Exam **Manual**

LearnSmart

Microsoft Server 2003 Active Directory Infrastructure

(70-294)

Microsoft Certified
Systems Engineer (MCSE)

Smarter Training

This LearnSmart exam manual covers the most important concepts you need to know in order to successfully complete the Server 2003 Active Directory Infrastructure exam (70-294). By studying this exam manual, you will become familiar with a wide variety of exam-related content, including:

- Planning and Implementing an Active Directory Infrastructure
- Managing and Maintaining an Active Directory Infrastructure
- Planning and Implementing Group Policy
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Server 2003 Active Directory Infrastructure (70-294) LearnSmart Exam Manual

Product ID: 10014
Production Date: July 18, 2011
Total Questions: 25

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Introduction

This exam is part of the "Design" series of Windows Server 2003. It assumes a basic knowledge of a Windows Server 2003 and Active Directory. A large part of the exam is focused on server placement and server roles and the proper implementation of Group Policies and Group Policy Objects.

What to Know

Microsoft's exam 70-294 is an exam that can really sneak up on you if you aren't careful. In addition to being a standard Microsoft exam (and all the difficulty that is associated with that), Microsoft will ask you very difficult questions involving active directory management and user administration. Before you take the exam, it's best that you already be intimately familiar with the Windows 2003 operating system and that you have at least some experience actually administrating the Windows 2003 active directoy environment.

If you have a spare computer, you may want to install Windows Server 2003. Order evaluation versions that are time bombed from the Microsoft Web Site. You may also try calling your local Microsoft office to see if there are any available there.

When installing Windows Server 2003, be sure the computer meets the minimum hardware requirements, all cards are supported and be sure to create a complex password (Seven character minimum, numbers, letters and non-alpha numeric that does not contain a common name, i.e., IedA87#c).

When studying, focus on server types and placement, all uses of group policies and troubleshooting.

A large part of the exam is focused on server placement and server roles and the proper implementation of Group Policies and Group Policy Objects.

- Know all forms of Group Policy Objects, and how and when to implement them.
- Know how to check effective group policies.
- Know how GPO's are applied and the order they are applied in.
- Know the differences in server types, and how that is going to affect their placement.
- Know when and how to create another Knowledge Consistency Checker.
- Know GPO troubleshooting.
- Know the effects of different types of server failures; i.e., KCC, Operations Master Role, etc.

Planning and Implementing an Active Directory Infrastructure

Many things go in to making sure that your Active Directory Implementation works the way it is supposed to. Some of these things, like DNS servers, domain controllers, and having Active Directory installed are obvious. Other parts may not be so self-evident.

Plan a strategy for placing Global Catalog servers

As you plan your Active Directory network, Global Catalog servers can go a long way to making it easier for users to find resources in the far-flung corners of your network. Of course, for smaller companies with one Domain and Forest, having a global catalog server may not even be necessary.

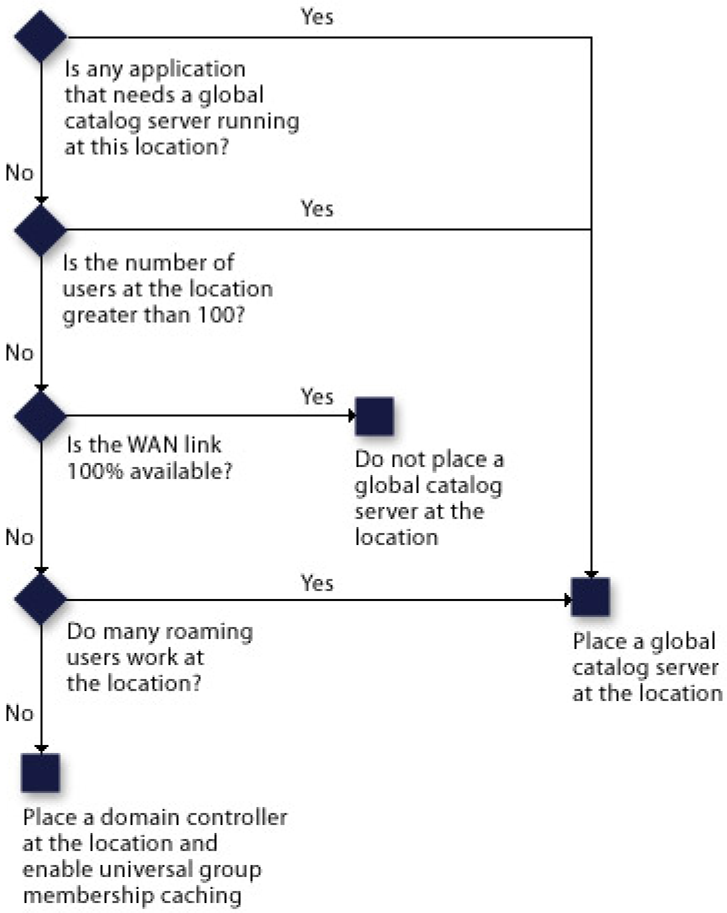

Yes
Is any application that needs a global catalog server running at this location?
No
Yes
Is the number of users at the location greater than 100?
No
Yes
Is the WAN link 100% available?
Do not place a global catalog server at the location
No
Yes
Do many roaming users work at the location?
Place a global catalog server at the location
No
Place a domain controller at the location and enable universal group membership caching

Figure 1 - Determining the Placement of Global Catalog Servers

As you can see from Figure 1, Global Catalog servers are key to efficiently finding information in other domains.

- Without a Global Catalog server, queries would require a search of every domain in the forest.
- If a Global Catalog server is not available when a user logs on to a domain running in Windows 2000 native mode or Windows Server 2003 domain functional level, and it doesn't host the user's account, the domain controller that processes the user's logon request denies the request, and the user cannot log on.
- Many applications require access to a Global Catalog server. For example, Exchange 2000 needs fast access to Global Catalog servers for all user transactions, making it very important to have a Global Catalog server nearby if you use Exchange Server 2000 or 2003.
- Apply the following guidelines to place Global Catalog servers in sites:
    - *Ensure that a Global Catalog server has enough disk space*. The disk must be able to hold partial replicas of all objects from all other domains in Active Directory.
    - *Ensure that a Global Catalog server can respond to client queries and authentication requests immediately*. If there are many users in a site or if logon authentication is slow, consider placing more than one Global Catalog server in the site.
    - *Provide enough WAN bandwidth*. Bandwidth is required to support Global Catalog replication traffic.
    - *Provide redundant Global Catalog servers*. If you have access to a second Global Catalog server on your network, it helps you protect against failure of a Global Catalog server. If the servers are remote, redundant Global Catalog servers will not protect your organization against WAN failures.
    - *Make all domain controllers Global Catalog servers if you have only one domain in a forest*. Because there is only one domain, making each domain controller a Global Catalog server will not increase replication traffic. Also, it will allow each domain controller to resolve queries to the Global Catalog locally, instead of contacting a Global Catalog server over the network.

A Note about Replication

Replication occurs so that users and services can access the latest in directory information at any time from any computer in the domain and in the forest. Replication of information occurs by category, and these categories are called a directory partition. There are four directory partitions:

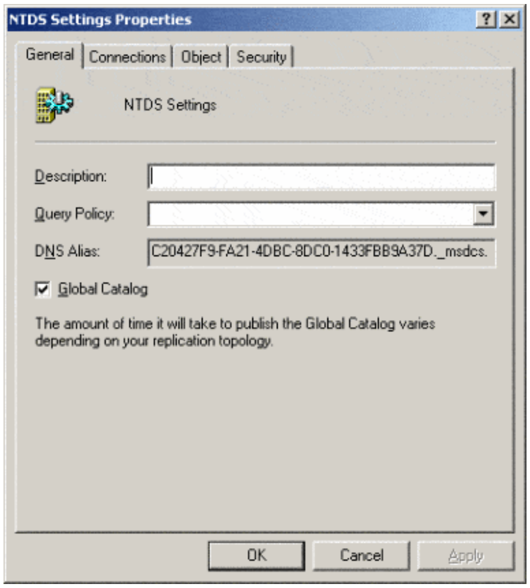
- **Schema partition** – Defines the objects that can be created in the directory and which attributes are associated with which objects. This data is common to each of the domains in a forest, and all domain controllers will receive the replicated information.
- **Configuration partition** – Describes the logical structure of networks, including data like the structure of domains or the way information is replicated. This information is common to each of the domains in the forest and all domain controllers will receive the replicated information.
- **Domain partition** – Contains information on all the objects in the domain. It is domain specific and thus not replicated to other domains. Information is replicated to all the domain controllers within the domain.

- **Application Directory partition** – Keeps dynamic application-specific information in Active Directory without affecting network performance. This partition can contain any type of objects except security principals like users, groups and computers. Data can be re-routed to specific domain controllers within a forest in order to prevent unnecessary replication traffic, or it can replicate all information to all domain controllers in the same way as the other partitions.

Installing a Global Catalog Server

To enable a Global Catalog server, perform the following steps:

- **Note**: To perform this procedure, you must be a member of the *Domain Admins* group or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate permissions.
- Open Active Directory Sites and Services.
- In the console tree, browse to and click the domain controller that will host the Global Catalog.
- In the details pane, right-click **NTDS Settings**, and then click **Properties**.
- In the NTDS Settings Properties dialog box, enter a description, if desired, indicating things like the location of server.
- Optionally, chose a query policy, if one is created. A query policy stops specific Lightweight Directory Access Protocol (**LDAP**) processes from slowing down the performance of a domain controller. It also makes a domain controller less prone to denial-of-service attacks. Query polices are created in Active Directory using the NTDSUTIL command line tool.
- Select the **Global Catalog** check box as shown in Figure 2, and then click **OK**.



NTDS Settings

Description:

Query Policy:

DNS Alias: C20427F9-FA21-4DBC-8DC0-1433FBB9A37D._msdcs.

☑ Global Catalog

The amount of time it will take to publish the Global Catalog varies depending on your replication topology.

Figure 2 – Enabling the Global Catalog Server

Evaluate network traffic considerations when placing Global Catalog servers

Users do not like it when network response falls below acceptable levels. As you will see, there are several parts of Active Directory that need to be replicated between servers in different parts of the network. Before placing Global Catalog servers, be sure to figure out how the quality of service is affected.
Global Catalog server placement tips:

- Client computers must have access to a Global Catalog server to log on. Therefore, in most cases, you must have at least one Global Catalog server in every site to gain the benefits of minimizing network traffic that using sites provides. However, in a single-domain forest environment, domain controllers do not contact a Global Catalog server when authenticating users because all universal group information is guaranteed to be stored on the domain controller.
- Place Global Catalog servers at all locations that contain more than 100 users to reduce congestion of network WAN links and to prevent productivity loss in case of WAN link failure.
- Enabling a Global Catalog server can cause additional replication traffic while the server gets a complete initial copy of the entire Global Catalog. The domain controller does not advertise itself as a Global Catalog server until it has received the Global Catalog information through replication.
- In an ideal environment, there is a Global Catalog server at each site that can process Active Directory query requests. However, too many Global Catalog servers may increase network traffic significantly because of the partial replication of all objects from all domains. Therefore, base your plan for placing Global Catalog servers on the capability of your network.
- Certain applications, such as Microsoft Exchange 2000, Message Queuing (also known as MSMQ), and applications using Distributed COM (DCOM), do not deliver adequate response over latent WAN links and therefore need a highly available Global Catalog infrastructure to provide low query latency. Determine whether any applications that perform poorly over a slow WAN link are running in these types of locations or whether the locations include Exchange servers. If your locations include applications that do not deliver optimum response over a WAN link, you must place a Global Catalog server at the location to reduce query latency.

Evaluate the need to enable universal group caching

If bandwidth is an issue, and you have a smaller network, you may not need another global catalog server. You can just enable **universal group caching**. Here are some things to consider:

- Network bandwidth and server hardware limitations may make it impractical for an organization to have a Global Catalog server in smaller branch office locations. For these sites, you can deploy domain controllers running Windows Server 2003, and then enable universal group membership caching for the site.
- Universal group membership caching in Windows Server 2003 reduces traffic and improves logon response across slow Wide Area Network (WAN) links. Universal group membership caching keeps information on the membership of Universal groups locally, without the need of another Global Catalog server.

