Removing and Deleting GPOs
Deleting a GPO removes it from any sites, domains or OUs it was linked to. When a GPO link is removed, it is no longer applied, but still exists.

Managing and Troubleshooting User Environments by Using Group Policy
Group policies can be used to control the abilities of a user to perform tasks or access portions of the operating system or network. System Policies are a collection of user environment settings that are enforced by the operating system and cannot be modified by the user. User profiles refer to the environment settings that users can change. Environment control takes place via Administrative Templates. Administrative Templates control a system through editing or overwriting portions of the Registry.

Using Incremental Security Templates
Settings can be stored locally or in AD. They are secure and can only be changed by Administrators. Templates can be filtered using Active Directory. Settings are imported/exported using .INF files.

Incremental Security Templates for Windows 2000

Template	Filename	Description
Compatibility	compatws.inf compatsv.inf compatdc.inf	Sets up permissions for local users group to ensure viability of legacy programs.
Secure	securews.inf securesv.inf securedc.inf	Increases security settings for Account Policy and Auditing. Removes all members from Power Users group.
High Secure	hisecws.inf hisecsv.inf hisecdc.inf	For Workstations running in Windows 2000 native mode only. Requires all communications to be digitally signed and encrypted. Cannot communicate with downlevel Windows clients. Changes ACLs to give Power Users ability to create shares and change system time.

Assigning Script Policies to Users and Computers
Startup/shutdown scripts are assigned to computers. Logon/logoff scripts are assigned to users and run when a user logs on or off the system. When a system is shut down, Windows 2000 processes the logoff scripts then the shutdown scripts. Multiple scripts can be assigned to the same user or computer and Windows processes them using top-down logic.

Managing and Troubleshooting Software by Using Group Policy
Deploying Software by Using Group Policy
Group Policy integrates software installation into Windows 2000 in a feature known as Software Installation and Maintenance. Administrators can automate the process of

installing, upgrading, managing, and removing software from systems on the network. Windows Installer packages have a .MSI file extension.

Maintaining Software by Using Group Policy
Software packages are installed on a Windows 2000 Server in a shared directory. A Group Policy Object is created. Behavior filters are set in the GPO to determine who gets the software. The package is added to the GPO under User Configuration, Software Settings, Software Installation. Choose the publishing method, then choose OK. AD can either uninstall the old application first or upgrade over top of it. When publishing upgrades, they can be optional or mandatory for users but are mandatory when assigned to computers. When applications are no longer supported, they can be removed from software installation without having to be removed from the systems of users who are using them. They can continue using the software until they remove it themselves, but no one else will be able to install the software through the Start menu, Add/Remove Programs, or by invocation. Applications that are no longer used can have their removal forced by an administrator. Software assigned to the user is automatically removed the next time that user logs on. When software is assigned to a computer, it is automatically removed at start up. Users cannot re-install the software. Selecting the "Uninstall this application when it falls out of the scope of management" option forces the removal of the software when a GPO no longer applies.

Configuring Deployment Options
You can assign or publish software packages. Software that is published can be installed from the Control Panel, Add/Remove programs. Assigned software is installed the next time the user logs on regardless of whether or not they run it.

When software is assigned to a user, the new program is advertised when a user logs on, but is not installed until the user starts the application. Software assigned to a computer is installed automatically. A local administrator can only remove software when it is assigned to a computer. Users can repair software assigned to computers, but not remove it.

Published applications are not advertised. Applications can only be published to users, not computers. They are only installed through Add/Remove Programs or through invocation. Published applications do not self-repair or re-install if deleted.

With invocation, when a user launches an unknown file type, the client computer queries Active Directory to see what is associated with the file extension. If an application is registered, AD checks to see if it has been published to the user. If it has, it checks for the auto-install permission. If all conditions are met, the application is installed.

Non-MSI programs are published as .ZAP files. .ZAP files can only be published, not assigned.

Managing Network Configuration by Using Group Policy
Used with roaming profiles to redirect folders to a central server to prevent files from being copied back and forth from the server to the workstation every time the user logs on and off.

Data that is centrally stored on a network server can be backed up regularly and does not require action on the part of the user. Use Group Policy to set disk quotas, limiting the amount of space used by special folders.

Deploying Windows 2000 Using Remote Installation Services

Deploying Windows 2000 Using Remote Installation Services (RIS)
Remote Installation Services allows you to support the installation of Windows 2000 Professional (only) onto network clients that don't have an operating system installed. A destination client can be a system with only a DHCP Preboot Execution Environment-based (PXE-based) remote boot ROM NIC, or a RIS boot disk. RIS can initiate a typical network share type of installation or use a system image transfer type of installation. A RIS Server requires DHCP Server Service, Active Directory, DNS Server Service and at least 2 GB of disk space. Hard disk must have at least two partitions, one for the Operating System and one for the images. The image partition must be formatted with NTFS. RIS packages cannot be installed on either the system or boot partitions.

Setting Up a RIS Server
Setup Wizard creates the folder structure, copies needed source files to the server, creates the initial CD-based Windows 2000 Professional image in its designated folder along with the default answer file (Ristandard.sif), and starts the RIS services on the server. To authorize the server, open Administrative Tools, DHCP. Right-click DHCP in the console tree and choose Manage authorized servers. Click Authorize and enter name or IP of the RIS server. Assign users/groups that will be performing RIS installations permissions to Create Computer Objects in Active Directory. The Client Computer Naming Format is defined through Active Directory Users And Computers. Right-click the RIS Server and click Properties, Remote Install, Advanced Settings, New Clients. Choose a pre-defined format or create a custom one. Associate an answer file (.SIF) with your image.

Install Remote Installation Services using Control Panel | Add/Remove Programs | Windows Components. Start the RIS Setup Wizard by running Risetup. Specify the Remote Installation Folder Location. For Initial Settings, choose Do not respond to any client requests. Specify the location of the Windows 2000 Professional source files for building the initial CD-based image. Designate a folder inside the RIS folder where the CD image will be stored. Provide a text name for the CD-based image.

Creating A RIPrep Image
Install Windows 2000 Professional on a source computer. Configure all components and settings for the desired client configuration. Install and configure applications. Copy the configuration to the Default User profile. To launch the RIPrep Wizard, click Start, Run and enter: *RISServerName*\reminst\admin\i386\riprep.exe. Provide the name of the RIS Server where the image will be stored.

Installing an Image on a RIS client

Custom RIS images can be built using the RIPrep tool. It creates an installation image from a preinstalled and configured system. You can use Remote Installation Services (RIS) for Windows 2000 to install a local copy of the OS throughout the organization from remote locations. Using existing network technologies, after booting, personal computers contact a Dynamic Host Configuration Protocol (DHCP) server for an Internet Protocol (IP) address, and then contact a boot server to install the OS. Using RIS, you can send personal computers directly to an end user or staging area and install an automated, customized version of Windows 2000. The client initiates the protocol by broadcasting a DHCP Discover packet containing an extension that identifies the request as coming from a client that implements the PXE protocol. The boot server sends an offer containing the IP address of the server that will service the client. The client uses TFTP to download the executable file from the boot server. The client then initiates execution of the downloaded image.

Creating A RIS Boot Disk

If the destination desktop does not have PXE-based remote-boot ROM on its NIC, you must create a boot disk to initiate the remote installation. The boot disk creates a PXE emulator that works on supported PCI network adapters that allow them to connect to the RIS server. Since one disk works for all network adapters, a specific network boot disk is no longer required. The supported network adapters are listed in the utility that creates the boot disk. This utility is named Rbfg.exe and can be found in the network folder: \reminst\admin\i386.

Configuring Remote Installation Options

Once installed, the RIS system can be re-created and altered via the RIS host's Properties dialog box from the Active Directory Users And Computers tool. RIS can be configured to respond to clients requesting server, to respond only to authorized and known clients, to verify that the server is properly configured, and to view the current RIS clients.

Troubleshooting Remote Installations

Error	Solution
Computer displays a BootP message but doesn't display the DHCP message.	Make sure the RIS server is online and authorized and that DHCP packets are being routed.
Computer displays the DHCP message but does not display the Boot Information Negotiations Layer (BINL) message.	Make sure the RIS server is online and authorized and that DHCP packets are being routed.
BINL message is displayed but system is unable to connect to RIS server.	Restart the NetPC Boot Service Manager (BINLSVC) on the RIS Server.
Client cannot connect to RIS Server using the Startup disk.	Check network adapter driver in rbfg.exe.
Installation options are not available.	Possible Group Policy conflicts. Check to make sure another Group Policy Object is not taking precedence.

Managing Images for Performing Remote Installations
You can customize existing CD-based installs by modifying the associated answer file (*.SIF). For RIPrep images, the files are stored as individual source files. If modifications need to be made to the RIPrep image, apply the existing image to a client, make any required changes, and rerun the RIPrep wizard from the RIS server Admin folder to upload the new, updated image to the RIS server. You can still modify the *.SIF file associated with a RIPrep-based install, but you'll only be able to modify options that can be configured via the answer file. The RIPrep answer file, named RISETUP.SIF by default, will be located under the I386\Templates subfolder of the folder created for the RIPrep image.

Managing, Monitoring, and Optimizing the Components of Active Directory

Managing Active Directory Objects
Moving Active Directory Objects within a Domain
Objects can be moved within a domain using the AD Users And Computers console. Permissions that have been assigned directly to an object will not change when it is moved. Objects without permissions inherit the permissions of the parent container they are moved to.

Moving Active Directory Objects between Domains
An OU can be moved from one domain to another without damaging any of its GPOs. The GPO link is automatically updated. Use the Movetree command-line utility to move objects between domains. Use the Netdom command-line utility to move workstations or member servers between domains. When objects are moved their GUID remains unchanged but they receive a new SID. User objects that contain any other objects cannot be moved.

