Last updated June, 2000. Click here for updates.

Click here to see additional documents related to this study guide. Click here to receive free practice questions for Implementing and Administering Windows 2000 Services Infrastructure.

Contents

Cramsession™ for Implementing and Administering Windows 2000 Directory Services Infrastructure

Abstract:

This Cramsession will help you to prepare for Microsoft exam 70-217, Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure. Exam topics include Installing, Configuring & Troubleshooting Active Directory, DNS for Active Directory, Change & Configuration Management, Components of Active Directory, and Active Directory Security Solutions.

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

Installing, Configuring, and Troubleshooting Active, configure and troubleshoot Directory:

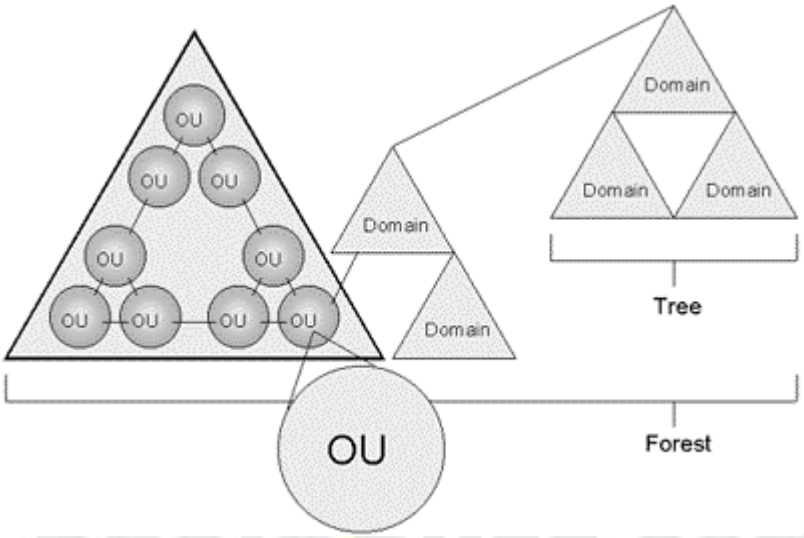
Install the components of Active Directory: (KB# Q242955)

Active Directory Overview:

Active Directory (AD) services provide a single point of network management, allowing you to add, remove, and relocate resources easily. It offers significant enhancements over the limitations of the older Windows NT domain based security model. Its features are:

- *Simplified Administration* - AD provides a single point of logon for *all* network resources - an administrator can logon to one computer and administer objects on any computer in the network.
- *Scalability* - NT 4 domains had a practical limitation of about 40,000 objects. AD scales to millions of objects, if needed.
- *Open standards support* - uses DNS as it's domain naming and location service so Windows 2000 domain names are also DNS domain names (RFCs 2052 & 2163). Support for LDAP v2 and v3 (RFCs 1823, 2247, 2251, 2252, & 2256) & LDIF (IETF draft) makes AD interoperable with other directory services that support the same, such as Novell's NDS. DHCP (RFC 2131) supports the automatic configuration of both Windows and non-Windows clients with IP addresses. HTTP support means that AD can be searched using a Web browser. SNTP (RFC 1769) provides a distributed time service. Kerberos 5 (RFC 1510) support provides interoperability with other products that use the same authentication mechanism.

Active Directory Structure:



- *Object* - distinct named set of attributes that represents a network resource such as a computer or a user account.
- *Classes* - logical groupings of objects such as user accounts, computers, domains or organizational units.
- *Organizational Unit (OU)* - container used to organize objects inside a domain into logical administrative groups such as computers, printers, user accounts, file shares, applications and even other OUs.
- *Domain* - all network objects exist within a domain with each domain storing information only about the objects it contains. A domain is a security boundary - access to objects is controlled by Access Control Lists (ACLs). ACLs contain the permissions associated with objects that control which users or types of users can access them. In Windows 2000, all security policies and settings (like Administrative rights) do not cross from one domain to another. The domain admin only has rights to set policies within his/her domain.
- *Tree* - a grouping or hierarchical arrangement of one or more Windows 2000 domains that share a contiguous name space (e.g., cramsession.brainbuzz.com, sales.brainbuzz.com, and jobs.brainbuzz.com). All domains inside a single tree share a common schema (formal definition of all object types that can be stored in an AD deployment) and share a common Global Catalog.
- *Forest* - a grouping or hierarchical arrangement of one or more domain trees that form a disjointed namespace (e.g., cramsession.com and brainbuzz.com). All trees in the forest share a common schema and Global Catalog, but have different naming structures. Domains in a forest operate independently of each other, but the forest enables communication across the domains.
- *Sites* - combination of one or more IP subnets connected by high-speed links. Not part of the AD namespace, and contain only computer objects and connection objects used to configure replication between sites.

Site Replication:

- Active Directory information is replicated between Domain Controllers (DCs) and ensures that changes to a domain controller are reflected in all DCs within a domain. A DC is a computer running Windows 2000 server which contains a replica of the domain directory (member servers do not).
- DCs store a copy of all AD information for their domain, manage changes to it and copy those changes to other DCs in the same domain. DCs in a domain automatically copy all objects in the domain to each other. When you change information in AD, you are making the change on one of the DCs.
- Administrators can specify how often replication occurs, at what times, and how much data can be sent.
- DCs immediately replicate important changes to AD like a user account being disabled. (KB# Q232690)
- AD uses *multimaster* replication meaning that no one DC is the master domain controller - all DCs within a domain are peers.
- Having more than one DC in a domain provides fault-tolerance. If a DC goes down, another is able to continue authenticating logins and providing required services using its copy of AD.
- Active Directory automatically generates a *ring topology* for replication in the same domain and site. The ring ensures that if one DC goes down, it still has an available path to replicate its information to other DCs.

Active Directory Concepts:

Schema - contains a formal definition of contents and structure of AD such as attributes, classes and class properties. For an object class, the schema defines what attributes an instance of a class must have, additional attributes that are allowed and which object class can be its parent. Installing AD on the first computer in a network creates the domain and default schema which contains commonly used objects. Extensions can be made to the schema whenever needed. By default, write access to the schema is limited to members of the Administrators group. (KB# Q229691)

Global Catalog - a central repository of info about objects in a tree or forest. AD automatically creates a global catalog from the domains that make up AD through the replication process. Attributes stored in the global catalog are usually those most often used in Search operations (like user names, logon names, etc.) and are used to locate a full replica of the object. Because of this, the global catalog can be used to find objects anywhere in the network without replication of all information between DCs.

Active Directory Naming Conventions:

- ***Distinguished Name (DN)*** - every object in AD has one. Uniquely identifies object and contains sufficient info for an AD client to retrieve it from the Directory. Includes the name of the domain that holds the object and also the complete path through the container hierarchy to it. DNs must be unique - AD will not allow duplicates.

- ***Relative Distinguished Name (RDN)*** - if the DN is unknown, you can still query an object by its attributes. The RDN is a part of the name that is an attribute of the object itself (e.g., a user's first name and location).
- ***Globally Unique Identifier (GUID)*** - unique 128-bit number assigned to objects when they are created. The GUID never changes so even if the object is renamed or moved, the GUID can be used to locate it.
- ***User Principal Name (UPN)*** - "friendly name" given to a user account (e.g., johndoe@brainbuzz.com). (KB# Q243280)

Trust Relationships:

- *Implicit two-way trust* - default in Windows 2000 AD. Trust relationships between domains in a tree are established and maintained automatically (implicitly). Feature of Kerberos authentication protocol.
- *Explicit one-way nontransitive trush* - default in Windows NT 4.0 domains. Trust is limited to the two domains in the relationship and does not flow to others. Must be manually (explicitly) created. Are the only form of trust possible with:
    - Windows NT 4.0 domains
    - Windows 2000 domains in a separate forest
    - Windows 2000 domains and MIT Kerberos 5 authentication realms.