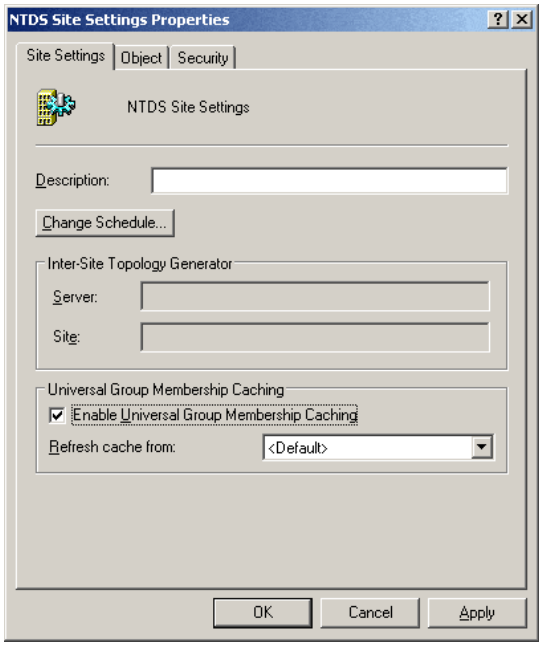
- For locations that include less than 100 users and do not include a large number of roaming users or applications that require a Global Catalog server, you can deploy domain controllers that are running Windows Server 2003 and enable universal group membership caching. Ensure that the Global Catalog servers are not more than one replication hop from the domain controller on which universal group membership caching is enabled, so that universal group information in the cache can quickly be refreshed.
- When you consider which sites to enable universal group membership caching for, develop a plan based on the ability of your network structure to manage replication and query traffic.
- Apply the following *guidelines* to determine whether to enable universal group membership caching for a site:
    - Enable universal group membership caching in sites that meet these conditions:
        - Hardware or bandwidth limitations prevent the placement of Global Catalog servers in the site.
        - One or more local domain controllers are available.
        - Loss of connectivity to the Global Catalog server may be frequent or prolonged.
        - Network resource access cannot be interrupted.
- Do not enable universal group membership caching if lost connectivity would affect connectivity to other network resources. For example, do not enable universal group membership caching in small satellite offices with no local servers. Consider alternatives before you enable universal group membership caching. The following alternatives may indicate situations for which universal group membership caching is NOT appropriate:
    - *Provide local Global Catalog servers*. This helps protect each site against WAN failures, but may not be possible if hardware limitations or bandwidth restrictions obstruct the conversion of local domain controllers to Global Catalog servers.
    - *Provide redundant WAN connections*. Many local area networks (LANs) have redundant WAN connections in times of emergency. Typically, these connections have less available bandwidth than more permanent connections, but they are usually sufficient until network connectivity is restored.
    - *Make all domain controllers Global Catalog servers*. If there is one single domain in the forest, a Global Catalog server is not contacted during authentication. However, a Global Catalog server is still used for Global Catalog searches.

Decisions on placement of Global Catalog servers and universal group caching sites must be made with an eye toward determining how important fast logins are for users in a site compared to higher replication throughput. However, for many Windows Server 2003 environments, the following *rules* apply:

Situation	Advice
Site with fewer than 50 users	Use a single domain controller configured with universal group caching
Sites with 50 – 100 users	Use two domain controllers configured for universal group caching
Sites with 100 – 200 users	Use a single Global Catalog server and a single domain controller server
Sites with 200+ users	Alternate adding additional domain controllers and Global Catalog servers/domain controllers for every 100 users

Enabling Universal Group Membership Caching
Follow the steps below to setup universal group caching on a site level:

- Open Active Directory Sites and Services.
- Navigate to Sites *SiteName*.
- In the right-hand pane, right-click NTDS Site Settings and select Properties.
- Check the Enable Universal Group Membership Caching box as shown in Figure 3 below.



☑ Enable Universal Group Membership Caching

Refresh cache from: <Default>

Figure 3 – Enabling universal group caching on a site

Plan flexible operations master role placement

Plan for business continuity of operations master roles and Identify operations master role dependencies

Most domain controller functionality in Windows Server 2003 is designed as distributed, multimaster-based. This effectively eliminated the single point of failure that was present with Windows NT 4 PDCs. However, five functions still require the use of a single server because their functionality makes it impossible to follow a distributed approach. These **Operations Master** (**OM**, or also known as **Flexible Single Master Operations,** or **FSMO**) roles are outlined, with their dependencies, in the following table:

Operations Master	Characteristics
Schema Master	There is only one writable master copy of the AD (Active Directory) schema in a single AD forest. It was deliberately designed this way to limit access to the schema and minimize potential replication conflicts. *There can be only one Schema Master in the entire Active Directory forest.*
Domain Naming Master	The Domain Naming Master is responsible for the addition of domains into the Active Directory forest. This OM role must be *placed on a Global Catalog server* because it must have a record of all domains and objects to perform its function. *There can be only one Domain Naming Master in a forest.*
PDC Emulator	The PDC Emulator does exactly what its name implies: it handles down-level clients by performing functionality previously handled by the NT primary domain controller (**PDC**). This functionality is not necessary when operating in Windows 2000 or Windows Server 2003 native mode. It is important to note that if the server running the PDC Emulator goes down, any down-level clients will have trouble with domain functions (just as though an NT PDC went down). *There is one PDC Emulator FSMO role per Active Directory domain.*
RID Master	All objects within Active Directory that can be assigned permissions are uniquely identified through the use of a Security ID (**SID**). Each SID is composed of a **domain SID**, which is the same for each object in a single domain, and a Relative ID (**RID**), which is unique for each object within that domain. When assigning SIDs, a domain controller must be able to assign a corresponding RID from a pool that it obtains from the RID master. When that pool is exhausted, it requests another pool from the RID Master. If the RID Master is down, you may not be able to create new objects in your domain if a specific domain controller runs out of its allocated pool of RIDs. *There is one RID Master per Active Directory domain*.

Infrastructure Master	The Infrastructure Master manages references to domain objects that are not within its own domain. In other words, a DC in one domain contains a list of all objects within its own domain, plus a list of references to other objects in other domains in the forest. If a referenced object changes, the Infrastructure Master handles this change. Because it deals with other referenced objects and not copies of the object itself, the Infrastructure Master must not reside on a Global Catalog server in multiple domain environments. The only exceptions to this are: 1) if every domain controller in your domain is a Global Catalog server; or 2) if you are in a single-domain environment. In the first case, there is no need to reference objects in other domains because full copies are available. In the second case, the Infrastructure Master role is not used because all copies of objects are local to the domain. There is one Infrastructure Master per Active Directory domain. **Note**: It is always best practice to locate your Infrastructure Master OM role on a domain controller without a copy of the Global Catalog, regardless of whether there is a single domain or not. This best practice stems from the fact that it is always a possibility that additional domains will be added to a forest, and setting this role up properly will help to eliminate confusion if this situation occurs. In addition, this will clear up some rather ominous-looking event errors that reappear often if the Infrastructure Master role is on a Global Catalog server.

Other best practices concerning **Operations Masters**:

- Place the domain controllers hosting operations master roles in areas where network reliability is high, and ensure that the PDC emulator and the RID master are consistently available.
- Operations master role holders like the Schema Master, Domain Naming Master, etc. are assigned automatically when the first domain controller in a given domain is created. *The two forest-level roles (Schema Master and Domain Naming Master) are assigned to the first domain controller created in a forest*. Additionally, the three domain-level roles, *RID master, Infrastructure Master, and PDC Emulator are assigned to the first domain controller created in a domain*.
- Place the first domain controller for a domain in a location that has the largest number of users for that domain. For larger companies, designate a standby Operations Master for a domain controller that hosts the operations master roles. The standby operations master is a domain controller that you identify as the computer that assumes the operations master role if the original role holder fails. Ensure that the standby operations master is a direct replication partner of the actual operations master.

For a worksheet to assist you in planning operations master role placement, go to "Domain Controller Place ment". A sample, completed worksheet can be found at "Example: Determining Domain Controller Placement"

- Operations Master Placement for a Single Domain Forest:

    - In addition to hosting the operations master roles, the first domain controller created in a forest also hosts the global catalog. In a single domain forest, the database of a global catalog server is identical to that of a domain controller. Therefore, *configure all domain controllers as global catalog servers* because it does not cause any additional workload for the domain controllers. In a single domain forest where all domain controllers are configured as global catalog servers, leave all operation master roles on the first domain controller that is created in the forest and use the second domain controller as a standby operations master.

- Operations Master Placement for a Forest Root Domain:

    - In a forest hosting multiple domains, if all domain controllers in the forest root domain are also global catalog servers, leave all the operations master roles on the first domain controller. Use the second domain controller deployed in the forest as the standby operations master.

    - If all domain controllers in the forest root domain are not also global catalog servers, move all the operations master roles to the second domain controller deployed in the forest root domain and ensure that this domain controller is never configured as a global catalog server. This is because the first domain controller is always a global catalog server and the infrastructure master should not be placed on a domain controller that is also a global catalog server unless all domain controllers are global catalog servers. To simplify the environment, *keep all the operations master roles on the second domain controller*. Configure the third domain controller deployed in the forest root domain as the standby operations master and ensure that this domain controller will also never be configured as global catalog server.

- Operations Master Placement for a regional child domain:

    - The **three domain-level roles** are assigned to the first domain controller in the domain by default. If any domain controllers in the regional domain will not host the global catalog, *leave the three-domain-level operations master roles on the first domain controller and ensure that the first domain controller is never configured as a global catalog server*. Configure the second domain controller deployed in this domain to be the standby operations master.

- **PDC Emulator placement:**

    - Place the PDC Emulator in a location that contains a *large number of users* from that domain for *password* forwarding operations. In addition, ensure that the location is well connected to other locations to minimize replication latency.

- Infrastructure Master placement:

    - *Do not place the Infrastructure Master on a domain controller that is also a global catalog server*. If the infrastructure master and global catalog are on the same domain controller, the infrastructure master will not function. The infrastructure master will never find data that is out of date, so it will never replicate any changes to the other domain controllers in the domain.

Implement an Active Directory directory service forest and domain structure

Create the forest root domain

While a rose may be a rose by another name, not all domains are created equally. Here are several important considerations:

- The first domain that you create in your Active Directory forest is automatically designated as the **Forest Root domain**. The forest root domain provides the foundation for your Active Directory forest infrastructure. You must create the forest root domain before you create regional domains or upgrade other Microsoft Windows NT 4.0 domains in order to join them to an existing forest. In addition, services that are running on forest root domain controllers, such as the **Kerberos** version 5 authentication protocol, must be highly available to ensure that users maintain access to resources throughout the forest.
- When determining the number of forests to deploy for your organization, consider the following points:
    - *Isolation requirements limit your design choices*. If you have a group of users or a department that needs to be isolated from the rest of the forest, this may impact the number of forests that need to be created. Therefore, if you identify isolation requirements, be sure that the department groups actually require data isolation and that data autonomy is not sufficient for their needs. Ensure that the various groups in your organization clearly understand the concepts of isolation and autonomy.
    - Negotiating the design can be a lengthy process, and it can be difficult for groups to come to agreement about ownership and utilization of available resources. Ensure that you allow enough time for the groups in your organization to conduct adequate research to identify their needs. Set firm deadlines for design decisions and get consensus from all parties on the established deadlines.
- *Determining the number of forests* to deploy involves balancing costs against benefits. A single forest model is the most cost-effective option and requires the least amount of administrative overhead. Although a group in the organization might prefer autonomous service operations, it might be more cost-effective for the organization to subscribe to service delivery from a centralized, trusted IT group, allowing the group to own data management without creating the added costs of service management. Balancing costs against benefits might require input from the executive sponsor.
- *A single forest* is the easiest configuration to manage and allows for maximum collaboration within the environment because:
    - All objects in a single forest are listed in the global catalog. Therefore, no cross-forest synchronization is required as well as no cross-forest trusts.
    - Management of a duplicate infrastructure is not required.
- Although the majority of small- and medium-sized organizations deploy a single Active Directory directory service forest to manage their Microsoft Windows networks, many **large organizations** find themselves in an environment that requires *multiple Active Directory forests* for the following reasons:

- **Service autonomy:** The nature of the structure or operation requires full control of delivery of the directory service.
- **Service isolation:** The nature of the structure or operation requires full protection from interference with delivery of the directory service.
- **Data isolation:** Legal ramifications require full protection from interference with directory data.
- **Schema modifications:** Because the schema is common to the entire forest, larger companies or merged companies may need more than one forest for creating or modifying schema classes and attributes.
- **Pilot deployments:** These forest deployments provide a protected test environment in which to roll out production plans before upgrading the working infrastructure. Members of the pilot forest require interaction with the production forest.
- **Grass roots deployments:** Certain departments in a larger company decide to deploy their own forest for development and testing reasons. Interaction is required between those forests and the primary network management infrastructure of the organization.
- **Mergers and acquisitions:** Companies that have separate Active Directory deployments and are merged or acquired by other companies must determine how these two deployments will interact and whether they will remain separate or be subsumed into a single network management infrastructure.
- **Divestitures:** When a segment of a large organization spins off into a separate company and deploys its own management infrastructure, the parent and child companies must determine what level of interaction is desired between the two forests, and for how long.