Resource Publishing in Active Directory
Publishing a resource refers to the process of creating an object in the directory that either contains the information you want to make available or that provides a reference to the object. General information is automatically published for all network users while account security information is only available to select administrator groups. Printers must be installed before they are added to AD. Use Administrative Tools, AD Users And Computers, domain node to find the container you want to add the printer to. Right-click the container and choose New, Printer. When the New Object-Printer dialog appears, type the UNC name of the printer in the Network Path box then click OK. Shared folders are published using Administrative Tools, AD Users And Computers, domain node. Right-click the container you want to add the shared folder to and choose New, Shared Folder. Enter the name of the folder in the Name box and the UNC name that you want to publish in AD in the Network Path box.

Locating Objects in Active Directory

Object	Description
Computer	Information on a computer that belongs to the domain.
Contact	A person connected to the organization. Includes phone number, e-mail, address, home page, etc.
Domain Controllers	Information on domain controllers including their DNS name,

	NetBIOS name, OS version, location, manager, etc.
Group	Collections of users, groups, or computers used to simplify administration.
OU	Container used to organize AD objects including other OUs.
Printer	Pointer to a printer. Windows 2000 automatically adds printers created on domain computers to AD.
Shared Folder	Pointer to a shared folder on a computer.

Using the Find Tool

Administrators can search AD via an LDAP query against the global catalog. To find objects in AD use Administrative Tools | AD Users And Computers. Right-click a domain or container in the console tree and select Find. Users can access directory objects via the search command from the Start menu, through My Network Places, or via the Find command from the AD Users And Computers snap-in. Users can search for computers, shared folders, printers, and users.

Creating and Managing Accounts Manually or by Scripting

Account	**Description**
Local accounts	Created in the local computer's Security Accounts Manager (SAM) database. Local accounts are not recognized by Active Directory. Added through Administrative Tools, Local Users and Groups.
Domain user accounts	Used by users to logon to the domain to gain access to network resources. Receive an access token from AD at logon that is checked against ACLs when accessing objects. Added through Administrative Tools, AD Users And Computers.
Built-in user accounts	Administrator and Guest.
Local user profile	Created on a computer the first time a user logs on. Stored on the local hard drive.
Roaming user profile	Created by system administrator. Stored on a server. Available from any computer on the network. Changes are saved to the profile on the remote server.
Mandatory user profile	Created by system administrator. Only administrators can change mandatory profiles.

Accounts should only be deleted when they will no longer needed. Renaming an account retains all rights, permissions and group memberships and assigns them to a different user. Disable accounts when they are not going to be needed for an extended period but may be needed again.

Creating and Managing Groups

Security groups are used to assign permissions for accessing objects in AD. Distribution groups are used for non-security related functions, and can only be accessed by AD-aware programs such as Exchange Server 2000. Accounts go into global groups which then go into

local groups that are assigned permissions to a resource. Global groups can only contain members from the domain in which the group was created. Use global groups to assign permissions for gaining access to resources located in any domain in the tree or forest. They contain other global groups when running in native mode. Domain Local groups can contain members from any domain. They only access resources in the domain where the group was created. They contain global groups, and should not be used to assign permissions to AD objects. Universal groups can include members from any domain. They contain other global and universal groups. Putting users in universal groups affects logon performance. Universal groups are not available in mixed-mode. Objects with identical security requirements should be placed into OUs. All objects inside the OU will inherit the same permissions.

Controlling Access to Active Directory Objects

The Access Control List (ACL) is a list of user access permissions for every AD object. Permissions can be used to assign administrative privileges to users, groups, OUs, or any other object without giving control over other AD objects. Permissions are cumulative, except for Deny. A user with read access to an object in one group and write access to the same object in another group would have a cumulative access of read and write. The exception to this is deny, which overrides all other permissions.

Standard permissions include:

Permission	Description
Read	Can view objects and their attributes, the owner of the object and AD permissions.
Write	Modify attributes of object.
Full Control	Change all permissions and take ownership.
Create All Child Objects	Can add any type of child object to an OU.
Delete All Child Objects	Can delete any type of object from an OU.

Delegating Administrative Control of Objects in Active Directory

Permissions flow from the parent container to the child container unless inheritance has been prevented. Delegations should be accomplished using the Delegation of Control Wizard. Options include:

Option	Description
AD Object Type	Selects scope for tasks being delegated: This folder, Existing Objects In This Folder, and Creation of Objects In This Folder, or Only The Following Objects In This Folder.
Permissions	General is the most common. Property Specific includes permissions that can be assigned to the attributes of the object. Creation/Deletion of Specific Child Objects is the ability to create and delete child objects.
Tasks to Delegate	Select tasks from a list or create custom tasks you want to delegate.

Users or Groups	Select the users/groups you want to delegate control to.

Managing Active Directory performance

Domain Controller Performance

Performance Console:

Object	Description
Cache	File system cache used to buffer physical device data.
diskperf	Command for activating disk counters. Is not supported in Windows 2000.
Logical disk - Disk Queue Length	If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set.
Logicaldisk	Logical drives, stripe sets and spanned volumes.
Memory	Physical and virtual/paged memory on system.
Memory - Committed bytes	Should be less than amount of RAM in computer.
Memory - Pages/sec	Add more RAM if more than 20 pages per second.
Physical disk - % Disk Time	If above 90%, move data/pagefile to another drive or upgrade drive.
Physical disk - Disk Queue Length	If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set.
Physicaldisk	Monitors hard disk as a whole.
Processor	Monitors CPU load.
Processor - % CPU DPC Time	Measures software interrupts.
Processor - % CPU Interrupts/Sec	Measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check driver.
Processor - % Processor Time	Measures time CPU spends executing a non-idle thread. If continually at or above 80%, upgrade CPU.
Processor - Processor Queue Length	More than 2 threads in queue indicates CPU is a bottleneck for system performance

Performance Alerts and Logs

By default, log files are stored in the \Perflogs folder in the system's boot partition. Log types include Alert logs, Counter logs, and Trace logs. Alert logs log an event, send a message or run a program when a user-defined threshold has been exceeded. Counter logs record data from local/remote systems on hardware usage and system service activity. Trace logs are event driven and record monitored data such as disk I/O or page faults.

Troubleshooting Active Directory Components

Problem	Solution
Cannot add/remove domain.	Domain Naming Master is not available. Network problem or failure of computer holding the master role.

	Seize the role to another system.
Cannot create objects in AD.	Relative ID master is not available due to failure of the computer holding master role or a network problem. If the network problem or the computer holding the master role cannot be repaired, seize the role to another system.
Cannot modify the schema.	Schema master is not available due to failure of computer holding master role or network problem. If problem cannot be resolved, seize the role to another computer.
Clients cannot access resources in a different domain.	Trusts may have failed between domains. Reset and verify trusts.
Clients without AD client software cannot logon.	PDC emulator not available possibly caused by network problem or failure of system holding master role. If problem cannot be resolved, seize the role to another system.

Managing and Troubleshooting Active Directory Replication

Managing Intersite Replication

Replication takes place for domain controllers between sites (intersite replication) based upon a schedule, the amount of network traffic, and costs. The replication schedule, defined by site link and connection objects, is used to define the time that replication is allowed to occur. The replication interval is used to define how often replication should occur during a "window of opportunity" based on the schedule. Bridgehead servers are computers with additional hardware or network capacity that are specified as preferred recipients for intersite replication. The bridgehead server subsequently replicates its AD information to its replication partners. Using bridgehead servers improves replication performance between sites. When using a firewall proxy server, you must establish it as a bridgehead server and allow it to replicate AD information to other domain controllers outside the firewall.

Managing Intrasite Replication

Replication takes place between domain controllers within a site (intrasite replication) as needed without regard to cost or schedules. Domain controllers in the same site replicate using notification. When one domain controller has changes, it notifies its partners. The partners then request the changes and the replication occurs.

Urgent replication triggers:

Events replicated immediately in native-mode domains:

- changing an LSA secret
- newly locked-out account
- RID manager state changes

Events replicated immediately in mixed-mode domains:

- changes to account lockout policy
- changes to domain password policy

- changing an LSA secret
- changing the password on a machine account
- inter-domain trust password changes
- newly locked-out account
- RID manager state changes

Active Directory Security Solutions

Configuring and Troubleshooting Security in a Directory Services Infrastructure
Applying Security Policies by Using Group Policy
You must have the Manage Auditing and Security Log user right on the system where you need to implement an audit policy or review the audit log. Used to track success/failure of events like logon attempts, accesses to a specific file, modifications to a user account, group memberships, and security setting modifications. Audited events are written to the Event Viewer.

Security Configuration and Analysis and Security Templates
The security database (mysecuresv.mdb) is compared to an incremental template (hisecsv.inf) and the results displayed in the right pane. The log of the analysis will be placed in %systemroot%\security\logs\mysecure.log.

Implementing an Audit Policy
Type secedit /refreshpolicy machine_policy at a command prompt to start policy propagation. By default policy propagation takes place every 8 hours.

Auditable Events:

Event	Description
Account logon events	A domain controller received a request to validate a user account.
Account management	An administrator created, changed, or deleted a user account or group. A user account was renamed, disabled, or enabled, or a password was set or changed.
Directory service access	A user gained access to an Active Directory object. Configure specific Active Directory objects for auditing to log this type of event.
Logon events	A user logged on or logged off, or a user made or canceled a network connection to the computer.
Object access	A user gained access to a file, folder, or printer. Configure specific files, folders, or printers for auditing. Directory service access is auditing a user's access to specific Active Directory objects. Object access is auditing a user's access to files, folders, and printers.
Policy change	A change was made to the user security options, user rights, or audit policies.