Planning an Active Directory Implementation:

Logical environment:

- Examine the functional divisions in the target organization such as Administration, Sales, Purchasing, Training, Research and Development, etc.
- Functional divisions are usually represented as Organizational Units in Active Directory. Multiple OUs can be placed in each domain and OUs can be placed within each other as well.

Physical environment:

- *User requirements* - for each geographical and functional division you must determine the number of employees, the growth rate and any plans for expansion.
- *Network requirements* - determine how network connections are organized, network connection speeds, utilization of network connections and TCP/IP subnetting.

Administrative requirements:

- *Centralized administration* - a single admin team handles network services. Appropriate for smaller companies with fewer locations.
- *Decentralized administration* - network services provided by a number of administrators or admin teams which may be divided by location or function.
- *Customized administration* - administration for some resources is centralized and others are decentralized depending on business needs.

Domain requirements:

- A single domain can contain millions of objects and span multiple sites. It is the easiest structure to administer. MS recommends that organizations start with a single domain and only add domains when necessary.
- Domain and site structures are separate and flexible.
- Do not create separate domains to reflect your organizations functional divisions, create OUs for these instead.
- MS recommends creating separate domains for the following reasons:
    - Massive numbers of objects (over several million)
    - Different password requirements between organizations
    - Decentralized network administration
    - Replication control
    - Different Internet names (non-contiguous name space)
    - Internal political requirements
    - International requirements

Domain organization needs:

Planning a domain namespace:

- In Active Directory, the namespace is based on DNS. You will need to plan your namespace if you choose to use multiple domains.
- MS recommends that you register any domain name you plan to use with AD even if it will only be for internal use. This is to prevent internal clients from being unable to distinguish between the internal name and a name that has been publicly registered by someone else. (e.g., I named my first internal domain seanmccormick.com but this domain had already been registered by a different Sean McCormick and it caused problems - talk about finding out things the hard way). (KB# Q169213)
- Select a root domain name that will be static - it may be too costly or even impossible to change it in the future.
- Use simple/short names that are easier to remember.
- Limit the number of domain levels (no more than five) as this increases administrative tasks.
- There are two types of namespace, Internal (used by Active Directory) and External (registered with Network Solutions for access from the Internet).
- When implementing AD, you can choose to use the same or different internal and external namespaces.
- Using the same internal and external namespaces has these advantages: use of the same logon name both internally and externally (jdoe@brainbuzz.com could serve as both the logon and e-mail ID) and the tree name, brainbuzz.com for example, is consistent on both the internal network and public Internet.
- Using the same internal and external namepaces results in a more complex proxy configuration and administrators must be careful not to publish internal resources externally. There is duplication of effort in managing resources (e.g., duplicate zone records). As well, users get a different view of internal and external resources even though the namespace is the same.
- Using separate namespaces makes it easier to distinguish between internal and external resources, there is no overlap or duplication of effort making things easier to manage and proxy configuration is much simpler.

- Disadvantages of using separate namespaces are that multiple names must be registered with an Internet DNS and logon names are different from e-mail IDs.

Planning an Organizational Unit (OU) structure:

- OUs let you model your organization in the most meaningful and manageable way. You can assign local authorities as administrators at any level as appropriate.
- Administrators can delegate control over resources to users or groups at the OU level, but maintain the ability to manage them.
- Use OUs to accommodate changes in your company's org structure. Users can be easily organized between OUs, while moving them between domains takes a lot more effort.
- There are no restrictions on the depth of an OU, but a shallow hierarchy performs better than a deep one.
- MS recommends that OUs represent business structures that are not subject to change. There are three types of OU hierarchy:
    1. *Business fuction-based OUs* - based on various business functions within an organization (e.g., the top level of the OU corresponds to business divisions while the second level corresponds to fuctional divisions within the business divisions).
    2. *Geographical-based OUs* - based on the location of organization's offices. (e.g., the top level of the OU could be a region and the second level corresponds to the physical location of offices).
    3. *Business fuction and geographical-based OUs* - based on both business function and the location of company offices. (e.g., the top level corresponds to a region and the second level corresponds to functional business divisions).

Planning a site structure:

Sites are part of the Active Directory physical structure and are defined as one or more well-connected TCP/IP subnets. Site structure deals strictly with the physical environment and is maintained separately from the domain structure (logical environment). There are two major concerns when setting up your sites:

1. *Logon and authentication* - When users log on, Windows 2000 attempts to locate a domain controller in the same site as the user's system to resolve the user's logon request and to handle subsequent requests for network resources.
2. *Directory replication* - inter-site replication should be set to occur less frequently than replication that takes place within a site. The schedule and path can be configured separately for replication to occur over each site link.

Install Active Directory: (KB# Q238369)

Miscellaneous:

- Active Directory services can only be installed on Windows 2000 Server, Advanced Server or Datacenter Server. Please see the cramsession for exam 70-215 for information on installing Windows 2000 Server.
- Servers install as Member Servers (standalone) by default. File, print and Web servers are usually installed as Member Servers to reduce the administrative overhead placed on the system by participating in Active Directory as a Domain Controller. Member Servers can access Active Directory information, but do not perform any AD related authentication or storage functions. To promote a machine to a Domain Controller, run **dcpromo**.
- If Windows 2000 is being integrated into an existing Windows NT 4.0 domain structure, mixed mode must be used (installed by default). If Windows 2000 is being installed into an infrastructure where all domain controllers will be running Windows 2000, then domain controllers should be switched to native mode to take advantage of Active Directory's full benefits. (KB# Q186153)
- To automatically promote a server to a Domain Controller during unattended setup, specify the following command to run after setup completes; **dcpromo /answer:<*answer_file*>**. The answer file is a text file containing only the [DCInstall] section. (KB# Q224390)
- A member server can be promoted to a Domain Controller or demoted to a member server at any time by using **dcpromo**. To remove AD and demote a DC to a member server, you will first need to log on as an Administrator, then supply Enterprise Administrator credentials during the demotion process.
- Directory services database is installed to %systemroot%\ntds\ntds.dit by default. (KB# Q222019)

AD Installation Wizard Options:

Domain Controller Type:

- *Domain controller for a new domain* - used to create a new forest, domain tree or child domain. Server automatically becumes the first DC in the new domain.
- *Replica domain controller for an existing domain* - creates additional domain controllers within the same domain (were called BDCs in NT4). Choosing this option will delete all local accounts on the server.

Create Tree or Child Domain:

- *Create new domain tree* - creates a new domain tree that is separate from any existing trees.
- *Create a new child domain in an existing domain tree* - creates a new child domain (e.g., cramsession.brainbuzz.com) as a child of a parent domain (e.g., brainbuzz.com). Namespaces must be contiguous in trees.

Create or Join Forest:

- *Create a new forest of domain trees* - used for when the first domain in your forest or when you want to be completely independent of your current forest (e.g., if you are using a different schema).
- *Place this new domain in an existing forest* - for when you want users in the new domain tree to have access to resources in existing domain trees, and vice versa. Forests can be used to join non-contiguous or disparate namespaces which exist in separate trees. (e.g., microsoft.com and msn.com)

Domain Modes: (KB# Q186153)

- *Mixed mode* - whenever you first install or upgrade a domain controller to W2K, it defaults to mixed mode. This allows it to interoperate with domain controllers running previous versions of Windows NT.
- *Native mode* - when all of your domain controllers are running W2K and you will not be adding any more pre-W2K domain controllers to your domain, you can switch the domain over to native mode. The caveats are:
    - The server that used to be the PDC during your migration no longer acts as the domain master, but acts as a peer with the other domain controllers (multimaster replication).
    - You can no longer add older NT domain controllers to your domain
    - You will lose support for pre-Windows 2000 replication making your new W2K domain controllers inoperable with the old ones. (KB# Q240305 & Q221111)
    - This change is one way only. You cannot switch back to mixed mode from native mode.