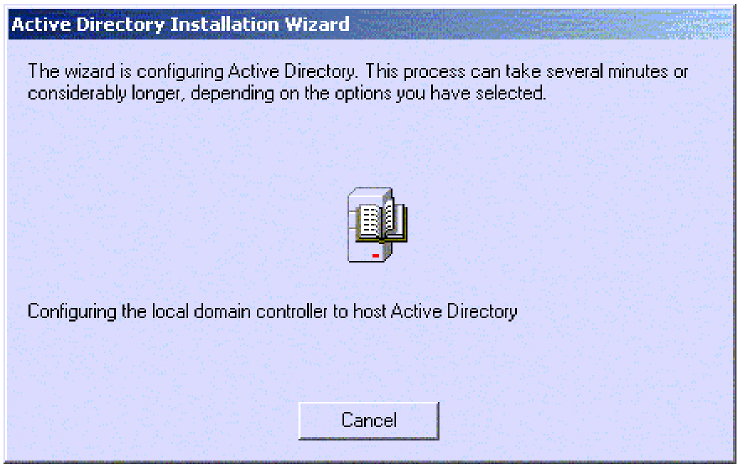
Create a child domain

A **child domain** is simply a domain created under another domain. You may have multiple levels of domains, so there can be grandchildren and even great grandchildren. For simplicity, though, domains are either parents or children. Here are other important considerations:

- Create a new child domain when you want to create a domain that shares a **contiguous namespace** with one or more domains. This means that the name of the new domain contains the full name of the parent domain. For example, sales.mydomain.com would be a child domain of mydomain.com. As a best practice, you create new domains as children of the forest root domain.
- You can create a new child domain by creating a new domain under a parent domain using the **Active Directory Installation Wizard**.
- After you create the child domain, you can create additional domain controllers in the child domain for fault tolerance and high availability of Active Directory.
- Before you run the Active Directory Installation Wizard:
    - Verify that the server on which you will be installing Active Directory has an *NTFS partition*.

  - Verify that you are a member of the *Enterprise Admins* group or the Domain Admins group of the parent domain.
  - Verify that *DNS* is properly configured before installing Active Directory.

- Follow the steps below to create a new child domain:
  - Click **Start**, click **Run**, and then type **dcpromo** to start the Active Directory Installation Wizard.
  - On the *Operating System Compatibility* page, read the information and then click **Next**.
  - On the *Domain Controller Type* page, click **Domain controller for a new domain**, and then click **Next**.
  - On the *Create New Domain* page, click **Child domain in an existing domain tree**, and then click **Next**.
  - On the *Network Credentials* page, type the user name, password, and user domain of the user account you want to use for this operation, and then click **Next**.
  - On the *Child Domain Installation* page, verify the parent domain and type the new child domain name, and then click **Next**.
  - On the *NetBIOS Domain Name* page, verify the NetBIOS name, and click **Next**.
  - On the *Database and Log Folders* page, type the location in which you want to install the database and log folders, or click **Browse** to choose a location, and then click **Next**.
  - On the *Shared System Volume* page, type the location in which you want to install the Sysvol folder, or click **Browse** to choose a location, and then click **Next**.
  - On the *DNS Registration Diagnostics* page, verify the DNS configuration settings are accurate, and then click **Next**.
  - On the *Permissions* page, select one of the following:
    - **Permissions compatible with pre-Windows 2000 server operating systems**
    - **Permissions compatible only with Windows 2000 or Windows Server 2003 operating** systems
  - On the *Directory Services Restore Mode Administrator Password* page, type and confirm the password that you want to assign to the Administrator account for this server, and then click **Next**.
  - Review the **Summary** page, and then click **Next** to begin the installation as shown in *Figure 4*.
  - Restart the computer when finished.



Active Directory Installation Wizard

The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.

Configuring the local domain controller to host Active Directory

Figure 4 – Active Directory Installation Wizard configuring Active Directory

Create and configure Application Data Partitions

There is dynamic application specific data stored in Active Directory that needs to be replicated between servers. Considerations are as follows:

- An Active Directory directory partition stores application-specific data that can be *dynamic* (subject to Time to Live restrictions). Application directory partitions can store any type of object except security principals and are not replicated to the global catalog. The replication scope of an application directory partition can be configured to include any set of domain controllers in the forest.
- Any of the following tools can be used to *create, delete, or manage application directory partitions:*
  - Application-specific tools from the application vendor.
  - **Ntdsutil** command-line tool.
  - **Lightweight Directory Access Protocol** (LDP).
  - **Active Directory Service Interfaces** (ADSI).
- Follow the steps below to create an application directory partition using the command line utility, Ntdsutil (HOW TO: Manage the Application Directory Partition and Replicas in Windows Server 2003):
  - Go to a **Command Prompt.**
  - Type **Ntdsutil** and press **Enter.**
  - At the Ntdsutil command prompt, type **domain management** and press **Enter.**
  - At the domain management command prompt, type **connection** and press **Enter.**

    - At the connection command prompt, type **connect to server <*ServerName*>** and press **Enter**
        - *Where ServerName* is the DNS name of the domain controller you want to connect to.
    - At the connection command prompt, type **quit** and press **Enter.**
    - At the domain management command prompt, type **create nc *ApplicationDirectoryPartition DomainController*** and press **Enter.**
        - *ApplicationDirectoryPartition* is the distinguished name of the application directory partition that you want to create or delete. For example, the distinguished name of the application directory partition test.mydomain.com is dc=test, dc=mydomain, dc=com.
        - *DomainController* is the DNS name of the domain controller on which to create the application directory partition. Type **NULL** to create the application directory partition on the domain controller to which you are currently connected.
    - At the domain management command prompt, type **quit** and press **Enter.**
    - At the Ntdsutil command prompt, type **quit** and press **Enter.**
    - **Note**: To perform this procedure, you must be a member of the *Domain Admins* group or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.
- There are three possible application directory partition placements within a forest namespace:
    - A child of a domain directory partition.
    - A child of an application directory partition.
    - A new tree in the forest.
- The **Knowledge Consistency Checker** (**KCC**) automatically generates and maintains the replication topology for all application directory partitions in the enterprise. When an application directory partition has replicas in more than one site, those replicas follow the same intersite replication schedule as the domain directory partition.
    - *Objects stored in an application directory partition are never replicated to the global catalog as read-only replicas.* Any domain controller running Windows Server 2003 can hold a replica, including global catalogs.
    - Additionally, *if an application requests data through the global catalog port, that query will not return any objects from an application directory partition,* even if the computer hosting the application directory partition is also hosting the global catalog. This is done so that LDAP queries to different global catalogs will not return inconsistent results because the application directory partition is replicated to only one of the global catalogs.

Install and configure an Active Directory Domain Controller

Windows Server 2003 domain controllers can be installed into existing Windows 2000 networks, or Windows NT networks. You can install the very first domain controller into a new domain in a new forest in a new network, or you can bring up a Windows Server 2003 domain controller into an existing Windows Server 2003 Active Directory network. Review the process for adding domain controllers to a site as shown in *Figure 5*. Each installation has its own set of gotcha's.

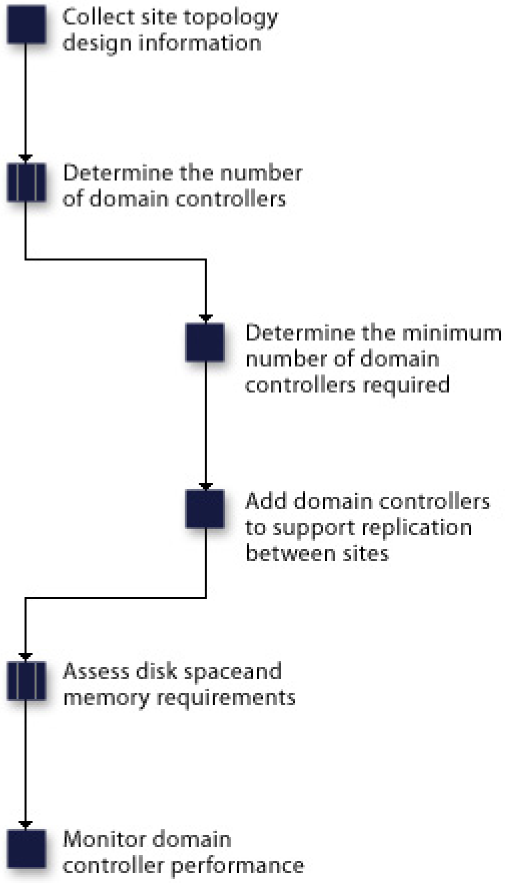

Collect site topology design information
Determine the number of domain controllers
Determine the minimum number of domain controllers required
Add domain controllers to support replication between sites
Assess disk spaceand memory requirements
Monitor domain controller performance

Figure 5 – Process for adding domain controllers to a site

Characteristics of domain controllers:

- An Active Directory domain is considered a security boundary because administrators of one domain do not have authority over another domain.
- An Active Directory domain controller is a server that contains a writable copy of the Active Directory database, participates in Active Directory replication, and controls access to network resources.
- Even a very small organization having a single local area network (LAN) with just one domain should have two domain controllers for high availability and fault tolerance.
- To configure a server as a domain controller, install Active Directory on a member server by running **dcpromo**. There are four options available in the Active Directory Installation Wizard:
    - Create an additional domain controller in an existing domain.
    - Create a domain controller for a new child domain.
    - Create a domain controller for a new domain tree.
    - Create a domain controller for a new forest.
        - Note: you must be a member of the *Domain Admins* group in the domain where you will be adding the domain controller or a member of the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority in order to complete this process.
- To install and create an additional domain controller, follow the steps outlined below:
    - Click **Start**, click **Run**, and then type **dcpromo /adv** to open the *Active Directory Installation Wizard* with the option to create an additional domain controller from restored backup files.
    - On the *Operating System Compatibility* page, read the information and then click **Next**.
    - On the *Domain Controller Type* page, click **Additional domain controller for an existing domain**, and then click **Next**.
    - On the *Copying Domain Information* page, do one of the following:
        - Click **Over the network**, and then click **Next**.
        - Click **From these restored backup files**, and type the location of the files restored from a previous backup, or click **Browse** to locate the restored files, and then click **Next**.
    - On the *Network Credentials* page, type the user name, password, and user domain of the user account you want to use for this operation, and then click **Next**.
    - On the *Database and Log Folders* page, type the location in which you want to install the database and log folders, or click **Browse** to choose a location, and then click **Next**.

- On the *Shared System Volume* page, type the location in which you want to install the Sysvol folder, or click **Browse** to choose a location, and then click **Next**.
- On the *Directory Services Restore Mode Administrator Password* page, type and confirm the password that you want to assign to the Administrator account for this server, and then click **Next**.
- Review the **Summary** page, and then click **Next** to begin the installation.
- Restart the computer.

Set an Active Directory forest and domain functional level based on requirements

Forest and **domain functionality** is a new concept introduced with Windows Server 2003. It provides a way to enable forest- or domain-wide Active Directory features within your network environment. Forest functionality enables features across all the domains within your forest. Three forest functional levels are available: **Windows 2000 (default)**, **Windows Server 2003 interim**, and **Windows Server 2003**. By default, forests operate at the Windows 2000 functional level. You can raise the forest functional level to Windows Server 2003.

The following table lists the forest functional levels and their corresponding supported domain controllers:

Forest functional level	Domain controllers supported
Windows 2000 (default)	Windows NT 4.0 Windows 2000 Windows Server 2003 family
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003 family
Windows Server 2003	Windows Server 2003 family

Once the forest functional level has been raised, domain controllers running earlier operating systems cannot be introduced into the forest. For example, if you raise the forest functional level to Windows Server 2003, domain controllers running Windows 2000 Server cannot be added to the forest.

If you are upgrading your first Windows NT 4.0 domain so that it becomes the first domain in a new Windows Server 2003 forest, you can set the domain functional level to Windows Server 2003 interim.