Privilege use	A user exercised a right, such as changing the system time.
Process tracking	A program performed an action.
System	A user restarted or shut down the computer, or an event occurred that affects Windows 2000 security or the security log.

Monitoring and Analyzing Security Events

Logs are accessed through Administrative Tools, Event Viewer. Logs include the Application log which contains errors, warnings, or information generated by programs running under Windows, the System log which contains errors, warnings, or information generated by Windows 2000, and the Security log which contains information about success/failure of audited events. The Event Viewer contains entries of events related to the operation of the operating system and various applications. A Windows 2000 domain controller has six logs available. These include:

Log	Description
Application log	Contains events generated by application programs. Contain errors, warnings, informational events, and events generated by the Alert log.
Directory Service	Contains events relating to the operation of AD.
DNS Server	Contains events relating to the operation of the DNS server.
File Replication Service	Contains errors and events that occur when domain controllers are updating.
Security Log	Contains information on security events, such as logon attempts and accessed resources.
System Log	Contains events generated by Windows 2000 components, drivers, and services.

Implementing and Administering a Microsoft Windows 2000 Network Infrastructure Practice Questions

1. **All users in your Support OU use an application named LocatorID. The LocatorID application was deployed using a GPO named Locator App, which was configured to publish the LocatorID application to the Support OU by using the Windows Installer package. Only users in the Support OU can start the LocatorID application. What should you do to ensure all users in the domain can install the locator application by using the Start menu shortcut?**

   A: Remove the Locator App GPO link to the Support OU.
   Assign the Locator App GPO to the domain.
   Change the configuration of the Locator App GPO to assign the LocatorID application to users.

2. **You are using Microsoft Systems Management Server to install applications on all of your client computers. A custom configuration is required for each of them. What do you need to do to use RIS to install Windows 2000 on all the client computers?**

   A: Create a CD-based RIS image and different answer files for each custom configuration.

3. **You are deploying an application named Accounting that will be used by all users in your domain. You have been given a Windows Installer package for the installation. During the initial deployment, only members of a security group named Accounting Pilot will use the application. In the second half of the deployment, all users in the domain will install and use the application. You want to accomplish the following Phase 1 goals:**
   - **Only members of the Accounting Pilot group will be able to install the application using a Start menu shortcut – no other users can.**
   - **The application will not be automatically installed when users log on.**
   - **After Phase 1, the application will be installed automatically the first time any user logs on.**

   You take the following actions:
   - **Create a GPO named Deploy Accounting and link the Deploy Accounting GPO to the domain.**
   - **Configure the Deploy Accounting GPO to assign the Accounting application to users.**
   - **For Phase 1, create a software category named Accounting Pilot. Assign the Accounting application to it.**
   - **For Phase 2, remove the Accounting application from the Accounting Pilot software category.**

Which results do these actions produce? (Choose all that apply)

A: During Phase 1, the Accounting application is not installed automatically when users log on.
During Phase 1, users who are members of the Accounting Pilot group can install the Accounting application by using a Start menu shortcut.

4. What actions should you audit to identify users who have been deleting files from your server? (Choose two)

A: Directory services access.
Process tracking.

5. Users in your Boston domain use different Windows 2000 Professional computers. You want to accomplish the following goals:

- **Changes made to the desktop settings will not be saved when users log off.**
- **All users in the domain will be able to work on all Windows 2000 Professional computers and have their own predefined desktop settings available.**
- **Users can make changes to their desktop settings.**

What should you do?

A: Configure a roaming profile for each user in the domain. Use \\Boston\Profiles\%Username% as the profile path. On the Boston server, rename the Ntuser.dat file to Ntuser.man for each user.

6. All users in your domain are members of the Power Users group, and use Windows 2000 Professional computers. Randy has dial-up access to the Internet. You do not want other users to share Randy's Internet connection. What should you do?

A: Create a GPO that disables the configuration of connection-sharing. Grant Randy Read and Apply Group Policy permissions to the GPO.

7. You have a single top-level OU named HQ, and five child OUs named after your company's internal departments, Sales, Marketing, Accounting, Shipping and Support. Users in the first four departments require the same desktop settings. Users in the Support OU require a less restrictive setting. You want to accomplish the following goals:

- **Group Policy will be automatically applied when new child OUs are added to the domain.**
- **Group Policy from the HQ OU will not be applied to the Support OU.**
- **All assigned Group Policy settings in the HQ OU will be applied to all users and computers in the Sales, Marketing, Accounting and Shipping OUs.**
- **Users should not be able to change their Group Policy settings.**

- **Administrators in the Support OU will be able to change the Group Policy settings.**

You take the following actions:

- **Create and configure the GPO, and link the GPO to the HQ OU.**
- **Select No Override in Group Policy Options for the HQ OU.**
- **For the Support OU, select Block Policy inheritance in the Group Policy dialog box.**
- **Assign the Authenticated Users group Full Control permission to the GPO.**

Which results do these actions produce? (Choose all that apply)

A: All assigned Group Policy settings in the HQ OU are applied to all users and computers in the Sales, Marketing, Accounting and Shipping OUs.
Group Policy from the HQ OU is not be applied to the Support OU.
Administrators in the Support OU are able to change the Group Policy settings.
Group Policy is automatically applied when new child OUs are added to the domain.

8. You have RIS installed on your Windows 2000 domain server. You want to use RIS to install new client computers. When you start a test client computer, the Client Installation Wizard does not appear. Your network adapter cards are not PXE compliant. What should you do to connect to the RIS server?

A: Run Rbfg.exe to create a RIS boot disk.

9. You want to standardize the Start menu for users in your Main OU. Some members of the Domain Admins group are in the Main OU. Folders and shortcuts are on the network at \\Srv1\Menu. The Everyone group has Change permissions on the Menu share. You want to accomplish the following goals:

- **Each user who is not a member of the Main OU will have a separate Start Menu that they can change.**
- **Users who use the \\Srv1\Menu Start menu will not be able to change the contents of the Start menu.**
- **Each Domain Admin member should have a separate Start menu that they can change.**
- **All users except Domain Admin members will use the \\Srv1\Menu Start menu.**

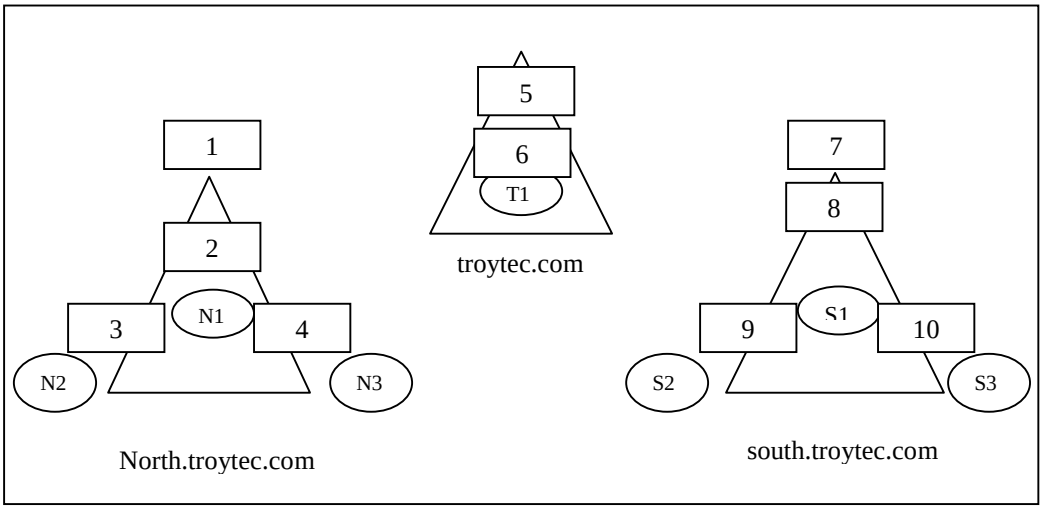
You take the following actions:

- **Create a GPO named Menu. Assign the Menu GPO to the Main OU.**
- **Configure the Menu GPO to redirect the Start menu folder for the Domain Users group to \\Srv2\Menu.**
- **Change the permissions on the Menu GPO to deny Apply Group Policy permission to the Domain Admins group.**

Which results do these actions produce? (Choose all that apply)

A: Each Domain Admin member has a separate Start menu that they can change.
All users except Domain Admin members use the \\Srv1\Menu Start menu.
Users who use the \\Srv1\Menu Start menu are not able to change the contents of the Start menu.
Each user who is not a member of the Main OU has a separate Start Menu that they can change.

10. Your network has three domains named troytec.com, north.troytec.com, and south.troytec.com. All are in a site named Sacramento, and contain OUs. You are implementing a new desktop policy for all users on the network in a GPO named Troydesktop. You are also implementing a logon script, which in configured in a GPO named Troyscript, for users from the N2 OU. Users in the N2 OU always log on to Windows 2000 Professional computers defined in the N3 OU. You do not want Group Policy filtering. What should you do to have the fewest GPO assignments possible? (Drag and drop each GPO only once)



A: Drag Troydesktop to position number 6, and drag Troyscript to position number 2.

11. You have four RIS servers in two segments. RIS server 1 and 2 are in segment A, and RIS server 3 and 4 are in segment B. The segments are linked by a router. Each segment has approximately the same number of Windows 2000 Professional clients. Using RIS, you deploy Windows 2000 Professional on 100 computers. RIS servers 1 and 3 are responding slowly, and are overworked. What should you do for a more consistent performance?

A: Create prestaged computer accounts for all the computers. Specify which RIS server will control each computer.