Active Directory Support Tools: (KB# Q246926)

Additional support tools are provided on the W2K Server CD-ROM for working with Active Directory. To install them, do the following:

1. Log into Windows 2000 as an Administrator
2. Put the W2K CD into your drive and browse to \support\tools
3. Run **setup.exe**

Description of AD support tools:

Tool	Function
acldiag.exe	ACL Diagnostics. Used to determine whether users have been granted/denied access to AD objects. Can be used to reset Access Control Lists to their default values.
ADSI edit	View all objects in the directory (including schema and config naming objects), modify objects, and set ACLs on objects. (KB# Q234001 & Q234234)
dfsutil.exe	Distributed File System Utility. Manages all aspects of distributed file system.
Dnscmd.exe	DNS Server Troubleshooting Tool. Check dynamic registration of DNS resource records including secure DNS update and deregister resource records.
Dsacls.exe	View or modify ACLs of objects in AD.
Dsastat.exe	AD Diagnostic Tool. Compare naming contexts on DCs and detect differences.
Ldp.exe	Allows LDAP operations be be performed against AD. (KB# Q224543 & Q244344)
movetree.exe	AD Object Manager. Move AD objects like Ous and users between domains in a single forest.
Netdom.exe	W2K Domain Manager. Used to manage W2K domains and trust relationships. (KB# Q222525 & Q232179)
nltest.exe	Create a list of PDCs, force a shutdown, provide info about trusts and replication. (KB# Q156684 & Q228477)
repadmin.exe	Replication Diagnostics Tool. Check replication consistency between partners, status, force replication events and knowledge consistency checker recalculation. (KB# Q229896)
replmon.exe	AD Replication Monitor. Graphically display replication topology, monitor status, force replication and knowledge consistency checker recalculation. (KB# Q232072)
sdcheck.exe	Security Descriptor Check Utility. Verify ACL propagation and replication for specified objects in AD.
SIDwalker	Security Administration Tools. Consists of 3 programs, showaccs.exe, sidwalk.exe and Security Migration Editor (MMC snap-in). First two used to examine and change ACL entries. Security Migration Editor edits mappings between old and new security Ids (SIDs).

Create Sites:

- To create a site use Administrative Tools > AD Sites & Services > Sites (right-click) > New Site. Type the name of your site and select a site link.
- MS defines sites as sets of domain controllers that are well-connected in terms of speed and cost.
- A site object named Default-First-Site-Name is created on the first domain controller installed in a site. This object can be renamed.
- If the IP address of a newly installed DC 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.

Create Subnets:

- To create a subnet use Administrative Tools > AD Sites & Services > Sites > Subnets (right-click) > New Subnet. Enter the subnet address and subnet mask then associate it with a site.
- IP subnets are used by AD to find a DC in the same site as the system that is being authenticated during a logon and also to determine the best routes between DCs.

Create site links:

- To create a new site link use Administrative Tools > AD Sites & Services > Inter-Site Transports > IP or SMTP (right-click) > New Site Link. Give the link a name and choose the sites you want to connect then click OK.
- Site links are not created automatically. They must be manually created using AD Sites & Services.
- Computers in different sites cannot communicate with each other or replicate data until a site link has been established between them.
- The DEFAULTIPSITELINK object is created in the IP container when AD is installed on the first DC in a site. This object can be renamed.
- 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 10080 (one week). No replication occurs based on the interval unless the schedule allows it (e.g., the interval may be set for 30 minutes, but the schedule only permits traffic between 3am and 5am. Replication would then occur every 30 minutes between 3am and 5am).
- Check the Ignore Schedules check box for the appropriate protocol in the properties of the Inter-site Transports folder to disable site link scheduling.
- There are two protocols used for replication over site links:
    - *IP replication* - uses Remote Procedure Calls (RPCs) for both intersite and intrasite replication. Intersite IP replication uses schedules by default. Does not require a Certificate Authority (CA).
    - *SMTP replication* - only used for intersite replication. Is synchronous and ignores all schedules. Requires installation of a CA. (KB# Q222962 & Q231881)

Create site link bridges: (KB# Q244368)

- To create a new site link use Administrative Tools > AD Sites & Services > Inter-Site Transports > IP or SMTP (right-click) > New Site Link Bridge. Give the site link bridge a name and choose the site links you want to connect and then click OK.
- 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 and an administrator is creating site link bridges, it is first necessary to disable the default site link bridging.
- To disable default site link bridging open Administrative Tools > AD Sites & Services > Inter-Site Transports > IP or SMTP (right-click) > Properties. On the General tab, uncheck the Bridge All Site Links check box then click OK.

Create connection objects:

- To create a connection object use Administrative Tools > AD Sites & Services > Sites > *server_name* > NTDS Settings (right-click) > New Active Directory Connection. In the Find DCs box, select the server that will be the replication source then click OK.
- Connection objects are automatically created by the Knowledge Consistency Checker (KCC). You should only create connection objects when the ones generated by the KCC do not meet your needs. (KB# Q224815)

Create global catalog servers: (KB# Q216970)

- To create a global catalog server use Administrative Tools > AD Sites & Services > Sites > *server_name* > NTDS Settings (right-click) > Properties. Check the box next to Global Catalog Server under the General tab then click OK.
- The global catalog should only be assigned to servers that are well connected to other DCs and have sufficient resources.
- AD creates one Global Catalog server per forest by default. 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.

Move server objects between sites:

- To create a server object in a site use Administrative Tools > AD Sites & Services > *site_name* > Servers (right-click) > New > Server. Enter the name for the new server then click OK.
- To move server objects between sites use Administrative Tools > AD Sites & Services > *server_name* (right-click) > Move. Select the site you want to move the server object to then click OK.
- Server objects can represent member servers or domain controllers. Member servers can only be upgraded to domain controllers through using **dcpromo**.

Transfer Flexible Single Operations Master (FSMO) roles: (KB# Q223346)

Miscellaneous:

- DCs in Active Directory act as peers and use multimaster replication to share changes to the AD database. There are some roles that cannot be performed in a multimaster fashion and these are called *Operations Master Roles.*
- When in a single domain with a single DC, all roles reside on one machine - the operations master domain controller.
- A second machine can be made the *standby operations master domain controller.* This machine will take over if the operations master fails. Both machines should be well-connected and direct replication partners.
- In single domain with a single DC, that DC will assume all of the domain roles.

Forest-Wide Operations Master Roles (automatically assumed by the first DC installed in the forest): (KB# Q197132)

- *Schema Master* - controls all updates and changes to the schema. Any time you update the schema you are accessing the schema master. There can only be one schema master in an entire forest.
- *Domain Naming Master* - controls the addition or removal of domains in the forest. Only one allowed per forest.

Domain-Wide Operations Master Roles (automatically assumed by the first DC in the new domain):

- *Relative ID Master* - assigns relative IDs to each of the DCs in its domain. Only one allowed per domain. Every object in a domain gets a unique security ID (SID) which contains a domain SID (same for everything in the domain) and a relative ID (RID - unique for every object created in the domain).
- *PDC Emulator* - acts as a Primary Domain Controller for domains with computers operating without W2K client software or with NT BDCs. In native mode it is the preferred replication partner for password changes in a domain. Used by other DCs to authenticate logons before rejecting due to a bad password. Only one allowed per domain.
- *Infrastructure Master* - updates group-to-user references when members of groups are changed or renamed.

Operations Master Placement: (KB# Q234790)

- The infrastructure master should be located on a non-global catalog server that has a direct connection object to some global catalog in the forest, preferably in the same AD site.
- At the forest level, the domain naming and schema master roles should be placed on the same DC as they are not used much and must be tightly controlled.
- MS recommends assigning the PDC Emulator and RID Master roles to the operations master DC.
- You can reduce the peak load on the PDC emulator by moving these roles to separate DCs (both of which should be direct replication partners with the standby operations master domain controller).
- To identify RID, PDC Emulator and Infrastructure master role assignments, use the AD Users and Computers (**dsa.msc**) console. In the console tree right-click the AD Users and Computers node then choose Operations Masters. The Operations Master dialog appears. Click the appropriate tab, RID, PDC, or Infrastructure to see which machine is the master.
- The AD Schema MMC snap-in is used to determine the schema master role assignment.
- Use the AD Domains and Trusts console to identify the domain naming master role assignment.