The following table describes the forest-wide features that are enabled for the Windows 2000 and Windows Server 2003 forest functional levels.

Forest feature	Windows 2000	Windows Server 2003
Global catalog replication improvements	Enabled if both replication partners are running Windows Server 2003. Otherwise, disabled.	Enabled
Defunct schema objects	Disabled	Enabled
Forest trusts	Disabled	Enabled
Linked value replication	Disabled	Enabled
Domain rename	Disabled	Enabled
Improved Active Directory replication algorithms	Disabled	Enabled
Dynamic auxiliary classes	Disabled	Enabled
InetOrgPerson objectClass change	Disabled	Enabled

To raise the forest functional level, perform the following:

- Open Active Directory Domains and Trusts.
- In the console tree, right-click the **Active Directory Domains and Trusts** node, and then click **Raise Forest Functional Level**.
- In **Select an available forest functional level**, click **Windows Server 2003**, and then click **Raise**.
- To perform this procedure, you must be a member of the *Domain Admins* group (in the forest root domain) or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.

If you have or will have any domain controllers running Windows NT 4.0 or Windows 2000, then do not raise the forest functional level to Windows Server 2003. Once the forest functional level has been set to Windows Server 2003, it cannot be reverted back to Windows 2000.

Domain functionality enables features that will affect the entire domain and that domain only. Four *domain* functional levels are available: **Windows 2000 mixed** (default), **Windows 2000 native, Windows Server 2003 interim, and Windows Server 2003**. By default, domains operate at the Windows 2000 mixed functional level.

The following table lists the domain functional levels and their corresponding supported domain controllers:

Domain functional level	**Domain controllers supported**
Windows 2000 mixed (default)	Windows NT 4.0 Windows 2000 Windows Server 2003 family
Windows 2000 native	Windows 2000 Windows Server 2003 family
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003 family
Windows Server 2003	Windows Server 2003 family

Once the domain functional level has been raised, domain controllers running earlier operating systems cannot be introduced into the domain. For example, if you raise the domain functional level to Windows Server 2003, domain controllers running Windows 2000 Server cannot be added to that domain.

The following table describes the domain-wide features that are enabled for three of the domain functional levels:

Domain feature	**Windows 2000 mixed**	**Windows 2000 native**	**Windows Server 2003**
Domain controller rename tool	Disabled	Disabled	Enabled
Update logon timestamp	Disabled	Disabled	Enabled
User password on InetOrgPerson object	Disabled	Disabled	Enabled
Universal Groups	Enabled for distribution groups. Disabled for security groups.	Enabled Allows both security and distribution groups.	Enabled Allows both security and distribution groups.

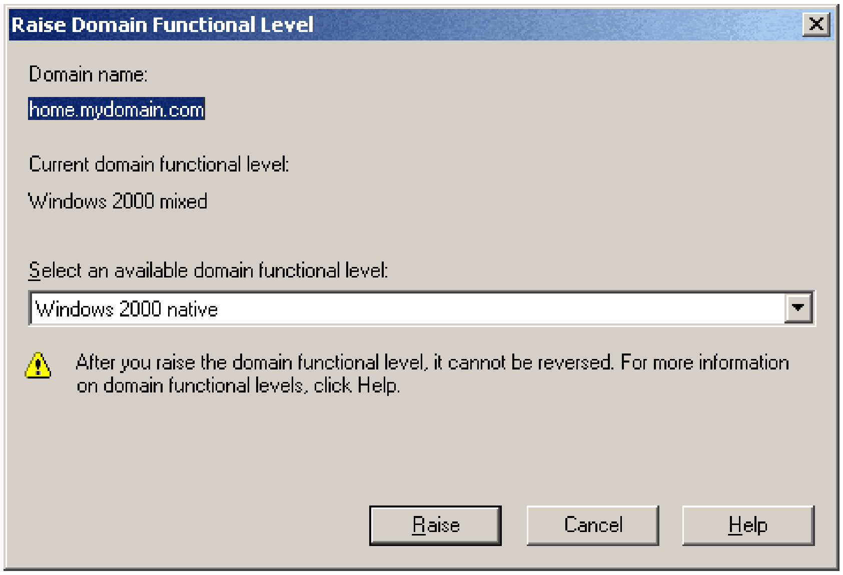
Group Nesting	Enabled for distribution groups. Disabled for security groups, except for domain local security groups that can have global groups as members.	Enabled Allows full group nesting.	Enabled Allows full group nesting.
Converting Groups	Disabled No group conversions allowed.	Enabled Allows conversion between security groups and distribution groups.	Enabled Allows conversion between security groups and distribution groups.
SID history	Disabled	Enabled Allows migration of security principals from one domain to another.	Enabled Allows migration of security principals from one domain to another.

To raise the **domain functional level**, do this:

- Open Active Directory Domains and Trusts.
- In the console tree, right-click the domain for which you want to raise functionality, and then click **Raise Domain Functional Level**.
- In **Select an available domain functional level text box as shown in *Figure 6***, do one of the following:
    - To raise the domain functional level to Windows 2000 native, click **Windows 2000 native**, and then click **Raise**.
    - To raise domain functional level to Windows Server 2003, click **Windows Server 2003**, and then click **Raise**.
- To perform this procedure, you must be a member of the *Domain Admins* group in the domain for which you want to raise functionality or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority

Important Note:

- If you have or will have any domain controllers running Windows NT 4.0 and earlier, then do not raise the domain functional level to Windows 2000 native. Once the domain functional level is set to Windows 2000 native, it cannot be changed back to Windows 2000 mixed.
- If you have or will have any domain controllers running Windows NT 4.0 and earlier or Windows 2000, then do not raise the domain functional level to Windows Server 2003. Once the domain functional level is set to Windows Server 2003, it cannot be changed back to Windows 2000 mixed or Windows 2000 native.



Raise Domain Functional Level

Domain name:

home.mydomain.com

Current domain functional level:

Windows 2000 mixed

Select an available domain functional level:

Windows 2000 native

After you raise the domain functional level, it cannot be reversed. For more information on domain functional levels, click Help.

Figure 6 – Raising Domain Functional Level

Establish trust relationships. Types of trust relationships include external trusts, shortcut trusts, and cross-forest trusts

Communication between domains occurs through trusts. Trusts are authentication pipelines that must be present in order for users in one domain to access resources in another domain. Two default trusts are created when using the Active Directory Installation Wizard. There are four other types of trusts that can be created using the **New Trust Wizard** or the **Netdom** command-line tool (to load **Netdom**, use the Windows 2003 Server CD: \Support\Tools\Suport.cab).

By default, two-way, **transitive** trusts are automatically created when a new domain is added to a domain tree or forest root domain using the *Active Directory Installation Wizard*. The two default trust types are defined in the following table:

Trust type	**Transitivity**	**Direction**	**Description**
Parent and child	Transitive	Two-way	By default, when a new child domain is added to an existing domain tree, a new parent and child trust is established. Authentication requests made from subordinate domains flow upward through their parent to the trusting domain.
Tree-root	Transitive	Two-way	By default, when a new domain tree is created in an existing forest, a new tree-root trust is established.

Four other types of trusts can be created using the **New Trust Wizard** or the **Netdom** command-line tool: **external**, **realm**, **forest**, and **shortcut** trusts. These trusts are defined in the following table:

Trust type	Transitivity	Direction	Description
External	Nontransitive	One-way or two-way	Use external trusts to provide access to resources located on a Windows NT 4.0 domain or a domain located in a separate forest that is not joined by a forest trust.
Realm	Transitive or non-transitive	One-way or two-way	Use realm trusts to form a trust relationship between a non-Windows Kerberos realm and a Windows Server 2003 domain.
Forest	Transitive	One-way or two- way	Use forest trusts to share resources between forests. If a forest trust is a two-way trust, authentication requests made in either forest can reach the other forest.
Shortcut	Transitive	One-way or two-way	Use shortcut trusts to improve user logon times between two domains within a Windows Server 2003 forest. This is useful when two domains are separated by two domain trees.

When creating external, shortcut, realm, or forest trusts, you have the option to create each side of the trust separately or both sides of a trust simultaneously.

A Windows Server 2003 domain can establish a one-way or two-way trust with:

- Windows Server 2003 or Windows 2000 domains in the same forest.
- Windows Server 2003 or Windows 2000 domains in a different forest.
- Windows NT 4.0 domains.
- Kerberos V5 realms.

When creating any type of trust, you must be a member of the *Domain Admins* group or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority to complete the process.

The process used to create any of the above trusts is very similar. Follow the steps below to create an **external trust** using the Windows GUI interface:

- Open Active Directory Domains and Trusts.
- In the console tree, right-click the domain node for the domain you want to establish a trust with, and then click **Properties**.
- On the *Trusts* tab, click **New Trust**, and then click **Next**. See *Figure 7* below.
- On the *Trust Name* page, type the DNS name (or NetBIOS name) of the domain, and then click **Next**. See *Figure 8* below.
- On the *Trust Type* page, click **External trust**, and then click **Next**.
- On the *Direction of Trust* page, do one of the following:
    - To create a two-way, external trust, click **Two-way**.
    - To create a one-way, incoming external trust, click **One-way:incoming**.
    - To create a one-way, outgoing external trust, click **One-way:outgoing**.
- Continue with the New Trust Wizard until finished.

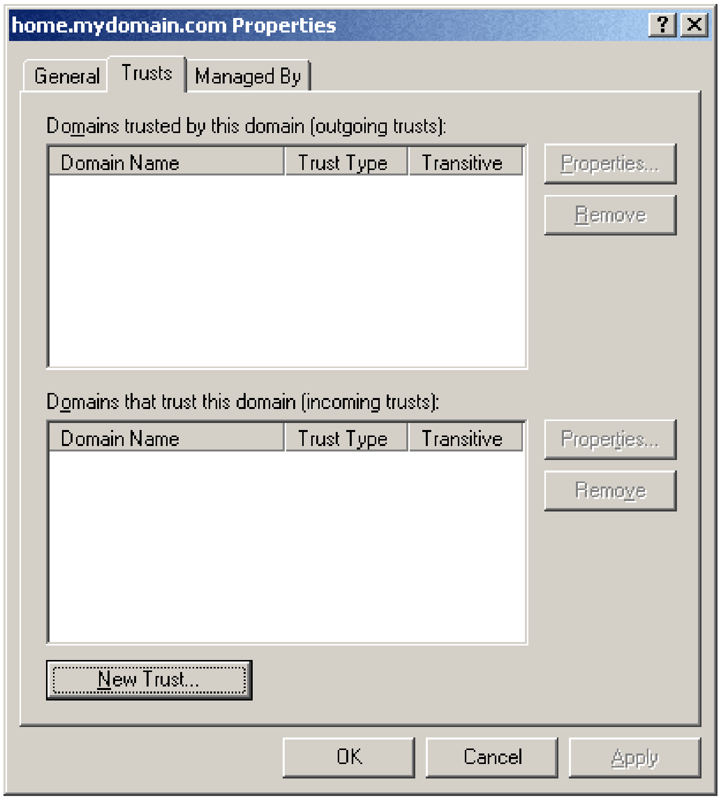
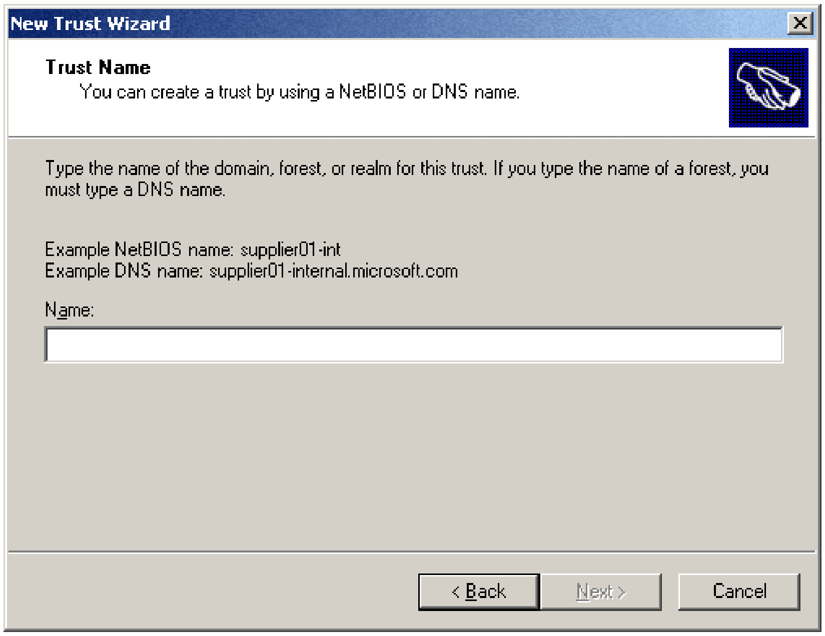


Figure 7 – Properties screen for the domain at Active Directory Domains and Trusts



Trust Name

You can create a trust by using a NetBIOS or DNS name.

Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com

Name:

Figure 8 – New Trust Wizard

Follow the steps below to create an **external trust** from a command prompt:

- Open a command prompt.
- Type: **netdom trust** *TrustingDomainName* **/d:***TrustedDomainName* **/add**
  - *TrustingDomainName* = Specifies the DNS name (or NetBIOS name) of the trusting domain in the trust being created.
  - *TrustedDomainName* = Specifies the DNS name (or NetBIOS name) of the domain that will be trusted in the trust being created.
- For more information on this command syntax, type **netdom trust | more**

Implement an Active Directory site topology

When you install Active Directory on the first domain controller in the forest, a site object named **Default-First-Site-Name** is created in the Sites container in Active Directory. The server object for the first domain controller is created in this site.

If no additional sites have been defined in Active Directory, the server object for all subsequent domain controllers will be added to the Default-First-Site-Name site object. However, if additional sites are defined in Active Directory and the IP address of the installation computer matches an existing subnet in a defined site, the domain controller is added to that site.

To simplify the placement of the domain controller into the appropriate site, configure your site topology before you install Active Directory on additional domain controllers. After all sites are created, a server object for each additional domain controller is created in the appropriate site according to its IP address.

Configure site links

Create a **site link design** in order to connect your sites with site links. Site links reflect the intersite connectivity and method used to transfer replication traffic. You must connect sites with site links so that domain controllers at each site can replicate Active Directory changes. Here are some other details:

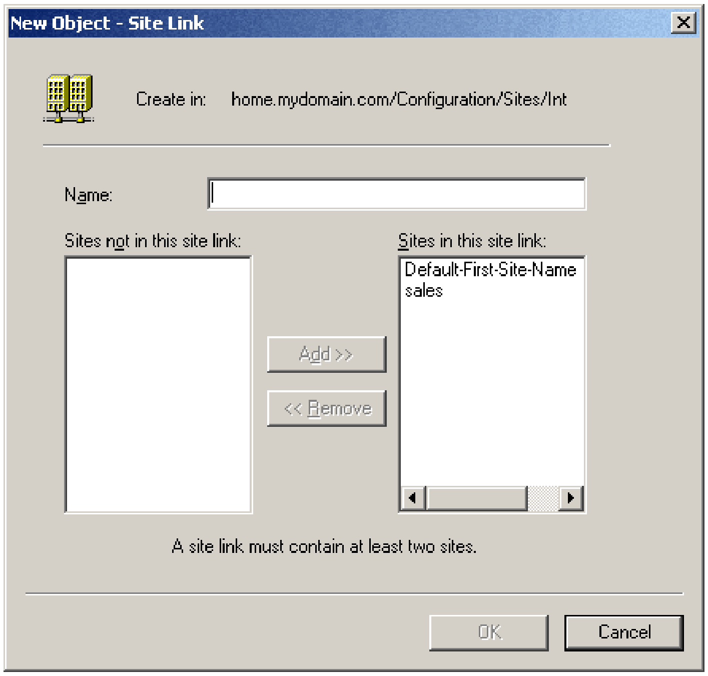
- To connect sites with site links, identify the member sites that you want to connect with the site link, create a *site link object* in the respective **Inter-Site Transports** container (Active Directory Sites and Services), and then name the site link. After you create the site link, you can proceed to set the site link properties.
- When creating site links, ensure that every site is included in a site link. In addition, ensure that all sites are connected to each other through other site links so that the changes can be replicated from domain controllers in any site to all other sites. If you fail to do this, then the KCC generates an error message in the Directory Service log in Event Viewer stating that the site topology is not connected.
- Whenever you add sites to a newly created site link, determine if the site being added is a member of other site links and change the site link membership of the site if needed. For example, if you make a site a member of the default-first-site-link when you initially create the site, be sure to remove the site from the default-first-site-link after you add the site to a new site link. If you do not remove the site from the default-first-site-link, the KCC will make routing decisions based on the membership of both site links, which may result in incorrect routing.
- The **Inter-Site Transports** container provides the means for mapping site links to the transport that the link uses. When you create a site link object, you create it in either the IP container, which associates the site link with the **RPC** (Remote Call Procedure) over IP transport or **SMTP** (Simple Mail Transfer Protocol) container, which associates the site link with the SMTP transport. When you create a site link object in the respective **Inter-Site Transports** container, Active Directory uses RPC over IP to transfer both *intersite* and *intrasite* replication between domain controllers. To keep data secure while in transit, RPC over IP replication uses both the *Kerberos* authentication protocol and *data encryption*.
- When a direct IP connection is not available, you can configure replication between sites to use **SMTP**. However, SMTP replication functionality is limited and requires an enterprise certification authority (CA). SMTP can only replicate the configuration, schema, and application directory partitions, and does not support the replication of domain directory partitions.
- To name site links, use a consistent naming scheme, such as *name_of_site1-name_of_site2*. Record the list of sites, linked sites, and the names of the site links connecting these sites in a worksheet.

Follow the steps below to create a site link:

- Open **Active Directory Sites and Services**.
- In the console tree, select Inter-Site Transports and right-click the intersite transport protocol you want the site link to use (IP or SMTP), and then click **New Site Link**. To summarize thus far:

- Active Directory Sites and Services
- Sites
- Inter-Site Transports
- inter-site transport protocol you want the site link to use

- In **Name**, type the name to be given to the link. See *Figure 9* below.
- Click two or more sites to connect, and then click **Add**.
- Configure the site link's cost, schedule, and replication frequency. See Site Link articles listed in Cramsession References for more information.
- If you create a site link that uses SMTP, you must have an Enterprise Certification Authority (Enterprise CA) available and SMTP must be installed on all domain controllers that will use the site link.
- To perform this procedure, you must be a member of the *Domain Admins* group (in the forest root domain) or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.



Create in: home.mydomain.com/Configuration/Sites/Int

Name:

Sites not in this site link:

Sites in this site link:
Default-First-Site-Name
sales

A site link must contain at least two sites.

Figure 9 – Creating a new Site Link

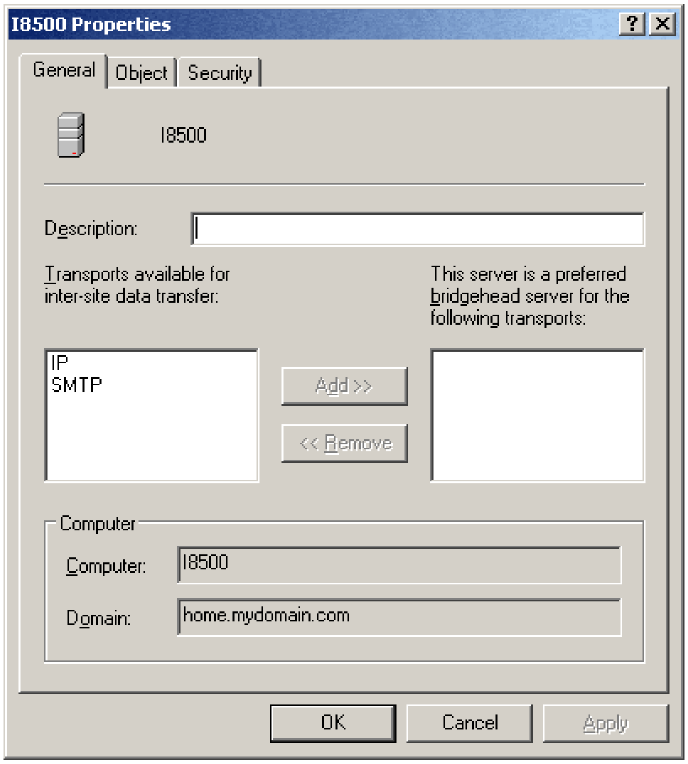
Configure preferred bridgehead servers

Even though the **Knowledge Consistency Checker (KCC)** can do this for you, there are times you may want to take control and define the preferred bridgehead servers manually.

- The **KCC** will automatically construct intersite replication topology, assigning one or more **bridgehead servers** for each site to ensure that directory changes only need to be replicated across a site link one time. Generally, it is best to allow the KCC to make the bridgehead server assignments.
- Assigning a bridgehead server manually can cause replication problems because it prevents the (KCC) from making an automatic failover assignment if a manually selected bridgehead server fails.
- If your site uses a *firewall* for protection, you must designate the *firewall proxy server* as the **preferred bridgehead server**, which makes it the contact point for exchanging information with other sites. If you do not do this step, Active Directory may not replicate the directory information successfully.
- To ensure efficient updates to the directory, a **preferred bridgehead server** must have the processing power and bandwidth to efficiently compress, send, receive, and decompress replication data. Active Directory uses only one bridgehead server at any time. If the first preferred server becomes unavailable, and others have been designated, another one on the preferred list is used.

Follow the steps below to designate a preferred bridgehead server:

- Open Active Directory Sites and Services.
- In the console tree, right-click the domain controller that you want to make a preferred bridgehead server, and then click **Properties**. To accomplish this open Active Directory Sites and Services, choose Sites then click on the *Site that contains the domain controller that you want to make a preferred bridgehead server*.
- Choose Servers and right click *The domain controller that you want to make a preferred bridgehead server.* Choose **Properties**.
- On the **General** tab, click the intersite transport or transports for which this computer will be a preferred bridgehead server, and then click **Add**. See *Figure 10* below.
- You can establish preferred bridgehead servers for one or more protocols (such as IP or SMTP).
- To perform this procedure, you must be a member of the *Domain Admins* group (in the domain of the selected domain controller) or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.


I8500 Properties
General
Object
Security
Description:
Transports available for inter-site data transfer:
This server is a preferred bridgehead server for the following transports:
Add >>
<< Remove
Computer
OK
Cancel
Apply

I8500

Transports available for inter-site data transfer: IP, SMTP

Computer: I8500

Domain: home.mydomain.com

Figure 10 – Configuring a bridgehead server

Plan an administrative delegation strategy

Why should you do all the work yourself? With decentralized management you can let other assistant administrators do part of your job for you. Here's how:

- Active Directory supports decentralized management. You can assign permissions and grant user rights in very specific ways. For example, you can delegate administrative privileges for certain objects to various departments in an organization.
- You can **delegate** the assigning of permissions:
  - For specific organizational units to different domain local groups. For example, delegating the permission Full Control for the Sales organizational unit.
  - To modify specific attributes of an object in an organizational unit. For example, assign the permission to change the name, address, and telephone number and to reset passwords on a user account object.
  - To perform the same task, such as resetting passwords, in all organizational units of a domain.

Plan an Organizational Unit (OU) structure based on delegation requirements

Organizational units are perfect objects to use to grant an assistant the rights to manage that section of the network. Listed below are several important considerations:

- Forest owners are responsible for creating organizational unit designs for their domains. Creating an OU design involves designing the OU structure, assigning the OU owner role, and creating account and resource OUs. Initially, design your OU structure to enable delegation of administration. When the OU design is complete, you can create additional OU structures for the application of Group Policy to the users and computers and to limit the visibility of objects. *Figure 11* shows the process for creating an organizational unit design.