12. You have a script file that changes settings to users' desktops in the current user profile. It is deployed as a logon script for all users in the domain. What should you do to ensure that each user's desktop only appears after the script file completes its work?

A: Create a new GPO.
Assign the GPO to the domain.
Add the script to the GPO as a logon script.
Configure the GPO to run logon scripts synchronously.

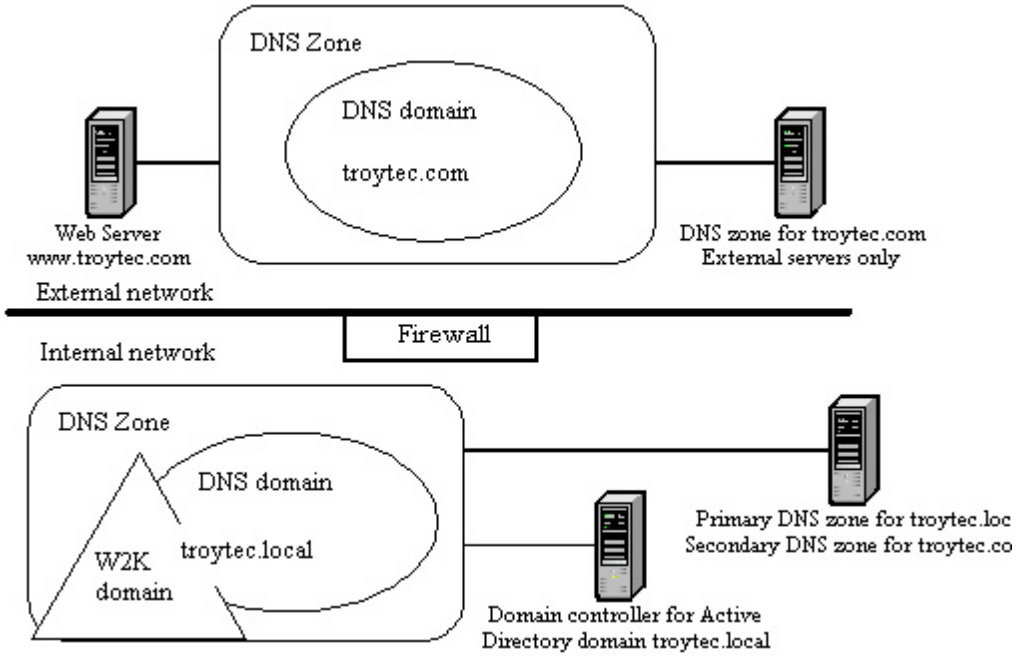
13. You want to use a GPO to assign a logon script to users in your Sales OU. What should you do?

A: Create a new GPO named Script and assign the Script GPO to the Sales OU.
Copy the logon script to the folder that is shared as Netlogon on the PDC emulator.
Add the script as a logon script to the Script GPO.

14. You are designing a Windows 2000 domain. Your company owns troytec.com, a registered domain name. The existing DNS zone is hosted on Windows NT 4.0 servers. You want to accomplish the following goals:

- **The existing DNS servers will not be upgraded.**
- **Internal users will resolve external names for access to Internet resources.**
- **Internal host names will not be exposed to the Internet.**
- **Depth of domain names and complexity for Active Directory will be minimized.**

You design a DNS implementation as shown:



Which results do these actions produce? (Choose all that apply)

A: Internal host names are not exposed to the Internet.
Internal users resolve external names for access to Internet resources.
Depth of domain names and complexity for Active Directory are minimized.

15. Your network consists of two segments connected by a router. Segment A contains downlevel client computers and a server serving as a DHCP relay. Segment B's client computers are all Windows 2000 Professional computers. All client computers in the network use DHCP. Segment B also contains a server serving as a domain controller and DNS server, a server serving as a DHCP server, and a server serving as a DNS server. Several days after you share some resources on client computers on Segment A, you are unable to resolve the host names of client computers when you attempt to connect to those resources from computers on Segment B. What should you do?

A: On the DHCP server in segment B, enable updates for DNS clients that do not support dynamic updates.

16. Server1 in your Windows 2000 network is configured with the primary zone for troytec.com. A DNS server in Boston and in Tampa are configured with secondary zones for troytec.com. You discover an error in several host records that prevents clients in Tampa from accessing shared resources. You make the necessary corrections on Server1. You want these changes to be propagated to Tampa immediately. What should you do?

A: On the DNS server in Tampa, perform the Transfer from master action for the troytec.com zone.

17. You are configuring DNS throughout your Windows 2000 domain which spans multiple subnets. You want to accomplish the following goals:

- **Zone transfer information will be secure.**
- **Administrative overhead for DNS zone files is minimized.**
- **DNS zone transfer traffic is minimized.**
- **Unauthorized host computers will not have records created in the zone.**
- **Zone updates will come only from authorized DNS servers.**

You take the following actions:

- **Create an Active Directory integrated zone.**
- **Set Allow Dynamic Updates to Yes.**
- **Enter the names and addresses of all DNS server on the network in the Name Servers tab of the Zone Properties dialog box.**

Which results do these actions produce? (Choose all that apply)

A: DNS zone transfer traffic is minimized.

Administrative overhead for DNS zone files is minimized.

18. **Your network has four servers located in two cities. Server1 and Server2 are in Boston, and Server3 and Server4 are in Dallas. You install Server2 and Server4 as domain controllers, and Server1 and Server3 as DNS servers for troytec.com. Each server has a standard primary zone named troytec.com, and the domain runs in native mode. When you attempt to contact Server4 by name from Server2, you cannot connect. But, you can ping Server2 and Server4 from any computer in either site. You want information to be regularly updated. What should you do to be able to resolve names of servers in both sites?**

    A: Re-create the troytec.com zone on Server3 as a secondary zone. Configure Server3 to replicate DNS data from Server1.

19. **A user's account has been deleted. You have been auditing all objects in Active Directory since the domain was created. You are not able to find a record of the deletion. What should you do to identify the person who deleted the account?**

    A: Search the security event logs on each domain controller for account management events.

20. **You have edited the Default Domain Controllers Group Policy to require passwords to be at least ten characters long. But, users are still able to create passwords with less than ten characters. What should you do?**

    A: Edit the Default Domain Group Policy to require passwords to be at least ten characters long.

21. **You want to implement a stricter network security policy that requires encrypted TCP/IP communication. What should you do?**

    A: Create a GPO for the domain, and configure it to assign the Secure Server IPSec Policy.

22. **You want to configure security auditing on your servers to monitor access to specific folders. When the security logs become full, you want to prevent users from gaining access to these servers. What should you do?**

    A: Create a GPO that applies to the servers. Configure the GPO to enable auditing for object access. Set up the individual objects to be audited in Windows Explorer. Configure the security event log so that it does not overwrite events. Configure the GPO to enable the Shut down the system immediately if unable to log security audits setting.

23. **You implement a security policy to be in effect at all times on all clients in your network. Administrators periodically change security settings on computers when they are troubleshooting. How can you automate the security analysis and configuration of**

client computers so that you can track changes to the security policy and reapply the original security policy when it is changed?

A: Schedule the secedit command to run on the client computers.

24. You want to use a custom built security template on five domain controllers in your domain. What should you do? (Choose two)

A: Import the custom-built template file.
Create a GPO on the Domain Controllers OU.

25. Using the least amount of administrative effort, how can you duplicate security settings from one domain controller to four other domain controllers?

A: Create a GPO for the Domain Controllers OU. Configure the GPO settings to match the settings of the secured domain controller.

26. Your domain has four OUs. In an effort to centralize security policy in your domain, you create three security template and GPOs:

- **SecPol1 defines Password, Audit and User Rights policies.**
- **SecPol2 defines User Desktop policy, File System security, and Registry security.**
- **SecPol3 defines a High Security User Desktop policy for network administrators.**

You want the GPOs to apply the security policies to users and computers in the domain with the fewest assignments possible. You want Group Policy to apply at the OU level for more granular administrative control. What should you do? (Select and Place)

A: Drag SecPol1 to all locations.

27. The volume that contains the Active Directory database file on Server1 is running out of disk space. What should you do to move the database file to an empty volume on a different disk on Server1?

A: Restart Server1 in directory services restore mode. Use Ntdsutil to move the database file to the empty volume.

28. Your network consists of two domains and six sites. Site A and Site C are connected by a T1 line. Site A and Site B are connected by a T1 line. Site C and Site F are connected by a T1 line. Site B and Site D utilize a 56 Kbps connection. Site C and Site E utilize a 128 Kbps connection. Each site has one or more domain controllers. One domain controller in each site is configured as a global catalog server. Network performance and data transfer for an application located in Site A are extremely poor. What should you do to improve performance?

A: Create site links between all sites and set less frequent replication schedules.

29. Your domain contains three domain controllers. DC1 does not hold any operations master roles. You backed up the System State data of DC1 two weeks ago. The hard drive on DC1 fails. You want to replace DC1 with a new computer that you've installed Windows 2000 Server on. What should you do next?

A: Use the Active Directory Installation wizard to make the new computer a replica in the domain.

30. One of your administrators has deleted an empty OU named Remote1 from ServerA. Before the deletion is replicated to ServerB, another administrator moves users into Remote1 from ServerB. What should you do to reinstate the configuration where users are moved into Remote1?

A: At ServerB, create a new Remote1 OU. Move the users from the LostAndFound container to the new Remote1 OU.

31. Your domain has three domain controllers name DC1, DC2, and DC3. You want to replace DC1 with a newer computer named DC4. DC4 should be a domain controller in the domain, and DC1 should no longer function as a domain controller. What should you do?