Seizing FSMO Roles: (KB# Q223787)

- *Schema master* - failure will only be noticeable to admins when they are trying to modify the schema - it will not affect network users. Seizing the role to the standby should only be done when the master has failed permanently. Use the AD Schema MMC snap-in to transfer roles.
- *Domain naming master* - failure will only be noticeable to admins when they are trying to add or remove domains - it will not affect network users. Seizing the role to the standby should only be done when the master has failed permanently. Use the AD Domains and Trusts console to transfer roles.
- *RID master* - failure is not visible to network users. Admins will notice it is dead if they are trying to create objects in a domain that has run out of relative identifiers. Don't seize the role to the standby unless the master has failed permanently. Use the AD Users and Computers (**dsa.msc**) console to transfer roles.
- *Infrastructure master* - failure is not visible to network users. Will only be visible to admins if they have recently renamed and moved a large number of accounts. Role can be seized to a DC that is not a global catalog server but is well-connected to one - the role can be returned to the original later on. Use the AD Users and Computers (**dsa.msc**) console to transfer roles.
- *PDC emulator* - affects network users, especially those using non W2K clients. Role may need to be seized to the standby immediately. The role can be returned to the original DC later on when it has been brought back online. Use the AD Users and Computers (**dsa.msc**) console to transfer roles.
- Roles can also be seized/transferred using the **ntdsutil.exe** command-line utility. (KB# Q243267)

Verify Active Directory installation:

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

- *Directory services database* - the file **ntds.dit** is installed in the %systemroot%\ntds directory by default following promotion to a DC.
- *Shared system volume* - default location is %systemroot%\Sysvol directory. Must be installed on an NTFS partition. Exists on all W2K DCs.
- *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.
- *Default first site name* - first site is automatically created when you install the first DC.
- *Default containers* - builtin, computers, and users are all created automatically when the first domain is created.
- *Default domain controllers OU* - contains the first domain controller.
- *SRV resource records* - can be verified by checking the Netlogon.dns file in the %systemroot%\system32\Config directory on each DC (if using non-MS DNS) and looking for the LDAP SRV entry; "**_ldap._tcp.*AD_domain_name* IN SRV 0 100 389 *domain_controller_name*** or (if using MS DNS) run **nslookup** and type **ls -t SRV *AD_domain_name*** and press enter - records will be listed if they exist. (KB# Q241515)

Implement an organizational unit (OU) structure:

- To create OUs use Administrative Tools > AD Users & Computers. Choose where you want to put your OU (can be in a domain or in another OU). Choose New from the Action menu then click Organizational Unit. Enter the name of the new OU then click OK.
- To set OU properties use Administrative Tools > AD Users & Computers > *domain_name* > *OU_name* (right-click) > Properties. Here are the properties you can configure:
    - *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.

Back up and restore Active Directory: (KB# Q216993 & Q216243)

Perform a non-authoritative restore of Active Directory: (KB# Q240363)

System State components such as AD information 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 instead.

Used for restoring System State data on a local computer. Cannot be performed on a remote computer.

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.

Steps for performing a non-authoritative restore are:

1. Restart the system
2. Press F8
3. At the options menu choose Directory Services Restore Mode
4. Choose W2K as the operating system to load
5. Log on as Administrator
6. Click OK when you are warned about running in safe mode
7. Select Start > Programs > Accessories > System Tools > Backup
8. Select the Restore Wizard
9. Find the data you want to restore and select it
10. Choose either Advanced to specify restore options (this is where you specify an alternate location) or Finish to begin the restore

Perform an authoritative restore of Active Directory: (KB# Q241594)

An authoritative restore is performed immediately after a non-authoritative restore and designates the information that is authoritative (meaning that it will be replicated to other DCs in the forest even though it is not current). The authoritative data is given a higher version number than data on other DCs which allows them to accept the changes. (KB# Q216243)

Steps for performing an authoritative restore:

1. Perform a non-authoritative restore
2. Restart the system
3. Press F8
4. At the options menu choose Directory Services Restore Mode
5. Choose W2K as the operating system to load
6. Log on as Administrator
7. Click OK when you are warned about running in safe mode
8. Drop to a command prompt and type **ntdsutil** and press enter
9. Type **authoritative restore** and press enter
10. Type **restore database** to restore entire directory or type **restore subtree *<subtree_distinguished_name>*** to restore a portion then press enter.
11. Type **restore database verinc** and press enter to restore the entire directory and override the version increase.
12. Type **quit** to exit NTDSUTIL.

Recover from a system failure:

Safe Mode:

Files used in the Windows 2000 boot process: (KB# Q114841)

File:	Location:
Ntldr	System partition root
Boot.ini	System partition root (KB# Q99743)
Bootsect.dos	System partition root
Ntdetect.com	System partition root
Ntbootdd.sys*	System partition root
Ntoskrnl.exe	%systemroot%\System32
Hal.dll	%systemroot%\System32
System	%systemroot%\System32\Config

* Optional - only if system partition is on SCSI disk with BIOS disabled

BOOT.INI switches: (KB# Q239780)

- **/basevideo** - boots using standard VGA driver
- /**fastdetect=[com*x,y,z*]** - disables serial mouse detection on all COM ports if port not specified. Included by default
- **/maxmem:*n*** - specifies amount of RAM used - use when a memory chip may be bad
- **/noguiboot** - boots Windows without displaying graphical startup screen
- **/sos** - displays device driver names as they load
- **/bootlog** - enable boot logging
- **/safeboot:minimal** - boot in safe mode
- **/safeboot:minimal(alternateshell)** - safe mode with command prompt
- **/safeboot:network** - safe mode with networking support (KB# Q236346)

Booting in Safe Mode: (KB# Q202485)

- Enter safe mode by pressing F8 during operating system selection phase
- Safe mode loads basic files/drivers, VGA monitor, keyboard, mouse, mass storage and default system services. Networking is not started in safe mode. (KB# Q199175)
- ***Enable Boot Logging*** - logs loading of drivers and services to ntbtlog.txt in the *windir* folder
- ***Enable VGA Mode*** - boots Windows with VGA driver
- ***Last Known Good Configuration*** - uses registry info from previous boot. Used to recover from botched driver installs and registry changes.
- ***Recovery Console*** - only appears if it was installed using **winnt32 /cmdcons** or specified in the unattended setup file.
- ***Directory Services Restore Mode*** - used for a non-authorative restoration of Active Directory.
- ***Debugging Mode*** - again, only in Server
- ***Boot Normally*** - lets you boot, uh, normally. ;-)

Windows 2000 Control Sets: (KB# Q142033)

- Found under HKEY_LOCAL_MACHINE\System\Select - has four entries
- ***Current***- CurrentControlSet. Any changes made to the registry modify information in CurrentControlSet
- ***Default*** - control set to be used next time Windows 2000 starts. Default and current contain the same control set number
- ***Failed*** - control set marked as failed when the computer was last started using the LastKnownGood control set
- ***LastKnownGood*** - after a successful logon, the Clone control set is copied here

Recovery Console:

- Insert Windows 2000 CD into drive, change to i386 folder and run **winnt32 /cmdcons** (KB# Q216417)
- After it is installed, it can be selected from the "Please Select Operating System to Start" menu
- When starting Recovery Console, you must log on as Administrator. (KB# Q239803)
- Can also be run from Windows 2000 Setup, repair option.
- Allows you to boot to a "DOS Prompt" when your file system is formatted with NTFS.
- Looks like DOS, but is very limited. By default, you can copy from removable media to hard disk, but not vice versa - console can't be used to copy files to other media (KB# Q240831). As well, by default, the wildcards in the copy command don't work (KB# Q235364). You can't read or list files on any partition except for system partition.
- Can be used to disable services that prevent Windows from booting properly (KB# Q244905)