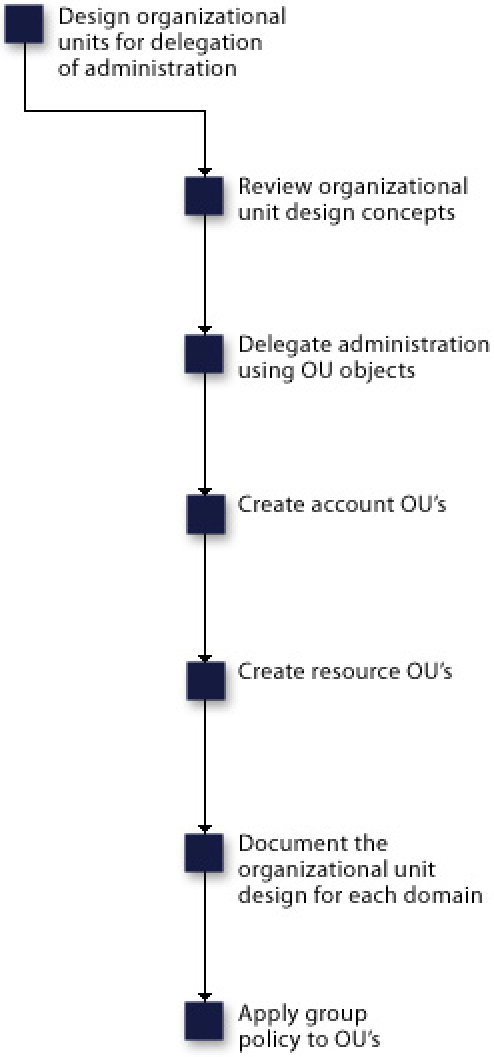

Design organizational units for delegation of administration
Review organizational unit design concepts
Delegate administration using OU objects
Create account OU's
Create resource OU's
Document the organizational unit design for each domain
Apply group policy to OU's

Figure 11 – Recommended process for planning an OU structure

- You can design your **OU** structure to delegate administration to individuals or groups within your organization that require the autonomy to manage their own resources and data. Microsoft recommends always delegating authority to a group not an individual. OUs represent administrative boundaries and enable you to control the scope of authority of data administrators.
- When you **delegate control** and allow a user or group to create objects in Active Directory, you allow them to create an unlimited number of objects. Microsoft Windows® Server 2003 has a new quotas feature that can be used to determine and limit the number of objects that can be owned in a directory partition (usually a domain) by a security principal. Quotas can help prevent a denial-of-service attack, which can occur if a security principal accidentally, or intentionally, creates objects until the affected domain controller runs out of storage space.
- **Quotas** are specified and administered for each *Active Directory partition* separately. The *schema partition*, however, has no quotas. On a given directory partition, you can assign quotas for any security principal, including users, inetOrgPersons, computers, and groups. Members of the Domain Admins and Enterprise Admins groups are exempt from quotas. In some situations, a security principal might be included in multiple quotas. For example, a user might be assigned an individual quota, and also belong to one or more security groups that also have quotas that are assigned to them. In such circumstances, the effective quota is the maximum (largest amount) of the quotas that are assigned to the security principal.
- If a security principal is not assigned a quota either directly or through a group membership, a **default quota** on the partition manages the security principal. If you do not explicitly set the default quota on a given partition, the default quota of that partition is *unlimited*, which means that there is no limit to the number of objects that can be owned by a security principal.
- **Tombstone** objects that are owned by a security principal are also counted as part of the quota consumption of that security principal. A tombstone object is an object that has been removed from Active Directory but has not yet been deleted. For each partition, you can specify a tombstone quota factor to determine the percentage weight that is given to a tombstone object in quota accounting. For example, if the tombstone quota factor for a given partition is set to 25 (or 25 percent), then a tombstone object on the partition is counted as 0.25 of a normal object. If a quota of 100 is specified for a user on this partition, then the user can own a maximum of 100 normal objects, or a maximum 400 tombstone objects. The default tombstone quota factor for each partition is initially set to 100 (or 100 percent); meaning that normal and tombstones objects are weighted equally.
- Only **domain controllers** that are running Windows Server 2003 can enforce quotas. Quotas are enforced only on originating directory operations; quotas are not enforced on replicated operations. For quotas to be fully effective for a given directory partition, all of the domain controllers that contain a writable copy of that partition must be running Windows Server 2003. Therefore, for quotas to be effective on a domain directory partition, all of the domain controllers in that domain must be running Windows Server 2003. For quotas to be effective on the configuration partition, all domain controllers in the forest must by running Windows Server 2003. Use **dsadd** quota to configure quotas, **dsmod** quota to modify quotas, and **dsquery** quota to view quota usage.

Plan a security group hierarchy based on delegation requirements

If you are delegating management you have to be careful of the security privileges you are giving away. Here are some tips:

- By delegating administration, you can assign a range of administrative tasks to the appropriate users and groups. You can assign basic administrative tasks to regular users or groups, and leave domain-wide and forest-wide administration to members of the Domain Admins and Enterprise Admins groups. By delegating administration, you can allow groups within your organization to take more control of their local network resources. You also help secure your network from accidental or malicious damage by limiting the membership of administrator groups.
- Delegate administration carefully and document all your delegated assignments. Before you delegate any tasks, ensure adequate training for users who will be assigned administrative control of objects.
- Use Microsoft Management Console (**MMC**) options to create a limited-use version of a snap-in such as Active Directory Users and Computers. This allows administrators to control the options available to groups to whom you have delegated administrative responsibilities by restricting access to operations and areas within that customized console.
- There are three types of **security groups** that can be used for delegation requirements: **domain local, global, and universal**:
    - Domain local groups
        - Use this group type when you are delegating authority for a specific domain controller.
    - Global groups
        - Use this group type when you are delegating authority for a specific OU within a single domain.
    - Universal groups
        - Use this group type when you are delegating authority to users that belong to different global groups within a domain or forest.

Managing and Maintaining an Active Directory Infrastructure

Manage an Active Directory forest and domain structure

As you create a network with multiple domains, and perhaps multiple forests, make sure that users can access resources. When a user gets to use a resource in another container, there is a trust relationship involved.

Manage trust relationships

While transitive **two-way trust relationships** are created between domains, there are times when an administrator must step in and manage trusts. Here are more details.

Management tasks associated with **trusts** include:

- Creating a (normal) two-way trust, **shortcut** trust, **external** trust, or **realm** trust.
- Verifying a trust.
- Removing a trust.
- Selecting or modifying the scope of authentication for users.
- Manage **forest trusts**:
    - Creating a forest trust.
    - Changing the routing status of a UPN name suffix.
    - Enabling or disabling an existing name suffix from routing.
    - Excluding name suffixes from routing to a local forest.

Two tools are used for all management trust activities:

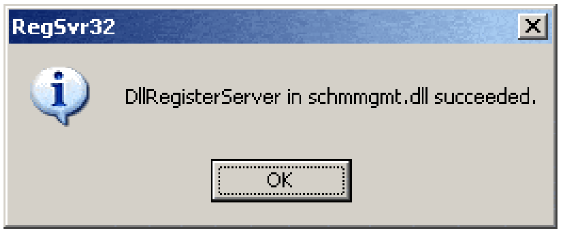
- Active Directory Domains and Trusts.
- The system command **netdom trust.**
    - To view the complete syntax for this command, at a command prompt, type: **netdom trust | more**

Manage schema modifications

It is important to remember that there is only one **schema** per forest. All schema changes are replicated throughout the entire forest. Here are other pointers about schema modifications:

- Windows Server 2003 Active Directory implementation offers the ability to *deactivate* **schema attributes**, allowing custom-built applications to use custom attributes without fear of conflict. In addition, attributes can be deactivated to reduce replication traffic.

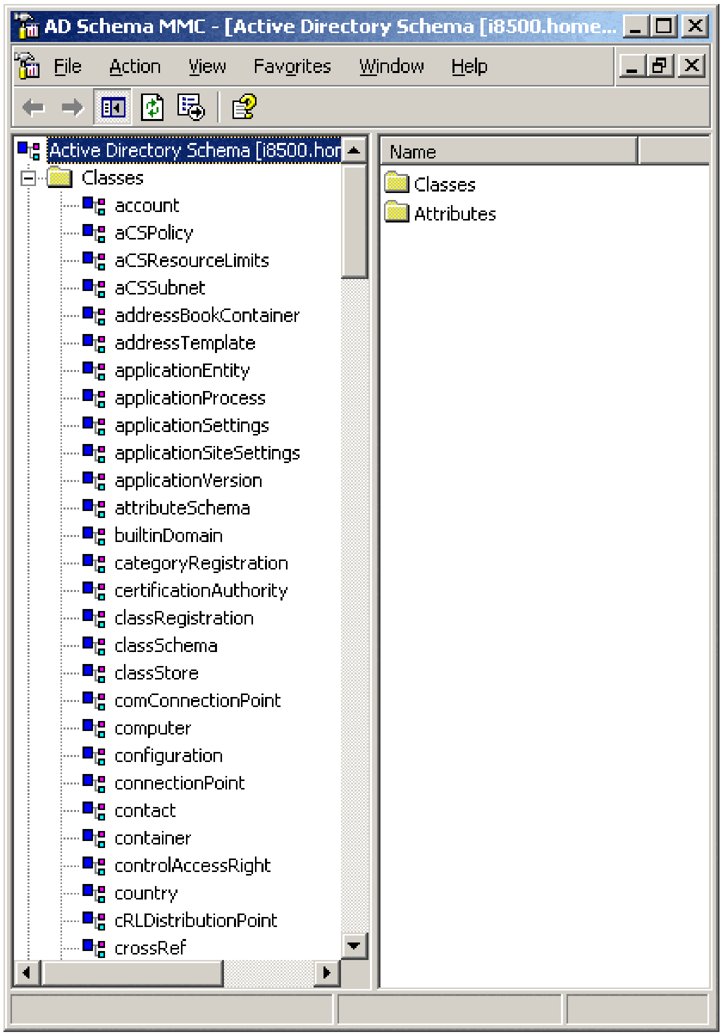
- You cannot deactivate default schema attributes or classes in the base schema. Only attributes or classes that are added as extensions to the base schema can be deactivated.
- Attributes can be *reactivated*, if necessary.
- Use the **Active Directory Schema MMC Snap-in** to make modifications to the Active directory schema. Follow the steps below to install the Active Directory Schema snap-in:
  - Open a Command Prompt.
  - Type: **regsvr32 schmmgmt.dll.** This command will register schmmgmt.dll on your computer.



DllRegisterServer in schmmgmt.dll succeeded.

Figure 12 – Registering schmmgmt.dll

- Click **Start**, click **Run**, type **mmc /a**, and then click **OK**.
- On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
- Under **Snap-in**, double-click **Active Directory Schema**, click **Close**, and then click **OK**. The AD Schema MMC displaying the Classes Objects is shown in *Figure 13*.
- To perform this procedure on a domain controller, *you must be a member of the Domain Admins group or the Enterprise* Admins group in Active Directory, or you must have been delegated the appropriate authority.



Active Directory Schema [i8500.hor

Classes

account
aCSPolicy
aCSResourceLimits
aCSSubnet
addressBookContainer
addressTemplate
applicationEntity
applicationProcess
applicationSettings
applicationSiteSettings
applicationVersion
attributeSchema
builtinDomain
categoryRegistration
certificationAuthority
classRegistration
classSchema
classStore
comConnectionPoint
computer
configuration
connectionPoint
contact
container
controlAccessRight
country
cRLDistributionPoint
crossRef

Classes
Attributes

Figure 13 – the Active Directory Schema MMC Snap-in

You can also run the **Active Directory Schema snap-in** from a computer running Windows XP Professional. Simply install the Windows Server 2003 Administration Tools Pack on the computer, and then complete step 9 above. For more information about the Administration Tools Pack, see the article mentioned in Cramsession References.

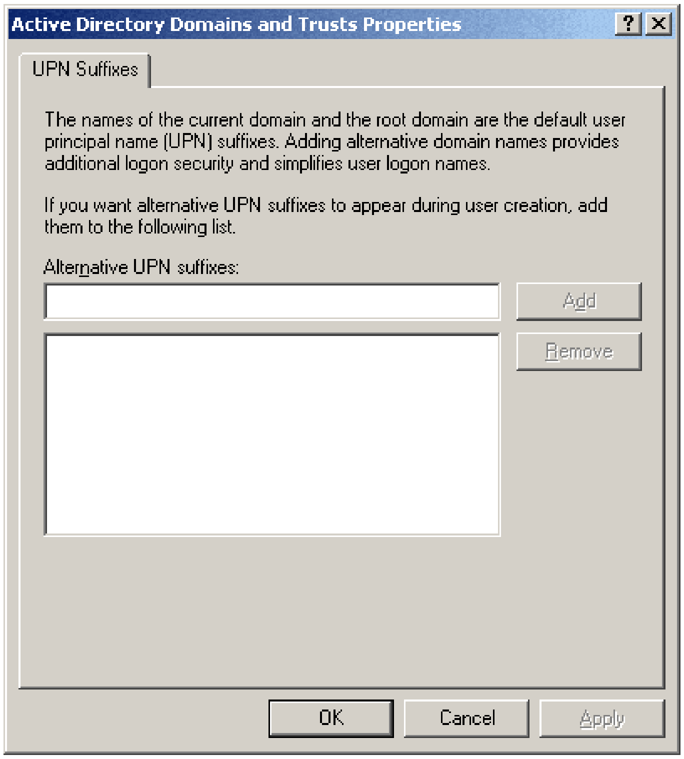
Note: Modifying the schema is an advanced operation that should not be taken lightly and requires careful planning.