A: Install DC4 as a member server in the domain.
On DC4, use the Active Directory Installation wizard to install Active Directory on DC4.
On DC1, use the Active Directory Installation wizard to remove Active Directory from DC1.

32. Your Windows 2000 Server servers as a domain controller and a DNS server. When Windows 2000 Professional clients attempt to log on, they receive an error message that the domain controller cannot be located. Active Directory is installed and functioning. What should you do?

A: Check DNS for the addition of an appropriate SRV (service) record in the zone.

33. You want to create an Active Directory structure to allow local administrators at branch offices to control users and local resources. They should be prevented from controlling resources in branch offices other than their own. What should you do?

A: Create a child OU for each office. Delegate control of each OU to the local administrators at each office.

34. You want to create an Active Directory structure to allow local administrators at each branch office to be able to only control their own local resources. Only administrators from the main office should be allowed to create and manage user accounts. What should you do?

A: Create a single domain. Create an OU for each branch office and an additional OU named MainUsers. Delegate authority for resource administration to the local administrators for their own OUs. Delegate authority to the MainUsers OU only to the Domain Admins group.

35. You manage a multi-domain Windows 2000 network for two companies; Troytec and Support Systems. Each of the six departments has an OU in Active Directory. Each domain and OU has specific Group Policy settings that must be applied to all of its members. Some users have moved to different departments, and some have changed domains. You want to accomplish the following goals:

- **No user access disruption.**
- **Place user accounts in the appropriate domains.**
- **Apply existing policies for each domain or OU to the moved accounts.**

What should you do?

A: Use the Movetree utility for the users moving between domains. For users moving between OUs in the same domain, select the accounts, then from the Action menu, choose Move.

36. Your single domain contains three sites with two domain controllers each. You have two IP site links: Boston_Chicago, and Salem_Chicago. You want to add another domain controller in each site to handle all replication from each site. What should you do?

A: Configure each new domain controller to be the IP preferred bridgehead server for its site.

37. You hire a LAN administrator for your Salem office. Your network consists of one domain. Each office has its own OU. The new LAN administrator needs to be able to create child OUs under only ou=Salem,dc=troytec,dc=com and verify the existence of the created OUs. What permissions should you assign the LAN administrator? (Choose three)

A: List Contents
Create OU Objects
Read

38. Your network has three native mode domains: troytec.com, sales.troytec.com, and support.troytec.com. You want to remove sales.troytec.com. How should you move the sales.troytec.com users at the same time to troytec.com?

A: At the command prompt, type:
Movetree /start /s dc1.sales.troytec.com /d dc1.troytec.com /sdn

cn=users,dc=sales,dc=troytec,dc=com /ddn cn=users,dc=troytec,dc=com

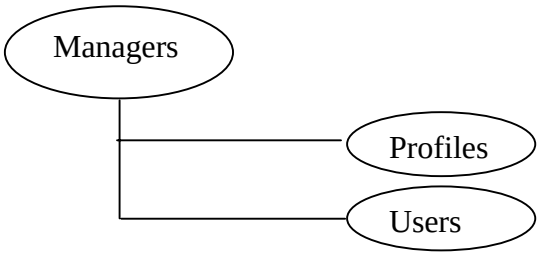
39. Your Ntds.dit file remains the same size over the course of a year, even though you have deleted numerous objects. How do you reduce the size of the Ntds.dit file? (Choose two)

A: Restart the server in directory services restore mode.
Use the Ntdsutil utility to compress the database to another drive.

40. All five of your domains run in native mode. Each domain has at least one Support personnel member. Each domain has a global group named Support Members that contains the Support personnel from each domain. You want all the Support staff to be able to reset passwords in an OU named Accountants. What should you do?

A: In the root domain create a new universal security group named Support Staff.
Place the five Support Members groups in the Support Staff group.
In the root domain create a new local security group named Reset Accountants. Place the Support Staff in this new local security group.
On the Accountants OU, assign the Reset Password permission to the Reset Accountants group.

41. Your OU structure is as follows:



You grant Create User Objects permissions to Lane for the Managers OU, but he is unable to create users objects in the Users OU. Lane is able to create users objects in the Profiles OU. What should you do?

A: In the Users OU, select Allow inheritable permissions from parent to propagate to this object.

42. You recently added three new SCSI hard disk drives to your domain controller which already had two physicals disks. The SCSI disks are configured in a RAID-5 array. How should you optimize the speed of the Active Directory database? (Choose two)

A: Move the Ntds.dit file to the RAID-5 array.
Move the log files to a separate physical disk from the operating system.

43. You enable a new domain controller name G1 as a global catalog. It will take the place of your existing G0 global catalog server. You want to use G0 only as a domain controller, and increase its disk space. What should you do? (Choose all that apply)

A: Use Active Directory Sites and Services.
Select the NTDS Setting object for the G0 server to clear the Global Catalog check box.
On the G0 server, run the Ntdsutil utility to defragment Active Directory.

44. You install a new Windows 2000 Server computer on your existing Windows NT network. To promote the server to a domain controller named domain.local, you run DCPromo.exe. There are no other Windows 2000 domains on your network, but you receive the error: "The domain name specified is already in use". What should you do?

A: Change the downlevel domain name to domain1.

45. Your network has two native mode domains in six sites. Each site has at least one domain controller. Authentication and directory searches are slow during high network usage. What should you do to improve network performance?

A: Designate a domain controller in each site as a global catalog server.

46. What should you do to automatically back up the Active Directory database files for your domain controllers once a week?

A: Schedule a backup job that will back up the System State data once a week.

47. You are installing a new domain named troytec1.local. You receive the error: "The domain name specified is already in use" during the promotion process. What is the cause of the problem?

A: The default-generated NetBIOS domain name is already in use.

48. Your company has four locations connected by 256 Kbps leased lines. You have a Windows 2000 domain controller at each location. What should you do to control bandwidth usage and the replication schedule of directory information to each domain controller in each location? (Choose two)

A: Create a site for each location.
Move each server object from Default-First-Site-Name to the appropriate site.

49. What should you do to strengthen your security to protect against brute force attacks? (Choose two)

A: Enable Password must meet complexity requirements.
Increase minimum password length.

50. You suspect someone has been modifying the properties of user accounts in Active Directory. You need to isolate and review events pertaining to a user reporting that they are unable to change their password. Using the least possible amount of time, how can you review the event logs for an isolated event?

A: In the security log, create a filter for events matching the criteria: Event source: Security, Category: Account Management. Search the remaining items for events referencing the user's account.

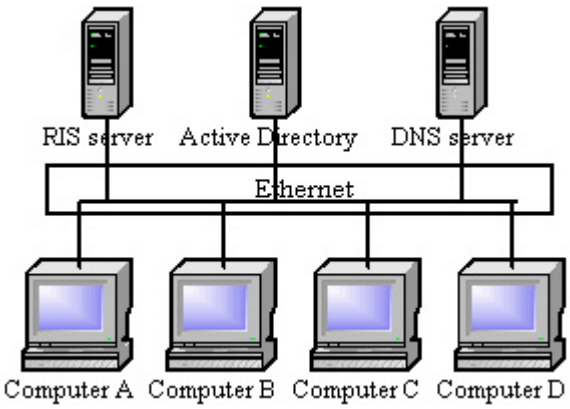
51. You have delegated the authority to create and delete computer accounts to one of your users. A second user is delegated with change user account information. A third user is delegated the ability to add client computers to the domain. What should you do to track the changes made to the directory by these three users?

A: Create a GPO for the domain controllers.
Assign Read and Apply Group Policy permissions to the three users.
Configure the GPO to audit directory services access and account management.

52. Users in your OU need to have a drive mapped during logon. Using a logon script, what should you do to implement this drive mapping for all current and future users in the OU?

A: Create a GPO that enforces the logon script as a logon script.
Assign the GPO to the OU.

53. You install a RIS server to expedite the deployment of Windows 2000 Professional on your network. When you attempt to use the RIS server to deploy Windows 2000 Professional on computers A and B, you cannot establish a connection. Computers C and D installed Windows 2000 from CD-ROM without any problems. What should you do?



A: Install a DHCP server and authorize it in Active Directory.

54. You have created a GPO and filter it to users in your Windows 2000 network. You discover that users are re-using the same password. You want to configure the GPO to require users to create different passwords periodically for security. What two settings should you enable to accomplish this goal? (Choose two)

A: Minimum password length.
Enforcement of password history.

55. Your Windows 2000 domain is running in native mode. You are going to implement a policy to disable the Shutdown command for all users, except for members of the Domain Admins security group. You create a new GPO named Shutdown, and configure it to disable the Shutdown option. You assign it to the domain. What should you do to ensure that the Domain Admins group is not affected by the policy?

A: Deny the Apply Group Policy permission to the Domain Admins group on the Shutdown GPO.

56. Your domain has an OU named HelpDesk. Users in the HelpDesk OU use their portable Windows 2000 Professional computers when they are not connected to the network. You have a Windows 2000 Server named Data1. Files used by the HelpDesk OU are contained in the \\Data1\SupFiles share. You want to accomplish the following goals:

- **Users of the HelpDesk OU can access the shared files when they are not connected to the network.**
- **Total disk space on the portable computers to automatically store files will not exceed 5 percent of the hard disk space.**

What should you do? (Choose all that apply)

A: Configure the SupFiles share on the Data1 server to cache documents automatically.
Create a new GPO named Maxdisk.
Assign the Maxdisk GPO to the HelpDesk OU.
Configure the Maxdisk GPO to limit the automatically cached offline files to 5 percent of the hard disk space.