Command	Description
attrib	changes attributes of selected file or folder
cd or chdir	displays current directory or changes directories.
chkdsk	run CheckDisk
cls	clears screen
copy	copies from removable media to system folders on hard disk. No wildcards
del or delete	deletes service or folder
dir	lists contents of selected directory on system partition only
disable	disables service or driver
diskpart	replaces FDISK - creates/deletes partitions
enable	enables service or driver
extract	extracts components from .CAB files
fixboot	writes new partition boot sector on system partition
fixmbr	writes new MBR for partition boot sector
format	formats selected disk
listsvc	lists all services on W2K workstation
logon	lets you choose which W2K installation to logon to if you have more than one
map	displays current drive letter mappings
md or mkdir	creates a directory
more or type	displays contents of text file

rd or rmdir	removes a directory
ren or rename	renames a single file
systemroot	makes current directory system root of drive you're logged into

Startup and Recovery Settings:

- Accessed through Control Panel > System applet > Advanced tab > Startup and Recovery
- Memory dumps are always saved with the filename memory.dmp (KB# Q192463)
- Small memory dump needs 64K of space. Found in %systemroot%\minidump
- A paging file must be on the system partition and the pagefile itself at least 1 MB larger than the amount of RAM installed for Write debugging information option to work
- Use dumpchk.exe to examine contents of memory.dmp (KB# Q156280)

Recover from disk failures:

ARC paths in BOOT.INI: (KB# Q113977 & Q141702)

The Advanced Risc Computing (ARC) path is located in the BOOT.INI and is used by NTLDR to determine which disk contains the operating system. (KB# Q102873)

When a system partition has been mirrored to another volume and the primary volume fails, a startup disk with a modified ARC pathname can be used to boot to the backup volume. (KB# Q119467 & Q117131)

multi(x)	Specifies SCSI controller with the BIOS enabled, or non-SCSI controller. x=ordinal number of controller.
Scsi(x)	Defines SCSI controller with the BIOS disabled. x=ordinal number of controller.
Disk(x)	Defines SCSI disk which the OS resides on. When *multi* is used, x=0. When *scsi* is used, x= the SCSI ID number of the disk with the OS.
Rdisk(x)	Defines disk which the OS resides on. Used when OS does not reside on a SCSI disk. x=0-1 if on primary controller. X=2-3 if on multi-channel EIDE controller.
Partition(x)	Specifies partition number which the OS resides on. x=cardinal number of partition, and the lowest possible value is 1.

multi(0)disk(0)rdisk(0)partition(1). These are the lowest numbers that an ARC path can have.

Installing, Configuring, Managing, Monitoring, and Troubleshooting DNS for Active Directory:

Install, configure, and troubleshoot DNS for Active Directory: (KB# Q237675)

Integrate Active Directory DNS zones with non-Active Directory DNS zones: (KB# Q198437)

- An Active Directory Integrated zone stores its data in Active Directory rather than on the local machine. Provides greater fault-tolerance and secure updates. (KB# Q227844)
- ACL editing provides granular access to either the zone or a specified resource record in the zone. (e.g., the ACL for a specific domain name can be set so that dynamic updates are only permitted for designated DNS clients or to authorize only specific groups with permissions for updating zone or record properties). This feature is not available for standard primary zones.
- Non Microsoft DNS servers can be used with AD so long as they support RFCs 2052 (SRV records) & 2163 (dynamic updates). The DNS server in Windows NT Server 4.0 cannot be used with AD however BIND versions 8.1.2 and later can.

Configure 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. (KB# Q228803 & Q222463)
- To configure DDNS, open the DNS console, double-click the server you want to administer and then double-click Forward Lookup Zones. Right-click your domain name and choose Properties. Check the Allow Dynamic Updates box on the General tab. You must now do the same for the Reverse Lookup Zones.
- The Only Secure Updates option is only available in Active Directory Integrated zones (enabled by default).
- Root or "." zones cannot be configured for dynamic update. (KB# Q232187)

Domain Name Service (DNS) Miscellaneous Information: (KB# Q217769)

- Resolves hostnames to IP addresses.
- Active Directory cannot run without it.
- A records are also called forward lookups or host records. An A record maps a domain name to an IP address.
- Start Of Authority (SOA) records names the primary DNS server for a domain, provides an e-mail address for the admin, and specifies how long it's okay to cache its data. Keeps track of data changes through serial numbers. (KB# Q163971)
- NS records designate which servers are Name Servers in the domain.
- CNAME (Canonical Name) Records or Aliases used to provide an alias for the hostname of the server. For example, a Web server at brainbuzz.com may have the hostname "jaxx", but its CNAME alias allows it to respond to "www.brainbuzz.com". (KB# Q168322)
- MX (Mail Exchange) records allow an admin to designate which machines receive mail in a domain by order of preference (a lower number equals higher preference).
- PTR (Pointer) records are also called reverse records or reverse lookups. Allow an IP address to be resolved to a host name. Creates ".in-addr.arpa" entries. (KB# Q164213)
- SRV records allow DNS to identify server types. (KB# Q232025 & Q178169)
- A Standard Primary zone stores a master copy of the zone in a text file. Used to exchange DNS data with other servers that use text-based storage methods.
- A Standard Secondary zone creates a copy of an existing zone - used for load balancing and fault-tolerance.
- A caching DNS server simply resolves requests and caches data from resolved requests until its TTL expires. (KB# Q167234)

Manage replication of DNS data:

- In MS speak, *Zone Transfer* refers to the duplication of data between DNS servers that do **not** participate in AD. *Zone Replication* refers to the replication of data between DNS servers (on domain controllers) that **do** participate in AD.
- Zone Transfer uses DNS Notification (RFC 1996) whereas in Zone Replication DNS servers poll AD approx every 15 minutes (by default - depends on SOA refresh interval) for updates.
- There are two zone transfer types, full zone transfer (AXFR) and incremental zone transfer (IXFR):
    - *AXFR* - supported by most DNS implementations. 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. (KB# Q164017)

- has changed rather than the entire database. 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 olds version of the zone on the server or the server responding to the IXFR request doesn't recognize that type of query. (RFC 1995)

Troubleshooting:

- Use **nslookup** to troubleshoot problems with DNS. (KB# Q200525)
- DNS server event messages are kept separate from events written by other applications and services in the DNS server log which can be viewed using Event Viewer. (KB# Q235427)
- A log file, **dns.log**, can be enabled for debugging purposes. It is stored in the %systemroot\system32\dns folder by default. All debugging options are disabled by default because they can be resource-intensive. The logging options are as follows:

Option	Description
answers	logs contents of answer section for each query message handled by the DNS server service.
full packets	logs number of full packets written and sent by the DNS server service.
notify	logs notification messages received from other servers by the DNS server service.
query	logs queries received by the DNS server service from clients.
questions	logs question section from each query message processed by DNS server service.
receive	logs number of query messages received by the DNS server service.
send	logs number of query messages sent by the DNS server service.
TCP	logs number of requests received over a TCP port by the DNS server service.
UDP	logs number of requests received over a UDP port by the DNS server service.
update	logs dynamic updates received from other computers by the DNS server service.
write through	logs number of packets written through and back to the zone by the DNS server service.

Installing, Configuring, Managing, Monitoring, Optimizing, and Troubleshooting Change and Configuration Management:

Implement and troubleshoot Group Policy: (KB# Q216359)

Group policies are collections of computer and user configuration settings that are linked to domains, sites, computers, and organizational units. They are not linked directly to groups but are used extensively with OUs. GPOs (Group Policy Objects) can contain Software Settings, Windows Settings, and Administrative Templates:

- Software settings contains only information on software installation settings by default.
- Windows settings holds scripts and security settings (used for both computer configuration and user configuration).
- Windows settings also hold settings for RIS, Internet Explorer (IE) maintenance, and folder redirection (used for user configuration only).
- Administrative templates hold all registry-based group policy settings for Windows Components, System, and Network.
    - Windows components includes NetMeeting, IE, Windows Explorer, MMC, Task Scheduler, and Windows Installer
    - System controls logon and logoff functions
    - Network controls settings for Offline Files, Network, and Dial-up Connections.