Note: The Windows Server 2003 Administration Tools Pack cannot be installed on computers running Windows 2000 Professional or Windows 2000 Server.

Add or remove a UPN suffix

UPN stands for a **User Principal Name**.
To add user principal name suffixes (UPN), follow these steps:

- Open Active Directory Domains and Trusts.
- In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Properties**.
- On the *UPN Suffixes* tab, type an *alternative UPN suffix* for the forest in the text box, and then click **Add**. See *Figure 14* below.
- Repeat the above step to add additional alternative user principal name suffixes.
- To perform this procedure, you must be a member of the *Domain Admins* group (in the forest root domain) or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.



The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

Figure 14 – Adding or removing Active Directory UPN Suffixes

- UPN suffixes should conform to DNS conventions for valid characters and syntax.

Manage an Active Directory site

After you have created an Active Directory site, understand how replication traffic will occur by noting the following.

- Active Directory handles replication within a site, or **intrasite** replication, differently than replication between sites because bandwidth within a site is more readily available. The Active Directory Knowledge Consistency Checker (**KCC**) builds the intrasite replication topology using a bi-directional ring design. Intrasite replication is optimized for speed, and directory updates within a site occur automatically on the basis of change notification. Unlike replication data traveling between sites, directory updates replicated within a site are not compressed.
- Replication between sites, or **intersite** replication, is different because bandwidth between sites is usually limited. The Active Directory Knowledge Consistency Checker (**KCC**) builds the intersite replication topology using a least-cost spanning tree algorithm. Intersite replication is optimized for bandwidth efficiency, and directory updates between sites occur automatically based on a configurable schedule. Directory updates replicated between sites are compressed to preserve bandwidth.

Configure replication schedules

Replication means moving data across otherwise busy wide area network links. You can minimize network disruptions to your users by scheduling the replication to occur during off hours.
Follow the steps below to configure site link replication *frequency*:

- Open Active Directory Sites and Services.
- In the console tree, click the inter-site transport folder that contains the site link you want to configure. To get there, open Active Directory Sites and Services, choose Sites, select Inter-Site Transports and then open the *inter-site transport folder that contains the site link you want to configure*.
- In the details pane, right-click the site link whose replication frequency you want to set, and then click **Properties**.
- In **Replicate every**, type the number of minutes between replications.
- To perform this procedure, you must be a member of the *Domain Admins* group (in the forest root domain) or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.
- The **default site link replication frequency** is 180 minutes.
- The **Replicate every** value will be processed as the nearest multiple of 15 ranging from a minimum of 15 to a maximum of 10,080 minutes, which corresponds to one week.

Configure site link costs

The **cost** of a site link determines the relative preference of the Active Directory Knowledge Consistency Checker (**KCC**) for using a site link in the replication topology. The higher the cost of the site link, the lower will be the KCC's preference for using the site link. For example, if you have two site links, site link A and site link B, and you set the cost of site link A to 150 and the cost of site link B to 200, the KCC will prefer to use site link A in the replication topology. By default, the cost of a newly created site link is 100.
Follow the steps below to configure **site link cost**:

- Open Active Directory Sites and Services.
- In the console tree, click the inter-site transport folder that contains the type of link you are going to configure. To get here, open the MMC Active Directory Sites and Services, open Sites, choose Inter-Site Transports and open the *inter-site transport folder that contains the type of link you are going to configure*.
- In the details pane, right-click the site link whose cost you want to set, and then click **Properties**.
- In **Cost**, enter a value for the cost of replication.
- To perform this procedure, you must be a member of the *Domain Admins* group (in the forest root domain) or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.

The Active Directory Knowledge Consistency Checker (**KCC**) considers a site link with a higher cost to be less desirable than a site link with a lower cost. When multiple paths for replication are available, the *KCC prefers the site link with the lower cost*.

Note: You cannot apply costs directly to site link bridges.

Configure site boundaries

With Windows Server 2003, site boundaries can now be based on Active Directory site names, rather than on Internet Protocol (IP) subnets.

Generally, sites are defined according to high-bandwidth connectivity. If possible, sites should contain local network services such as domain controllers, global catalog servers, DNS servers, DHCP servers, and WINS servers (if necessary). This will ensure that the local site will remain functional if network connectivity between sites is disrupted.

Use the Active Directory Sites and Services Administrative Tool to configure sites.

Monitor Active Directory replication failures. Tools include Replication Monitor, Event Viewer, and support tools

To begin, open **Active Directory Domains and Trusts** to view the *logical* structure of Active Directory. To do so, perform the following steps:

- Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
- In the left pane, expand the node that represents the forest-root domain to view the domains that make up the logical structure of Active Directory.

Open **Active Directory Sites and Services** and view the *physical* structure of Active Directory. To do so, perform the following steps:

- Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.

- In the console tree, expand Sites, and then expand the folder that represents the site for which you want to view a list of servers.
- Click Servers Folder to view a list of servers in the right pane.

Monitor Active Directory replication

Before you start the monitoring process, you need to determine when **intersite** replication actually occurs:

- Active Directory preserves bandwidth between sites by minimizing the frequency of replication and by allowing you to schedule the availability of site links for replication. By default, **intersite** replication across each site link occurs every 180 minutes (3 hours). You can adjust this frequency to match your specific needs. Be aware that increasing this frequency increases the amount of bandwidth used by replication. In addition, you can schedule the availability of site links for use by replication. By default, a site link is available to carry replication traffic 24 hours a day, 7 days a week. You can limit this schedule to specific days of the week and times of day. You can, for example, schedule intersite replication so that it only occurs after normal business hours.

Determining when **intrasite** replication occurs:

- Directory updates made within a site are likely to have the most direct impact on local clients, so intrasite replication is optimized for speed. Replication within a site occurs automatically on the basis of change notification. Intrasite replication begins when you make a directory update on a domain controller. By default, the source domain controller waits 15 seconds and then sends an update notification to its closest replication partner. If the source domain controller has more than one replication partner, subsequent notifications go out by default at 3-second intervals to each partner. After receiving notification of a change, a partner domain controller sends a directory update request to the source domain controller. The source domain controller responds to the request with a replication operation. The 3-second notification interval prevents the source domain controller from being overwhelmed with simultaneous update requests from its replication partners.
- For some directory updates in a site, the 15-second waiting time does not apply and replication occurs immediately. Known as *urgent* replication, this immediate replication applies to critical directory updates, including the assigning of account lockouts and changes in the account lockout policy, the domain password policy, or the password on a domain controller account.

It is important to monitor replication regularly to help identify and fix problems before they grow. **Repadmin.exe** and **dcdiag.exe** (Windows Support Tools) and the **directory service event log** (in Event Viewer) are the primary tools for monitoring replication.

Here are more details:

- **Repadmin** is a command-line tool that reports failures on a replication link between two replication partners. The following **repadmin** example displays the replication partners and any replication link failures for *Server1* on the *mydomain.com* domain:
    - repadmin /showreps server1.mydomain.com
    - For a complete list of **repadmin** options, use the ? option: **repadmin /?**

- **Dcdiag** is a command-line tool that can check the DNS registration of a domain controller, check to see that the security descriptors (SIDs) on the naming context heads have appropriate permissions for replication, analyze the state of domain controllers in a forest or enterprise, and more. The following **dcdiag** example checks for any replication errors between domain controllers:
    - dcdiag /test:replications
    - For a complete list of **dcdiag** options, use the ? option: **dcdiag /?**
- The directory service log reports replication errors that occur after a replication link has been established and lists them in the Event Viewer Directory Service.
- If you have the 2003 Resource Kit, you can use **gpotool.exe** to check Group Policy object replication. It reads the Group Policy object instances from each domain controller and compares them (selected GPC properties and full recursive compare for GPT).
- Large enterprises may also want to use the Microsoft Operations Manager for automated monitoring of large numbers of domain controllers.

Monitor File Replication service (FRS) replication

File Replication Service (**FRS**) is the replication engine used by Windows Server 2003 to keep **Distributed File System** (**DFS**) shares synchronized. FRS is also used by the operating system to replicate the contents of the **SYSVOL** folder in domain controllers and is integral to the domain controller advertising itself. In either scenario, it is important to ensure that the service is functioning properly and that replicated content is in a consistent state. There are a number of tools for managing FRS, including both continuous monitoring tools such as Ultrasound and Sonar and snapshot troubleshooting tools such as FRSDiag.

The **File Replication Service Diagnostics** Tool (FRSDiag.exe) provides a graphical interface to help troubleshoot and diagnose problems with the File Replication Service (**FRS**). FRSDiag helps to gather snapshot information about the service, perform automated tests against that data, and compile an overview of possible problems that may exist in the environment.

Lastly, another way to check for information about FRS is to go to Administrative Tools, Event Viewer, and check events listed under File Replication Service.

Restore Active Directory services

When an undesired change happens in Active Directory or the Active Directory database has become corrupted on a domain controller, it is often necessary to restore the Active Directory database. There are two ways to restore the Active Directory database: **authoritative** and **nonauthoritative**.

- When an undesired change has been made in Active Directory, for example, an Admin assistant accidentally deletes an OU object, and the database needs to be rolled back, an authoritative restore (**primary** restore) should be performed.
- When a domain controller is rebuilt from backup, or if its copy of the Active Directory database has become corrupted, a nonauthoritative restore (**normal** restore) should be performed.

Backup copies of the Active Directory database should not be used if they are older than the Active Directory Tombstone Lifetime (default is 60 days). Restoration of a backup older than the tombstone lifetime may cause the restored domain controller to have objects that will not be replicated on other domain controllers.

Perform an authoritative restore operation

To authoritatively restore Active Directory data, you need to run the **Ntdsutil** utility after you have restored the **System State** data but before you restart the server. The **Ntdsutil** utility lets you mark Active Directory objects for authoritative restore. When an object is marked for authoritative restore, its update sequence number is changed so that it is higher than any other update sequence number in the Active Directory replication system. This will ensure that any replicated or distributed data that you restore is properly replicated or distributed throughout your organization.

Distributed Data	Reason for using Authoritative Restore of System State Data
Active Directory	Rolling back or undoing changes.
SYSVOL	Resetting data.
Replica Sets	Rolling back or undoing changes.

The difference between doing an Active Directory restore and a replica set restore is that with the Active Directory restore you are restoring all of Active Directory, while with the Replica Set, you are restoring a replica of a partition, or a part of Active Directory.

Follow the steps below to perform an **authoritative restore** of the Active Directory database:

- Power up the domain controller and press the **F8** key when the boot loader screen is displayed.
- Select **Directory Services Restore Mode** from the advanced menu boot options and press **Enter**. Using this mode does not start the Active Directory Service and boots the Active Directory database in an offline state.
- After the server boots, log in using the Administrator username and the Restore mode password (specified when the server was promoted to a domain controller).
- Go to Start, Run and type **Ntbackup.exe** and press **Enter**.
- When the Backup/Restore windows opens, select **Advanced Mode**.
- Select the **Restore and Manage Media** tab.
- Select the appropriate backup media, expand it, and check the system state check box.
- Choose to restore the data to the original location and click **Start Restore**.
- When the pop-up window appears, indicating that restoring the system state to the original location will overwrite the current system state, click **OK**.
- A pop-up window will appear allowing you to choose advanced restore options, click **OK** to continue.
- When the restore is complete the system will prompt you to restart the system. Because this is an authoritative restore, click **No**.
- Close the Backup window and go to Start, Run and go to a command prompt.

- Type **ntdsutil.exe** and press **Enter**.
- Type **Authoritative restore** and press **Enter**.
- Type **Restore Database** and press **Enter**.
- An authoritative restore confirmation dialog box will appear, click **Yes** to start the authoritative restore.
- The command prompt window will display whether the authoritative restore was successful or not. If successful, close the command prompt and reboot the server.
- To *verify* that the restore was successful, log in to the server in Normal mode and use the Active Directory tools to check the database. Also, check other domain controllers to ensure that the restored data is being replicated to them.

Perform a nonauthoritative restore operation

During a normal restore operation, the backup operates in nonauthoritative restore mode. That is, any data that you restore, including Active Directory objects, will have their original update sequence number. The Active Directory replication system uses this number to detect and propagate Active Directory changes among the servers in your organization. Because of this, any data that is restored nonauthoritatively will appear to the Active Directory replication system as though it is old, which means the data will never get replicated to your other servers. Instead, if newer data is available from your other servers, the Active Directory replication system will use this to update the restored data. To replicate the restored data to the other servers, you must use an authoritative restore.