57. Your Windows 2000 domain has a Windows 2000 Server named Boston. You want to enable roaming profiles for all users, as they use different Windows 2000 Professional computers. You want to accomplish the following goals:

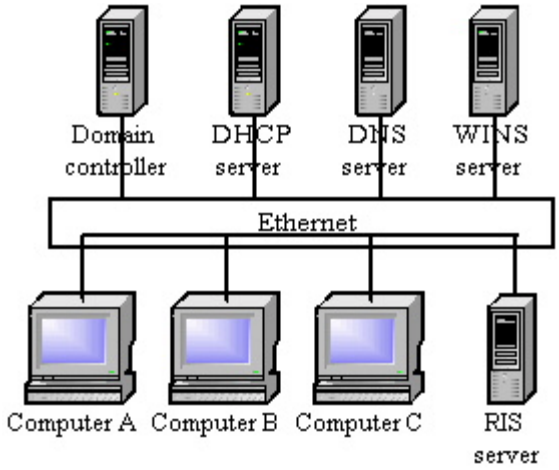
- **All users can use any Windows 2000 Professional computer utilizing their own desktop settings.**
- **Users can make changes to their desktop settings.**
- **Users can access their documents in the My Documents folder from any computer.**

- **The amount of data copied between the server and the My Documents folder will be minimized during log on or log off.**

What should you do? (Choose two)

A: Configure a roaming profile for each user. For the profile path, use \\Boston\Profiles\%Username%.
Create a new GPO named Docs. Assign the Docs GPO to the domain. Configure the Docs GPO to redirect the My Documents folder to the \\Boston\Docs\%Username% location.

58. You recently install a RIS server to deploy installation of Windows 2000 Professional. Client computers meet requirements for RIS deployment. You cannot connect the RIS client computers to the RIS server. Existing clients are able to connect to all the servers for network resources. What is the problem? (Choose all that apply)



A: The RIS server is not authorized in Active Directory.
The RIS server is not configured to respond to client computers.

59. You are deploying an application named Accounting that will be used by all users in your domain. You have been given a Windows Installer package for the installation. During the initial deployment, only members of a security group named Accounting Pilot will use the application. In the second half of the deployment, all users in the domain will install and use the application. You want to accomplish the following Phase 1 goals:

- **Only members of the Accounting Pilot group will be able to install the application using a Start menu shortcut – no other users can.**
- **The application will not be automatically installed when users log on.**
- **After Phase 1, the application will be installed automatically the first time any user logs on.**

You take the following actions:

- **Create a GPO named Deploy Accounting and link the Deploy Accounting GPO to the domain.**
- **Configure the Deploy Accounting GPO to publish the Accounting application to users.**
- **For Phase 1, configure the Deploy Accounting GPO permissions. Remove the Apply Group Policy permission for the Authenticated Users group. Grant the Apply Group Policy permission for the Accounting Pilot group.**
- **For Phase 2, configure the Deploy Accounting GPO permissions. Grant the Apply Group Policy permission for the Authenticated Users group. Remove the Apply Group Policy permission for the Accounting Pilot group.**

Which results do these actions produce? (Choose all that apply)

A: During Phase 1, the Accounting application is not installed automatically when users log on.
During Phase 1, users who are not members of the Accounting Pilot group cannot install the Accounting application by using a Start menu shortcut.

60. Your finance staff use portable computers and Routing and Remote Access to connect to your network. They need local administrator rights to their computers so they can run a third-party application. What should you do to configure their computers to prevent users from modifying their existing network connections?

A: Create a GPO for the domain. Filter the GPO for the finance users. Configure the GPO to deny the finance users access to the properties of a LAN or Routing and Remote Access connection.

61. All users in your Finance OU use an application named Accounting. It is deployed by using a GPO named Account App on the Finance OU. The Accounting App GPO is configured to assign the Accounting application to users by using a Windows Installer package. The Accounting application will be replaced in the near future. You want to accomplish the following goals:

- **Users who have not yet installed the Accounting application will be prevented from installing the application.**
- **Users who already have the application will be able to continue to use it.**
- **If key application files are missing, they will be reinstalled automatically when the Accounting application starts.**
- **If a software patch is released, you will be able to assign the patch to only users who have already installed the application.**

You take the following actions:

- **Create a new software category named Ledger Apps.**
- **Configure the Accounting App GPO to add the Accounting application to the Ledger Apps software category.**

- **Configure the Accounting App GPO to remove the Accounting application, but select the option to allow uses t continue to use the software.**

Which results do these actions produce? (Choose all that apply)

A: Users who have not yet installed the software are prevented from installing it.
Users who have already installed the software can continue to use it.

62. Your Windows 2000 Server is not a domain controller. Members of the domain Users group have the right to log on locally at this server. When one of these members logs on locally, you want a script named Params.vbs to be executed. It defines environment variables in the current user profile that are need for the Windows 2000 Server. What should you do?

A: Add the Params.vbs script to the local Group object as a logon script.

63. You are deploying a custom application named Painting. You need to set a custom policy setting in the HKCU\Software\Policies location in the registry for every user in the domain to configure the Painting application. What should you do?

A: Create a GPO named Paint Setting.
Assign the Paint Setting GPO to the domain.
Create a new administrative template that defines the custom policy setting.
Add the new administrative template to the Paint Setting GPO.
Configure the Paint Setting GPO to set the appropriate policy.

64. Your network consists of a Windows 2000 domain with three OUs. The Support OU has a Windows 2000 Server running RIS, and client computers. The Sales OU has 250 client computers, and the Research OU has 200 client computers. You are deploying Windows 2000 Professional on the computers in the Support and Sales OUs. You create a group named RIS Install which contains users from the Support OU. Only these members will use RIS to deploy Windows 2000. You want to accomplish the following goals:

- **Computers in the Research OU will not be able to download images during RIS deployment.**
- **New computer accounts will be organized into their appropriate OUs.**
- **The RIS Install group should be able to choose client computer names during installation.**
- **The existing company naming convention will be applied to new computers.**

You take the following actions:

- **Place Research computers in a different IP subnet from Support and Sales.**
- **Create an OU. In the RIS properties sheet, specify the client account location.**
- **In the RIS properties sheet, specify a custom Client computer naming format.**

Which results do these actions produce? (Choose all that apply)

A: The RIS Install group is able to choose client computer names during installation.
The existing company naming convention is applied to new computers.

65. Your network consists of two Windows 2000 domains named troytec.com and support.troytec.com. On your DNS server, you create separate zones for each domain. You then add a second DNS server which also functions as a domain controller. After you convert the troytec.com zone to an Active Directory integrated zone, and set the zone to allow only secure updates, you discover that unauthorized computers are registering themselves in the support.troytec.com domain. The zone's properties sheet shows that the zone is allowing dynamic updates, and the option to select secure dynamic updates is not available. What should you do?

A: Convert support.troytec.com to an Active Directory integrated zone.

66. You are configuring DNS throughout your Windows 2000 domain which spans multiple subnets. You want to accomplish the following goals:

- **Zone transfer information will be secure.**
- **Administrative overhead for DNS zone files is minimized.**
- **DNS zone transfer traffic is minimized.**
- **Unauthorized host computers will not have records created in the zone.**
- **Zone updates will come only from authorized DNS servers.**

You take the following actions:

- **Create an Active Directory integrated zone.**
- **Set Allow Dynamic Updates to Only Secure Updates.**
- **Enter the names and addresses of all DNS server on the network in the Name Servers tab of the Zone Properties dialog box.**
- **Select Allow zone transfers only to servers listed on the Name Servers tab on the Zone Transfers tab of the Zone Properties dialog box.**

Which results do these actions produce? (Choose all that apply)

A: DNS zone transfer traffic is minimized.
Zone updates come only from authorized DNS servers.
Administrative overhead for DNS zone files is minimized.
Unauthorized host computers do not have records created in the zone.

67. You are configuring your Windows 2000 DNS server which resides on one Windows NT domain. DNS on a Windows NT Server already exists. You are going to use dynamic updates on the DNS database. Current policy prohibits you from upgrading or decommissioning the Windows NT DNS server. All DNS information must be synchronized between your two DNS servers. What should you do? (Choose three)

A: Create a standard primary zone on the Windows 2000 DNS server and import the existing zone file.
Delete the existing zone and create a new secondary zone on the Windows NT DNS server.
Configure the secondary zone on the Windows NT DNS server to use the Windows 2000 standard primary zone as its master zone.

68. You are the network administrator for a company that is planning a merger with another company. Your network segment consists of a DNS server, a domain controller, a WINS server, and a RAS server. The network segment of the company you will be merging with consists of a domain controller which serves as a DNS server with Active Directory integrated zone, a domain controller, a WINS server, and a DHCP server. The two segments will be connected by routers. You want to host the merged domain on your DNS server. What should you do to host the merged company while retaining its domain structure after the merger is complete?

A: On the merged company's DNS server, configure DNS zone transfers to allow your DNS server to replicate data. On your DNS server, create a secondary zone with the domain name of the merged company.

69. Your Active Directory database is taking up too much space on your domain controller. What should you do to reduce the size of the Active Directory database file? (Choose three)

A: Restart the server in directory services restore mode.
Use the Ntdsutil utility to compact the database folder. Move the compacted file to the original location.
Restart the server and boot normally.

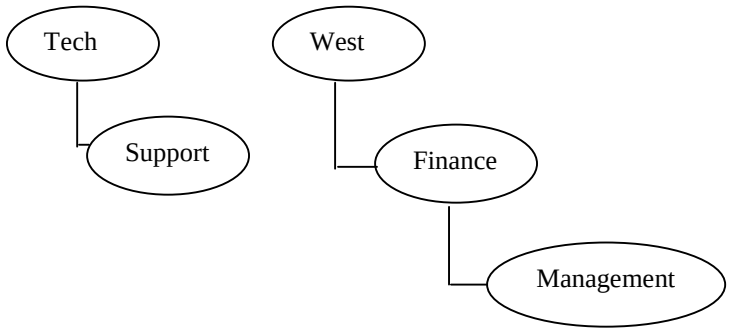
70. Your network has one domain, with three locations all connected by T1 lines. Each site contains a global catalog server. All site links have the same cost. You want users located in the West site to query the Central site if the West site global catalog server is offline. What should you do?