Computer configuration settings apply group policies to computers, regardless of what user logs on to them. These settings are applied when Windows initializes.

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.

The more GPOs you apply, the longer it takes to startup and/or logon to a system. GPOs are handy, but don't go completely nuts with them.

Create a Group Policy Object (GPO):

- Each W2K computer can have one local GPO. These 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.
- Local GPOs are opened/created using the Group Policy snap-in for the MMC and make sure that Local Computer appears in the Group Policy Object box.
- The Local Users and Group snap-in is disabled on DCs.
- Site GPOs are opened/created using Administrative Tools > AD Sites & Services > *site_name* (right-click) > Properties > Group Policy tab.
- Domain/OU GPOs are opened/created using Administrative Tools > AD Users & Computers > *domain or OU* (right-click) > Properties > Group Policy tab.

Link an existing GPO:

- To link a GPO to an existing, domain or OU, use Administrative Tools > AD Users & Computers > *domain or OU* (right-click) > 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 & Services > *domain or OU* (right-click) > Properties > Group Policy tab. Click Add then choose the policy and click OK.

Delegate administrative control of Group Policy:

Allows you to specify which groups of Administrators have access permissions to the GPO. 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

Steps to follow:

1. Open the GPO's Group Policy snap-in
2. Right-click the root node of the console and select Properties
3. Click the Security tab
4. Choose the security group you wish to edit

Write access is required to open and view the Group Policy snap-in and see the settings it contains.

Modify Group Policy inheritance: (KB# Q231903 & Q221241)

Group policy settings are processed (inherited) in the following order:

1. *Local GPO* - there can be only one local GPO and it is processed first.
2. *Site GPOs* - these are processed next - administrator can specify the order they are processed in. Overwrites local.
3. *Domain GPOs* - multiple GPOs are processed synchronously in the order specified by the administrator. Overwrites site and local.
4. *OU GPOs* - GPOs linked to the OU highest in AD are processed first followed by GPOs linked to any child OUs. 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 processing (inheritance) order:

- *Block inheritance* - 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. Block inheritance cannot be applied to GPOs or GPO links.
- *No override* - any GPO linked to a site, domain or OU can be set to no override so that none of its policies will be overridden by a child container it is linked to.
- *Loopback setting* - only used in closely managed environments like kiosks, labs, classrooms and reception areas. Can only be set to merge or replace modes.

Filter Group Policy settings by associating security groups to GPOs: (KB# Q221930)

Setting permissions for security groups allows an administrator to filter group policy so that it only applies to the users and computers specified.

Removing GPO Links vs. Deleting GPOs:

- When a GPO link is removed, the GPO remains in AD until it is deleted, but it is no longer applied.
- Deleting a GPO removes it from any sites, domains or OUs it was linked to. You can simply remove the GPO link if you no longer want it applied and it remains in AD so that you can modify it or use it again in the future.

Manage and troubleshoot user environments by using Group Policy:

Control user environments by using administrative templates:

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.

System Policy Editor (poledit.exe) - Windows NT 4, Windows 95 and Windows 98 all use the System Policy Editor (poledit.exe) to specify user and computer configuration that is stored in the registry.

- Not secure because settings can be changed by a user with the Registry Editor (regedit.exe). Settings are imported/exported using .ADM templates.
- Are considered "undesirably persistent" as they are not removed when the policy ends.
- Windows 2000 comes with system.adm (system settings), inetres.adm (Internet Explorer settings) and conf.adm (NetMeeting settings) although the latter is not loaded by default.

Group Policy snap-ins - Exclusive to Windows 2000 and supercedes the System Policy Editor. Uses Incremental Security Templates.

- Should only be applied to Windows 2000 systems that have been clean installed onto an NTFS partition. For NTFS computers that have been upgraded from NT4 or earlier, only the Basic security templates can be applied.
- Settings can be stored locally or in AD. They are secure and cannot be changed by users - only Administrators.
- More flexible than System Policies as they can be filtered using Active Directory.
- Settings are imported/exported using .INF files. The Group Policy snap-in can be focused on a local or remote system.

Incremental Security Templates for Windows 2000: (KB# Q234926)

Template:	Filename:	Description:
Compatibility	compatws.inf compatsv.inf compatdc.inf	Compatibility template, but also referred to in MS documentation as Basic template. Sets up permissions for local users group so that legacy programs are more likely to run. Not considered a secure environment.
Secure	securews.inf securesv.inf securedc.inf	Increases security settings for Account Policy and Auditing. Removes all members from Power Users group. ACLs are not modified.
High Secure	hisecws.inf hisecsv.inf hisecdc.inf	Secure template provided for Workstations running in W2K native mode only. Requires all network 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.

*ws.inf is for a workstation, *sv.inf is for a member server, *.dc.inf is for a domain controller.

Assign script policies to users and computers:

Startup/shutdown scripts run at system startup and shutdown and are assigned to computers.

Logon/logoff scripts are assigned to users and run when the users logs on or off the system.

When a system is shut down, Windows 2000 processes the logoff scripts first followed by the shutdown scripts.

Multiple scripts can be assigned to the same user or computer and Windows processes them from top to bottom. Security settings allow the administrator to manually set the security levels assigned to a local or non-local GPO.

The default timeout value for script processing is 10 minutes. If your scripts require more than this, you must manually adjust the timeout value with a software policy.

The following scripting languages can be used: VBScript, JScript, Perl, and MS-DOS style batch files.

Manage and troubleshoot software by using Group Policy:

Deploy software by using Group Policy:

- Replaces setup.exe. Windows Installer packages are recognized by their .MSI file extension.
- Integrates software installation into Windows 2000 so that it is now centrally controlled, distributed, and managed from a central-point.
- The software life cycle consists of four phases, *Preparation*, *Deployment*, *Maintenance*, and *Removal*.

Maintain software by using Group Policy:

- Software package is installed on a Windows 2000 Server in a shared directory. A Group Policy Object (GPO) is created. Behavior filters are set in the GPO to determine who gets the software. Then the package is added to the GPO under User Configuration > Software Settings > Software Installation (this is done on the server). You are prompted for a publishing method - choose it and say OK.
- Set up Application Categories in Group Policy > *computer or user config* > Software Settings > Software Installation (right-click) > Properties > Categories > Add. Creating logical categories helps users locate the software they need under Add/Remove Programs on their client computer. Windows does not ship with any categories by default.
- When upgrading deployed software, AD can either uninstall the old application first or upgrade over top of it.
- When publishing upgrades, they can be option 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 removal of software when a GPO no longer applies.

Configure deployment options:

- You can *assign* or *publish* software packages. Software that is published has a shortcut appear on a user's Start > Programs menu, but is not installed until the first time they use it. 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 from an icon or double-click a file-type associated with the icon. Software assigned to a *computer* is not advertised - the software is installed automatically. When software is assigned to a computer it can only be removed by a local administrator - users can repair software assigned to computers, but not remove it.
- Published applications are not advertised. They are only installed through Add/Remove Programs in the Control Panel or through *invocation.* Published applications lack resiliency (do not self-repair or re-install if deleted by the user). Finally, applications can only be published to users, not computers.
- With *invocation*, when a user double-clicks on 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 invoked (installed).
- Non-MSI programs are published as .ZAP files. They cannot take advantage of MSI features such as elevated installation privileges, rolling back an unsuccessful installation, installing on first use of software or feature, etc. (KB# Q231747) .ZAP files can only be published, not assigned.
- Non-MSI programs can be repackaged using a 3rd party tool on the W2K Server CD called WinINSTALL LE. It works like SYSDIFF as it lets you take a snapshot of a system, install your application, take another snapshot and create a difference file that becomes your MSI install package. If you wish to assign a non-MSI program to a user or computer, you must first repackage it as an MSI file. (KB# Q236573)
- When software requires a CD key during installation, it can be pushed down with the installer package by typing **misexec /a <*path to .msi file*> PIDKEY="[*CD-Key*]"** (KB# Q223393)
- Modifications are created using tools provided by the software manufacturer and produce .MST files which tell the Windows Installer what is being modified during the installation. .MST files must be assigned to .MSI packages at the time of deployment. (KB# Q236943)
- Patches are deployed as .MSP files. (KB# Q226936)

Manage network configuration by using Group Policy:

Group Policy can be used to redirect the following special folders: (KB# Q232692 & Q242557)

- Application Data
- Desktop
- My Documents (KB# Q221837 & Q216463)
- My Pictures
- Start Menu

Advantages are:

- When used with roaming profiles, redirecting folders to a central server prevents files from being copied back and forth from the server to the workstation every time the user logs on and off.
- Makes a user's documents available to them even if they log onto different computers on the network.
- 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.
- User specific data can be redirected to a different volume from the user's operating system on her local computer so that her data will not be lost if her system drive needs to be formatted and her operating system reinstalled.
- Sysadmin can use group policy to set disk quota, limiting the amount of space used by special folders.