A: Configure the site link between the Central site and the West site to have a lower cost than the site link between the West site and the East site.

71. Your network consists of four domains named troytec.com, north.troytec.com, south.troytec.com, and salem.com. The root of the forest is troytec.com. Each domain has two Windows NT 4.0 BDCs. Technical Writers place documents for Salem, LLC in a shared folder on a domain controller named docs.salem.com. Read and Write permissions are granted to the Writers Domain Local group in the salem.com domain. Lane is a member of the Tech Writers global distribution group in the north.troytec.com domain. He is unable to gain access to the shared folder. What should you do?

A: Change the Tech Writers group type to Security and add it to the Writers Domain Local group.

72. A user in your network is moving from the Tech department to the Management department. You move his account from the Tech OU to the Management OU. You want him to be able to create user accounts in ou=finance,ou=west,dc=troytec,dc=com. What should you do?



A: Grant the user's account Create User Objects permission for the Finance OU.

73. The distinguished name for your Tech OU is ou=tech,ou=south,dc=troytec,dc=com. You want to assign a user the ability to manage all the objects in the Tech OU only. What should you do?

A: Grant the user Full Control permission to the Tech OU.

74. Your Windows 2000 network runs in native mode. It has two domains named troytec.com and support.troytec.com. Adam has a user account in the troytec.com domain, and needs to support files in the support.troytec.com domain. To accomplish this goal, you create a global group named Support in support.troytec.com. Support is a member of the Domain Local group named IS. IS has Read permission to the IS shared folder in the support.troytec.com domain. What should you do to grant Adam Read permission to the IS shared folder?

A: Create a new global group named Global IS in troytec.com. Add Adam to the new global group. Add the Global IS group to the IS group.

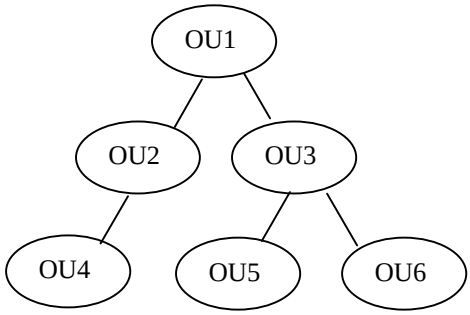
75. Your company has six locations. Three of these locations are in Europe, and three in South America. The European sites are in the eur.troytec.com domain. The South American sites are in the sa.troytec.com domain. The connection between one of the South American and one of the European sites is unreliable. You want to configure replication between these two sites. What should you do?

A: Create an SMTP site link between the two sites.

76. Your network consists of five sites in one domain. Cleveland, Louisville, and Newark will have DNS running on their domain controllers. Memphis and Salem will have DNS running on dedicated member servers. You want to allow client computers in Cleveland, Louisville, and Newark to perform secure dynamic updates to the DNS servers. The DNS servers should be configured so that each site has a replicated copy of the DNS database. What zone type should be designated for each site?

A: Drag Active Directory integrated to Louisville, Cleveland and Newark, and Secondary to Memphis and Salem.

77. You are designing a domain-wide security policy. Your OUs are organized as shown:



All domain controllers are in OU1. Resources for two buildings are in OU2 and OU3. Non-administrative users are in OUs 4 and 5. Administrative users are in OU6. You want to accomplish the following goals:

- **The number of GPO links will be minimized.**
- **All users will have the same password and account lockout policies.**
- **Only domain controllers and servers will have strict audit policies.**
- **Administrative and non-administrative computers will have different security settings.**

You take the following actions:

- **Create a single GPO.**
- **Create one security template that has all the required settings.**
- **Import the security template into the GPO.**
- **Link the GPO to the domain.**

Which results do these actions produce? (Choose all that apply)

A: All users have the same password and account lockout policies.
The number of GPO links is minimized.

78. You need to immediately implement a new security policy which renames the Administrator account on all computers in your network. You do not want to manually edit each account. What should you do? (Choose all that apply)

A: Use a Group Policy to implement a user logon script.
Use Group Policy to force all users to log off within 30 minutes.

79. You move a printer from your Sales OU to your Research OU. After you move the printer, the administrator of the Sales OU can still remove print jobs from it, although he is the administrator of resources only in the Sales OU. What should you do?

A: Remove the permission for the administrator from the printer.

80. Most of the resources your Sales team utilizes are in the west.troytec.com domain. You have a subsidiary of your company in South America with the domain salem.com. Members of the Sales team report that it is taking excessive time to access resources in the sa.salem.com domain. Network utilization is at 5 percent. What should you do to improve network performance?

A: Create an explicit trust between west.troytec.com and sa.salem.com.

81. Your na.troytec.com and eur.troytec.com domains are in mixed mode. Your troytec.com and salem.com domains are in native mode. Na.troytec.com has two Windows NT 4.0 BDCs that support legacy applications. Na.troytec.com users report when they try to access resources in a shared folder in the troytec.com domain, they are denied access. A universal group that has Read permissions to the Research folder exists. Research is assigned Read permission for the shared folder. When you log on as a member of the Research group from the troytec.com domain, you are able to access the shared folder. What should you do?

A: Create a global group in the na.troytec.com domain.
Add the user accounts from the na.troytec.com domain to the global group.
Grant Read permission to the global group for the shared folder.

82. Your company is installing a new network in Durango using 10.1.3.0/24. What should you do to prepare the network in advance so when your staff installs a new domain controller, it will automatically join the appropriate site?

A: Create a new subnet for the Durango network. Create a new site and associate the new subnet with the new site.

83. Your Domain Local group named WI has Change permissions for the Workorders In folder. The Workorders In folder is a subfolder of the Workorders folder. The Workorders In global group is a member of the WI Domain Local group. Amanda's user account is a member of the Workorders In global Group. Amanda moves to a

different department. She needs to access only resources in that department. You remove Amanda's user account from Workorders In global group, but she is still able to access the Workorders In folder. What are two possible causes of this problem? (Choose two)

A: Amanda's user account has explicit permissions on the Workorders folder.
Amanda's user account belongs to another group that gives her permissions on the Workorders In folder.

84. While you run DCPromo.exe on a failing domain controller on your domain to remove Active Directory, the hard disk drive fails. The server will not reboot. Objects for the failed server are still appearing in Active Directory. What option should you use in Ntdsutil to remove the old server from Active Directory?

A: metadata cleanup.

85. You are deploying an application named Vacation that will be used by all users in your domain. The vendor of the application did not provide a Windows Installer package. You want to use Group Policy to deploy the application with the following goals:

- **If key application files are missing, the application will be automatically reinstalled.**
- **Users can install the application by using a Start menu shortcut.**
- **Users can install the application by using Add/Remove Programs.**
- **Users can install the application by using document invocation.**

You take the following actions:

- **Create a zero administration package text file.**
- **Copy the .zap file to a shared folder on the network.**
- **Create a new GPO named Install Vacation and assign the Install Vacation GPO to the domain.**
- **Configure the Install Vacation GPO to publish the Vacation application to users by using the .ZAP file.**

Which results do these actions produce? (Choose all that apply)

A: Users can install the application by using Add/Remove Programs.
Users can install the application by using document invocation.

86. You are using RIS to deploy Windows 2000 Professional on your network. You want to allow members of the Managers group access to create custom images and post them to the RIS server for deployment, and allow them to install client computers from the RIS server. What should you do?

A: Grant the Managers group Read and Write permissions to the RemoteInstall folder.

87. Your Windows 2000 domain has an OU named Management. Your Windows 2000 Server is named Boston. All of your Windows 2000 Professional computers are on the same domain, and each is shared by many users. You want to accomplish the following goals:

- **Management OU users can use any Windows 2000 Professional computer and receive their own user profile settings.**
- **Users can access their documents in the My Documents folder from any computer.**
- **Documents will not be automatically copied to or from the server and the user's My Documents folder when users log on or log off.**

What should you do? (Choose all that apply)

A: Configure a roaming profile for each user in the Management OU. For the profile path, use \\Boston\Profiles\%Username%.
Create a new GPO named Redirect. Assign the Redirect GPO to the Management OU. Configure the Redirect GPO to redirect the My Documents folder to \\Boston\Docs\%Username%.

88. Your domain is in native mode, and contains an OU named Support. You want to delegate the control of Group Policy settings for the Support OU to a global group named Tech Support. Members of the Tech Support group should be able to create and edit new GPOs and assign these GPOs to only the Support OU. What should you do? (Choose two)

A: On existing GPOs, assign Read and Write permissions to the Tech Support group.
On the Support OU, delegate the predefined task named Manage Group Policy links to the Tech Support group.

89. You are configuring RIS to deploy Windows 2000 Professional on your new client computers. But when new users attempt to install their computers, they report that they cannot receive an IP address. What should you do?

A: Authorize the DHCP server.

90. You have numerous departments in your company. Each department needs to use specific features of Windows 2000 and custom third-party applications. You want to provide customized software installations to your users, while minimizing the administrative time required to set up the client computers. What should you do?

A: Install and configure a RIS server.
User RIPrep.exe to create multiple images for each department.
Connect the client computers to the RIS server, and deploy the custom images.