Deploy Windows 2000 by using Remote Installation Services (RIS):

Overview:

Remote Installation Services (RIS) is used to lower the Total Cost of Ownership (TCO) of Windows by simplifying the process of installing new client workstations. Currently only Windows 2000 Professional clients can be installed using RIS.

RIS Server requirements:

- DHCP Server Service
- Active Directory
- DNS Server Service
- 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. Image partition must be formatted with NTFS. RIS packages cannot be installed on either the system or boot partitions. Also cannot be on an EFS volume or DFS shared folder.

Steps for setting up RIS Server:

- 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* (default setting - RIS Server must be authorized first). Specify the location of the W2K 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 friendly text name for the CD-based image.
- Setup Wizard creates the folder structure, copies needed source files to the server, creates the initial CD-based W2K Professional image in its designated folder along with the default answer file (Ristandard.sif), and starts the RIS services on the server.
- Server must now be authorized. Open Administrative Tools > DHCP. Right-click DHCP in the console tree and choose *Manage authorized servers*. When dialog appears, click *Authorize* and enter name or IP of the RIS server (user must be a member of the Enterprise Admins group to do this).
- You may now configure your RIS Server to respond to client requests.

- 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 & 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. Variables are: %Username (user logon name), %First (user first name), %Last (user last name), %# (incremental number), %MAC (NIC hardware address) (KB# Q244964)
- Associate an answer file (.SIF) with your image.

Creating a RIPrep Image:

- Procure a Source Computer and install Windows 2000 Professional. Configure all components and settings for your desired client configuration keeping everything on a single partition (RIPrep Wizard can only image a single partition).
- Install your applications and configure them. Do not install unnecessary applications - remember that RIS requires Active Directory which can be used to publish or assign software as needed using Group Policy.
- As you created and configured the system using the Administrator profile, you will need to copy your configuration to the Default User profile so that your custom settings will not be lost.
- To launch the RIPrep Wizard, click Start > Run and type the following into the Open box: *RISServerName***reminst\admin\i386\riprep.exe**. Provide the name of the RIS Server where the image will be stored, the folder that will hold the image and a friendly text description.

RIS Client requirements: (KB# Q228908)

- Client machine must meet minimum hardware requirements for Windows 2000 Professional and must use the same Hardware Abstraction Layer (HAL).
- Must have a network adapter that meets the Pre-boot Execution Environment standard (PXE) version 99c and higher (there is a confirmed problem with v99j - KB# Q244454) or a 3 1/2" floppy drive and PCI network adapter supported by the RIS Startup Disk utility's list of supported adaptors. (KB# Q244036 & Q246184)

Comparing RIPrep images with CD-based images:

RIPrep Image	CD-based image
Can only be deployed to a computer with the same HAL as the source computer.	Can be deployed to ANY computer with a HAL supported by W2K.
Contains the OS and applications	Contains the Operating System only and applications are deployed separately using Group Policy.
Created manually	Created automatically upon installation of RIS Server
Based on a preconfigured client computer. Cannot be changed without recreating the image. Separate image required for each installation type.	Based on default settings of operating system. An image file is used to customize the image. Multiple answer (.SIF) files can be used to customize the same image.
Only necessary files and registry keys are copied to the client system. Fastest method.	All files are copied to client hard drive before Setup program is started. Slower and places and additional burden on a network.

Troubleshooting Remote Installations:

- If computer displays a BootP message but doesn't display the DHCP message, check to see if it can obtain an IP address. If it cannot, make sure a DHCP server is online, is authorized, has a valid IP address scope and that the DHCP packets are being routed. (KB# Q174765)
- 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. (KB# Q235979)
- BINL message is displayed but system is unable to connect to RIS server. Try restarting the NetPC Boot Service Manager (BINLSVC) on the RIS Server.
- If the Client cannot connect to RIS Server using the Startup disk check to make sure you used the right network adapter driver in **rbfg.exe**.
- If the installation options you expected are not available, there may be Group Policy conflicts. Check to make sure another Group Policy Object did not take precedence over your own.

Other considerations:

- You cannot create RIPrep images on a server unless it already has an existing CD-based image.
- The Remote Boot Floppy Generator utility (**rbfg.exe**) only works on Windows 2000 systems (KB# Q246618). To create boot floppies, click Start > Run and then type:
  \\RISServerName**reminst\admin\i386\rbfg.exe** and click OK
- The answer file (.SIF) supports the new [RemoteInstall] section. Setting the repartition parameter to yes causes the install to delete all partitions on the client computer and reformat the drive with one NTFS partition.
- Pre-staging images using the GUID of PXE-based workstations prevents unauthorized users from illegally installing Windows 2000 onto their systems.

- The MAC address of the network adapter can be entered into the GUID field and padded with zeros.

Managing, Monitoring, and Optimizing the Components of Active Directory

Manage Active Directory objects:

Moving Active Directory objects within a domain:

- Objects can be moved within a domain using the AD Users & 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.
- It's possible to move multiple objects at once.

Moving Active Directory objects between domains:

- Done using the **movetree** command-line utility included with the Windows 2000 Support Tools.
- When objects are moved their GUID remains unchanged but they receive a new SID.
- An OU can be moved from one domain to another without damaging any of its GPOs. The GPO link is automatically updated and continues to work.
- Users that are members of Global groups cannot be used (except for Domain users – if this is the only Global group the account belongs to then the move will be successful)
- User objects that contain any other objects cannot be moved.
- Use the **netdom** command-line utility included with the Windows 2000 Support Tools to move workstations or member servers between domains.

Publish resources in Active Directory:

- User and computer accounts are added using the AD Users & Computers console. General info is automatically published for all network users while account security info is only available to select administrator groups.
- Shared folders are published using Administrative Tools > AD Users & 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.
- Printers must be installed before they are added to AD. Use Administrative Tools > AD Users & 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. The printer will now appear in the folder you selected. (KB# Q234270 & Q234619)

Locate objects in Active Directory:

Common Active Directory Objects:

Object	Description
Computer	Info 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	Info on DCs 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. W2K automatically adds printers created on domain computers to AD.
Shared Folder	Pointer to a shared folder on a computer.

Using the Find tool:

- To find objects in AD use Administrative Tools > AD Users & Computers. Right-click a domain or container in the console tree and select Find. This allows administrators to search AD via an LDAP query against the global catalog.
- Users query AD using Search from their Start menu. They can search for computers, shared folders, printers, and users.

Create and manage accounts manually or by scripting: (KB# Q222525)

- *Local accounts* - are 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 & 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. Domain user accounts are stored in AD. Added through Administrative Tools > AD Users & Computers.
- *Built-in user accounts* - Administrator (can perform all domain related administration tasks) and Guest (allows temporary access to resources by users - disabled by default).
- *Local user profile* - created on a computer the first time a user logs on and is stored on the local hard drive. Any changes made to the profile affect that computer only.
- *Roaming user profile* - created by system Administrator and 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. Users cannot change a mandatory profile - only administrators can.
- Renaming an account retains all rights, permissions and group memberships and assign them to a different user.