91. Your Windows 2000 domain has a Windows 2000 Server named West. Users use different Windows 2000 Professional desktop and portable computers. You want to accomplish the following goals:

- **All users can use any Windows 2000 Professional computer or portable computer when they are traveling, and have their own desktop settings.**
- **Users can access their documents in the My Documents folder from any computer, including when users dial in to the network.**
- **When users dial in to the network, the logon, and logoff times will not be delayed because of the transfer of the contents of the My Documents folder.**

What should you do? (Choose two)

A: Configure a roaming profile for each user in the domain. For the profile path, use \\West\Profiles\%Username%.
Create a new GPO named Redocs. Assign the Redocs GPO to the domain. Configure the Redocs GPO to redirect the My Documents folder to the \\West\Docs\%Username% location.

92. Your company wants to minimize the number of GPOs that are processed at logon. The Support OU has a GPO named Disable Regedit that disables the use of registry editing tools. They have decided that the restriction on the use of the registry editing tools should no longer apply to the users in the Support OU. What should you do?

A: Remove the Disable Regedit GPO from the Support OU.

93. You have two Windows 2000 Servers and only enough Windows 2000 Professional licenses for 250 of your users. What should you do to minimize user intervention, centralize the installation files, and restrict the deployment so that Windows 2000 Professional can be installed only on the licensed computers?

A: Install RIS on one of the servers.
Create computer accounts for only the licensed computers.
Configure the RIS server to accept connections from only known computers.
Perform unattended installations for all connection computers.

94. What tools should you use to find the GUIDs on client computers to complete deployment of Windows 2000 Professional using RIS?

A: Use Network Monitor to capture the DHCPDiscover frames from the client computers. Search the data fields for the GUIDs in hexadecimal format.

95. You are designing the structure of your DNS servers in your Windows 2000 network which consists of five sites in your troytec.com domain. You have 15,000 users in Cleveland, 5,000 in Lacrosse, 2,000 in Memphis, 10,000 in Newark, and 2,000 users in Salem. You must allow secure dynamic updates to DNS in Cleveland, Lacrosse, and

Newark. You want full DNS replication to occur in all the sites. You do not want Memphis to have an editable copy of the DNS zone. What zone types and server types should be assigned to each of the sites?

A: Cleveland: Domain controller, Active Directory integrated; Lacrosse: Domain controller, Active Directory integrated; Memphis: Member server, Cache only; Newark: Domain controller, Active Directory integrated; Salem: Member server; Secondary.

96. What two things must you do to set up replication so that two domain controllers in separate sites replicate every half-hour between the hours of 5 a.m. and 4 p.m.

A: Configure the replication period with a setting of once every 30 minutes.
Configure the replication schedule to allow replication between 5 a.m. and 4 p.m.

97. What is the name given to a single server that is designated in each site to perform site-to-site replication?

A: Bridgehead Server.

98. What is true about Operations Masters' placement in a Windows 2000 network? (Choose all that apply)

A: The Schema Master should always be the same machine as the Domain Naming Master.
The Infrastructure Master should never be placed on a Global Catalog Server.

99. In what order do you restore an erroneously deleted organizational unit?

A: Restart the machine. Enter directory services restore mode for the domain controller. Restore the System State data from a recent tape backup. Using Ntdsutil.exe, perform an authoritative restore.

100. What tasks can Windows Installer perform? (Choose all that apply)

A: Monitoring of file resiliency.
Modifying an existing application.
Removing an existing application.

101. You use Active Directory Users and Computers to create a distribution group with Domain Local scope. When you attempt to assign permissions to the group you are unsuccessful. Why?

A: Distribution groups are not security principals and cannot be used to assign permissions.

102. You are in charge of administering all users within the Sales OU of a domain in a multinational company. You have been delegated Full Control permission for the Sales

OU. You are configuring Group Policies to deploy Office 2000 to the desktops in the OU, and would like the applications to be available to all users who access computers in the Sales OU regardless of whether their user accounts reside in the Sales OU. What should you do?

A: Create a policy for the Sales OU. Edit the policy and assign a new package under the Computer Configuration, Software Settings, Software Installation node.

103. Which of the following require the NTFS file system? (Choose all that apply)

A: A partition that you will be enforcing Windows 2000 disk quotas on.
A partition containing the SYSVOL folder structure.
A partition where you will install Remote Installation Services (RIS).

104. When should you establish non-transitive trust relationships? (Choose all that apply)

A: Between a Windows 2000 domain and a Windows NT domain.
Between a Windows 2000 domain and a Kerberos V5 protocol security realm.
Between a Windows 2000 domain in one forest and a Windows 2000 domain in another forest.

105. What is the best way to have a Group Policy apply only to a single user within an organizational unit?

A: Set a Group Policy at the Organizational Unit level. Configure the Discretionary Access Control List for the Group Policy so that only that user account has the Apply Group Policy permission allowed.

106. What are potential benefits of using SMTP replication versus RPC-based replication? (Choose all that apply)

A: Where end-to-end online IP connectivity is impossible mail can be used and routed appropriately.

107. You configure a password policy for your domain so that all users must have a minimum password length of 6 characters. Within the domain, there is an organizational unit (OU) named Support. Due to the sensitive nature of security within the Support OU, you want to set a more secure password restriction on users within Support. You set a password policy at the organizational unit level so that all accounts within Support must have a password of 10 characters or greater. When testing the policy, you discover that you can still use a password of less than 10 characters. What is the most likely the cause?

A: Group Policies for certain account settings such as password length can only be applied at the domain level. A policy applied at an OU level would affect local logons to computers located in the OU, but it would not affect domain logons.

108. If a user attempts to log on and the domain controller that is servicing the authentication request does not recognize the user's password, the authentication request is then passed on to the machine receiving preferred replication of password changes. What is the machine performing this role on the domain called?

A: PDC emulator.

109. You want to delegate administrative tasks to several users. You create two organizational units within your root domain called Main and Branch. You grant a user named Randy to have full administrative power over the Main OU and grant a user named Grace full administrative power over the Branch OU. You do not want them to configure settings which would override the security settings that you has configured at the domain level. What should you do?

A: Configure a group policy at the domain level with the security settings and give it the setting of "No Override".

110. You configure several Group Policies to be applied to users in your company whose desktops you want to restrict. You want the Group Policies to be applied immediately to all the users that they affect. What should you do?

A: Run the secedit command to refresh the policy.

111. After installing Active Directory, Mark sets up a Group Policy to place restrictions on some of the users in his company. Mark's company currently has a single domain with four organizational units (OUs) named Sales, Finance, Marketing and Research. There are ten scientists in the company that Mark would like to place restrictions on. The user accounts for these scientists are distributed among all four of the company's OUs. All of the scientists are members of a global group called Scientists which is located in the Research OU. Mark would like a policy to apply to members of the Scientists group but not to apply to anyone else in the company. He creates a policy for the Research OU and changes the permissions so that the Scientists group has the Read and Apply Group Policy permissions. He removes the default permissions for the Authenticated Users group. However, when testing the policy, Mark does not get the results he had expected. What is the most likely reason for this and how should Mark correct the problem?

A: All of the user accounts are not located in the Research OU. A user account will only have policies applied to it based on the location of its user object. Configure the policy to be applied at the domain level rather than at the organizational unit level.

112. You want to upgrade an NT 4.0 domain on your network to Windows 2000 and minimize the amount of time that a Primary Domain Controller is unavailable. You need the ability to roll back to your current environment. What should you do?

A: . Save a pre-Windows 2000 backup domain controller (BDC). Upgrade the Windows NT primary domain controller. Install Active Directory on the Windows NT PDC, and upgrade any remaining backup domain controllers.

113. There are several schema objects created on your Windows 2000 schema upon schema installation. You want to deactivate these objects you are trying to minimize schema replication traffic. When you try to deactivate them you are unsuccessful. What is the most likely reason for this?

A: You cannot deactivate objects that were created when the schema was installed.

114. Grace is trying to change the description of the mailboxes for seven user objects in Active Directory from her workstation. Every time she tries to enter the new description for each user, it fails. She has permission to modify the Active Directory schema. What is the most likely problem?

A: Her workstation does not have the Active Directory connector management components installed.

115. Troy's Windows 2000 network has only one class for user objects called "corporate users". He wants to subdivide the users into different departments such as sales, marketing, and support. Troy creates the child classes to "corporate users" and sets the attributes. How should he move the user objects to their new classes?

A: Delete the user objects and recreate them as new instances of the new classes.

116. Drew wants to create two new classes in separate trees that will be used to identify salesmen. The trees are in different sites and are not directly connected. The name for both classes is "IT" and they have different LDAP names and object identifiers. After creating the first class and adding it to the schema, Drew tries to create the second class and fails. What is the most likely reason why?

A: Two classes cannot share a common name.

117. Your single-domain organization currently has two organizational units (OUs) for the Sales and Support. Each division has multiple departments. You have developed a Group Policy for every job category within the organization. How can you structure your OU hierarchy for Active Directory to support delegation and group policy needs?

A: Within each division, create an OU for each job category. Create a GPO for each category-based OU.

118. You are creating an unattended answer file with Setup Manager. You type the name of your downlevel domain, troytec, in the Workgroup option box rather than selecting the domain name option. You will use this answer file to install Windows 2000 Server on ten computers. How will this impact your rollout when these servers join the upgraded domain, troytec.com?

A: The computers of this unattended installation can join the domain from their current workgroup status with the identical name.

119. You need to reinstall Windows 2000 Server on a domain controller because the operating system is corrupt. How can you get the Active Directory to automatically copy domain information to the new installation?

A: Remove all existing references to the old domain controller using Sites And Services snap-in. Reinstall Windows 2000 server, reinstall Active Directory with the wizard to promote the server to a domain controller.

Index