- Disable accounts when they are not going to be needed for an extended period but may be needed again.
- Accounts should only be deleted when they will no longer needed.
- When a user forgets his password it can be reset. The Administrator does not need to have access to the user's old password to reset his account.

Create and manage groups: (KB# Q231273)

- *Security groups* - used to assign permissions for accessing objects in AD.
- *Distribution groups* - used for nonsecurity related functions such as sending e-mail to groups of users at the same time. Can only be accessed by AD aware programs such as Exchange Server 2000.
- *Group scopes* - domain local, global, and universal - accounts go into global groups which then go into local groups that are assigned permissions to a resource:
    - Domain local groups can contain members from any domain. Can only access resources in the domain where the group was created. Can contain global groups. Should not be used to assign permissions to AD objects.
    - 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. Can contain other global groups when running in native mode.
    - Universal groups can include members from any domain. Can contain other global and universal groups. Never put users in universal groups - affects logon performance. 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.

Control access to Active Directory objects:

- W2K keeps a list of user access permissions for every AD object called the Access Control List (ACL).
- Permissions can be used to assign admin 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.

- provide granular control over object permissions. Standard permissions are:

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.

Delegate administrative control of objects in Active Directory:

- Most common method of delegation is to assign permissions at the OU or container level rather than at the object level – easier to keep track of.
- Permissions flow from the parent container to the child container unless inheritance has been prevented.
- Should be done using the Delegation of Control Wizard – it can only assign permissions at the OU or container level. Its options are:

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 – most common. Property Specific – permissions that can be assigned to the attributes of the object. Creation/Deletion of Specific Child Objects – 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.

Manage Active Directory performance:

Monitor, maintain, and troubleshoot domain controller performance:

Performance Console: (KB# Q146005)

- Important objects are *cache* (file system cache used to buffer physical device data), *memory* (physical and virtual/paged memory on system), *physicaldisk* (monitors hard disk as a whole), *logicaldisk* (logical drives, stripe sets and spanned volumes), and *processor* (monitors CPU load)
- *Processor - % Processor Time* counter measure's time CPU spends executing a non-idle thread. If it is continually at or above 80%, CPU upgrade is recommended
- *Processor - Processor Queue Length* - more than 2 threads in queue indicates CPU is a bottleneck for system performance

- *Processor - % CPU DPC Time* (deferred procedure call) measures software interrupts.
- *Processor - % CPU Interrupts/Sec* measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check for a poorly written driver (bad drivers can generate excessive interrupts) or upgrade CPU.
- *Logical disk - Disk Queue Length* - If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set
- *Physical disk - Disk Queue Length* - same as above
- *Physical disk - % Disk Time*- If above 90%, move data/pagefile to another drive or upgrade drive
- *Memory - Pages/sec* - more than 20 pages per second is a lot of paging - add more RAM
- *Memory - Committed bytes* - should be less than amount of RAM in computer
- *diskperf* command for activating disk counters is not supported in Windows 2000

Performance Alerts and Logs: (KB# Q244640)

- *Alert logs* are like trace logs, but they only 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
- By default, log files are stored in the \Perflogs folder in the system's boot partition
- Save logs in CSV (comma separated value) or TSV (tab separated value) format for import into programs like Excel
- CSV and TSV must be written all at once. They do not support logs that stop and start. Use Binary (.BLG) for logging that is written intermittently
- Logging is used to create a baseline for future reference

Monitor, maintain, and troubleshoot Active Directory components:

Cannot create objects in AD:

RID 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 add/remove domain:

Domain Naming Master is not available. Could be due to a network problem or failure of computer holding the master role. If the problem cannot be resolved, 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 w/out 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.

Clients cannot access resources in a different domain:

Trusts may have failed between domains. Reset and verify trusts - PDC emulator must be available for this.

Manage and troubleshoot Active Directory replication: (KB# Q232072 & Q244368)

Manage intersite replication:

Replication takes place for DCs *between* sites (intersite replication) based upon a schedule, the amount of network traffic, and costs.

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 DCs outside the firewall.

Manage intrasite replication:

Replication takes place between DCs *within* a site (intrasite replication) as needed without regard to cost or schedules.

DCs in the same site replicate using notification. When one DC has changes, it notifies its partners. The partners then request the changes and the replication occurs.

Urgent replication triggers: (KB# Q232690)

The following events are replicated immediately in native-mode domains:

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

The following events are replicated immediately in mixed-mode domains:

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

Monitor replication traffic with Replication Monitor:

Replication Monitor (**replmon.exe**) is a utility that can be installed from the Windows 2000 Support Tools on the W2K CD. It can be run from any W2K DC or member server. It allows administrators to:

- synchronize between just two domain controllers
- show which objects have not yet replicated from any given machine
- trigger the KCC into recalculating the replication topology
- monitor failed replication attempts. If a preset threshold is reached, it can write an event to the event log and e-mail the administrator

- poll the server at defined intervals for current statistics and replication state and to write this to a log file
- display the Update Sequence Number (USN) value, the number of failed attempts and the reason, and flags used for direct replication partners
- show the servers participating in replication (both direct and transitive)

Monitor replication traffic with Performance Console:

The following Directory Replication Agent (DRA) counters are added to the Performance Console to measure the efficiency of AD replication traffic:

- *DRA inbound bytes total since boot* - total number of bytes inbound and sum of the number of uncompressed bytes and the number of compressed bytes
- *DRA inbound bytes not compressed (within site) since boot* - number of inbound bytes replicated that were not compressed at the source
- *DRA inbound bytes compressed (between sites - before compression) since boot* - original size in bytes of inbound compressed replication data.
- *DRA inbound bytes compressed (between sites - after compression) since boot* - Size of inbound replication data bytes in compressed format.
- *DRA outbound bytes not compressed (within site) since boot* - total number of bytes replicated out that were not compressed.

Configuring, Managing, Monitoring, and Troubleshooting Active Directory Security Solutions:

Configure and troubleshoot security in a directory services infrastructure: (KB# Q235531)

Apply security policies by using Group Policy:

- 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.
- You must have the Manage Auditing & Security Log user right on the system where you need to implement an audit policy or review the audit log.
- NTFS file system required for files and folders being audited.

Create, analyze, and modify security configurations by using Security Configuration and Analysis and Security Templates:

- The Security Configuration and Analysis snap-in is used to troubleshoot security in Windows 2000.
- The security database (e.g., **mysecuresv.mdb**) is compared to an incremental template such as hisecsv.inf and the results displayed in the right hand pane. The log of the analysis will be placed in %systemroot%\security\logs\mysecure.log
- There is a text based version of this tool that can be run from the command line - **secedit.exe**.

Implement an audit policy:

- Policy propagation takes place every 8 hours by default.
- Type **secedit /refreshpolicy machine_policy** at a command prompt to start policy propagation.
- The following event categories can be audited:

Event	Description
Account logon	Request to validate a user account received by a DC
Account management	User account added, modified, enabled/disabled, password set/changed
Directory service access	Tracks access to specified AD objects
Logon events	User logs on or off, creates or cancels a network connection
Object access	File, folder, or printer access.
Policy change	User security options, user rights, or audit policies
Privilege use	Tracks user access of rights
Process tracking	Used by programmers needing to track details of program execution
System events	System startup/shutdown or W2K security event (e.g., full audit log)

Monitor and analyze security events:

- *Application log* - contains errors, warnings, or information generated by programs running under Windows
- *System log* - contains errors, warnings, or information generated by W2K.
- *Security log* - contains info about success/failure of audited events. Only records events that auditing is set for.
- Logs are accessed through Administrative Tools > Event Viewer.

Special Thanks to Sean McCormick, MCSE, MCT, MCP+I, A+, Network+ for contributing material for this Cramsession. Sean is Chief Technology Officer, Internet-University.net
webmaster@internet-university.net