Distributed Data	Reason for using Normal Restore of System State Data
Active Directory	Restoring a single domain controller in a replicated environment.
SYSVOL	Restoring a single domain controller in a replicated environment.
Replica Sets	Restoring all but the first replica sets (that is, sets 2 through *n*, for *n* replica sets). Note: If you had to restore the first replica set, you would have to reinstall Active Directory.

Follow the steps below to perform a **nonauthoritative restore** of the Active Directory database:

- Power up the domain controller and press the **F8** key when the boot loader screen is displayed.
- Select **Directory Services Restore Mode** from the advanced menu boot options and press **Enter**. Using this mode does not start the Active Directory Service and boots the Active Directory database in an offline state.
- After the server boots, log in using the Administrator username and the Restore mode password (specified when the server was promoted to a domain controller). This may or may not be the Administrator password.
- Go to Start, Run and type **Ntbackup.exe** and press **Enter**.

- When the Backup/Restore windows opens, select **Advanced Mode**.
- Select the **Restore and Manage Media** tab.
- Select the appropriate backup media, expand it, and check the system state check box.
- Choose to restore the data to the original location and click **Start Restore**.
- When the pop-up window appears indicating that restoring the system state to the original location will overwrite the current system state, click **OK**.
- A pop-up window will appear allowing you to choose **advanced restore options**, including things like restoring security settings, restoring volume mount points and restoring replicated data sets. These are things you probably don't want to change so just click **OK** to continue.
- When the restore is complete the system will prompt you to restart the system. Because this is a nonauthoritative restore, click **Yes** to restart the server.
- Log in as a Domain Administrator after the server reboots. Check the Event log and the Active Directory information by using the Active Directory tools to ensure that the database has been restored successfully.

Troubleshoot Active Directory

There are many new command line tools for Windows Server 2003, many of which can be used to monitor and troubleshoot Active Directory.

Diagnose and resolve issues related to Active Directory replication

Monitoring AD replication regularly is a good way to determine the normal replication latency on your network. With this knowledge, you can more easily determine if a problem is occurring.
Review the directory service log for any recent replication errors. Also, run **repadmin /showreps** and review any resulting errors.
Some common replication problems and their solutions are listed below:

- Received Event ID 1311 in the directory service log.
- Common *causes* of **Event ID 1311** include:
    - One or more domain controllers are offline.
    - **Bridgehead** servers are online but experiencing errors replicating a required naming context between Active Directory sites.
    - **Preferred bridgehead** servers defined by administrators are online but do not host the required naming contexts.
    - One or more sites are not contained in **site links**.
    - Site links contain all sites but the site links are not all *interconnected*.
    - Preferred bridgeheads defined by the administrator are offline.

- *Solutions* for **Event ID 1311** include:
    - Make sure all sites belong to at least one site link.
    - Make sure that the combination of site links you have created allows a path between all domain controllers containing a replica of a given directory partition. For example, if a directory partition is held by domain controllers in both Site A and Site C, make sure that Site A and Site C belong to a common site link, or that an intermediary site exists that has at least one site link in common with Site A and at least one site link in common with Site B.
    - Make sure that you have cleared the **Bridge all site links** check box in Active Directory Sites and Services if your network is not fully routed. Or, if your network is fully routed and you have cleared the **Bridge all site links** check box, you may need to select it again to allow full replication of a directory partition.
    - If you have manually assigned preferred bridgehead servers, make sure these servers are not offline. (It is generally recommended that you allow Active Directory to select bridgehead servers automatically.)
    - Use **Ping.exe** and Network Monitor to verify connectivity through WAN links and across routers.
- Received **Event ID 1265** "Access denied," in the directory service log. Or, received "Access denied" from the **repadmin** command.
- This error can occur if the local domain controller failed to authenticate against its replication partner when creating the replication link or when trying to replicate over an existing link. This typically happens when the domain controller has been disconnected from the rest of the network for a long time and its computer account password is not synchronized with its computer account password stored in the directory of its replication partner.
- Solution:
    - Stop the Key Distribution Center (**KDC**) service using **net stop KDC**.
    - Purge the ticket cache on the local domain controller.
    - Reset the domain controller's account password on the primary domain controller (PDC) emulator master using **netdom /resetpwd**. (**Netdom.exe** is available in Windows Support Tools).
    - Synchronize the domain directory partition of the replication partner with the PDC emulator master .
    - Manually force replication between the replication partner and the PDC emulator master.
    - Start the Knowledge Consistency Checker (**KCC**) on the local domain controller: **net start KDC**.

Diagnose and resolve issues related to Operations Master (OM) role failure

Some of the **operations master roles** are crucial to the operation of your network. Others can be unavailable for quite some time before their absence becomes a problem. Generally, you will notice that a single master operations role holder is unavailable when you try to perform some function controlled by the particular operations master. As a rule, network users will be unaware of any problems with operations masters. Here are more pointers:

- If an operations master is not available due to computer failure or network problems, you can **seize** the operations master role. This is also referred to as forcing the transfer of the operations master role. Do not seize the operations master role if you can transfer it instead. Transferring implies the computer holding the Operations Master Role is available. Seizing will not be available if you are going to move the role to another computer. Before forcing the transfer, first determine the cause and expected duration of the computer or network failure. If the cause is a networking problem or a server failure that will be resolved soon, wait for the role holder to become available again. If the domain controller that currently holds the role has failed, you must determine if it can be recovered and brought back online.
- In general, seizing an operations master role is a *drastic* step that should be considered only if the current operations master will never be available again. The decision depends upon the role and how long the particular role holder will be unavailable. A domain controller whose operation master role has been seized must *never* be brought back online.
- To seize an operations master role, use the **ntdsutil** command. To perform this procedure, you must be a member of the *Domain Admins* group (in the forest root domain) or the *Enterprise Admins* group in Active Directory, or you must have been delegated the appropriate authority.

Diagnose and resolve issues related to the Active Directory database

You can download a script to add performance counters to a domain controller to monitor the performance of Active Directory. You can review error log entries in the Event Viewer under Directory Service. Active Directory Management tools supplied with the Windows Server 2003 Support Tools toolkit are described in the following table:

Executable	**Name**	**Function**
Acldiag.exe	ACL Diagnostics	This command-line tool detects and reports discrepancies in the access control lists (ACLs) of objects in Active Directory. It can also reapply a security delegation template to an ACL, eliminating special permissions and restoring incomplete delegations. With AclDiag, you can: - Display the access control entries (ACEs) in the ACL, and inheritance and audit settings. - Display the effective permissions of users and groups to an Active Directory object. - Compare the ACL for an object in Active Directory to the default permissions defined in the schema. - Compare the ACL of an Active Directory object to a delegation template. - Reapply the delegation template to the ACL of an Active Directory object.
Adsiedit.msc	ADSI Edit	This GUI tool is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for Active Directory. Network administrators can use Active Directory Service Interfaces (ADSI) for common administrative tasks such as adding, deleting, and moving objects with a directory service. Attributes for each object viewed can be changed or deleted. Many of the features of ADSIEdit are similar to the Active Directory Users and Computers snap-in, but ADSIEdit provides a much lower-level view of Active Directory information.
Dcdiag.exe	Domain Controller Diagnostic Tool	This command-line tool analyzes the state of domain controllers in a forest or enterprise and reports any problems to assist in troubleshooting. As an end-user reporting program, DCDiag encapsulates detailed knowledge of how to identify abnormal behavior in the system. DCDiag consists of a framework for executing tests and a series of tests to verify different functional areas of the system. This framework selects which domain controllers are tested according to scope directives from the user, such as enterprise, site, or single server.

Dsacls.exe	DsAcls	This command-line tool displays and changes permissions (access control entries) in the access control list (ACL) of objects in Active Directory. The ACEs that you add by using DsAcls must be object-specific permissions that override the default permissions defined in the Active Directory schema for that object type. Do not add ACEs unless you are well-informed about security for Active Directory objects. DsAcls is the command-line equivalent of the Security tab in the Properties dialog box for an Active Directory object in Active Directory tools, such as Active Directory Users and Computers. You can use either tool to view and change permissions to an Active Directory object.
Dsastat.exe	Directory Services Utility	This command-line diagnostic tool compares and detects differences between naming contexts on domain controllers. DsaStat can be used to compare two directory trees across replicas within the same domain or, in the case of a global catalog, across different domains. The tool retrieves capacity statistics such as megabytes per server, objects per server, and megabytes per object class, and performs comparisons of attributes of replicated objects. The user specifies the targeted domain controllers and additional operational parameters from the command line. DsaStat determines whether domain controllers in a domain have a consistent and accurate image of their own domain. In the case of Global Catalogs, DsaStat checks to see if the Global Catalog has a consistent image with domain controllers in other domains. As a complement to the replication-monitoring tools, Repadmin and Replmon, DsaStat can be used to ensure that domain controllers are up to date with one another.
Ldp.exe	LDP Tool	This GUI tool is a Lightweight Directory Access Protocol (LDAP) client that allows users to perform operations (such as connect, bind, search, modify, add, delete) against any LDAP-compatible directory, such as Active Directory. LDP is used to view objects stored in Active Directory along with their metadata, such as security descriptors and replication metadata. LDP is a GUI-based, Windows Explorer–like utility with a scope pane on the left that is used for navigating through the Active Directory namespace, and a details pane on the right that is used for displaying the results of the LDAP operations. Any text displayed in the details pane can be selected with the mouse and "copied" to the Clipboard.

Sdcheck.exe	Security Descriptor Check Utility	This command-line tool displays the security descriptor for any object stored in Active Directory. The security descriptor contains the access control lists (ACLs) defining the permissions that users have on objects stored in Active Directory. To enable administrators to determine the effective access controls on an object, SDCheck also displays the object hierarchy and any ACLs that are inherited by the object from its parent. As changes are made to the ACLs of an object or its parent, Active Directory propagates these changes automatically. SDCheck displays the security descriptor propagation metadata, so that administrators can monitor these changes with respect to propagation of inherited ACLs, as well as replication of ACLs from other domain controllers. As a complement to the replication monitoring tools (Repadmin.exe and Replmon.exe), SDCheck can be used to ensure that domain controllers are up-to-date with one another.
Search.vbs	Active Directory Search Tool	This command-line tool performs searches against a Lightweight Directory Access Protocol (LDAP) server. An Administrator or any user who wants to get information from Active Directory can use it. All search criteria are taken from the command line. However, modifying variable values in the script can only change certain properties of the search, such as the page size.
Setspn.exe	Manipulate Service Principal Names for Accounts	This command-line tool allows you to read, modify and delete the Service Principal Names (SPN) directory property for an Active Directory service account. SPNs are used to locate a target principal name for running a service. SetSpn allows you to view the current SPNs, reset the account's default SPNs, and add or delete supplemental SPNs. It is not usually necessary to modify SPNs. A computer sets them up when it joins a domain and when services are installed on the computer. In some cases, however, this information can become stale. For instance, if the computer name is changed, the SPNs for installed services would need to be changed to match the new computer name. Also, some services and applications may require manual modification of a service account's SPN information to correctly authenticate.

The following command-line tools can be used to *manage* Active Directory:

Tool	**Function**
Csvde	Import and export Active Directory data using comma-separated format.
Dsadd	Add users, groups, computers, contacts, and organizational units to Active Directory.
Dsmod	Modify an existing object of a specific type in the directory. The types of objects that can be modified are: users, groups, computers, servers, contacts, and organizational units.
Dsrm	Remove objects of the specified type from Active Directory.
Dsmove	Rename an object without moving it in the directory tree, or move an object from its current location in the directory to a new location within a single domain controller. (For cross-domain moves, use the Movetree command-line tool.)
Movetree	Used to move objects such as users and organizational units between domains in a single forest.
Dsquery	Query and find a list of objects in the directory using specified search criteria. Use in a generic mode to query for any type of object or in a specialized mode to query for selected object types. The specific types of objects that can be queried through this command are: computers, contacts, subnets, groups, organizational units, sites, servers and users.
Dsget	Display selected attributes of specific object types in Active Directory. Attributes of the following object types can be viewed: computers, contacts, subnets, groups, organizational units, servers, sites, and users.
Ldifde	Create, modify, and delete directory objects. This tool can also be used to extend the schema, export Active Directory user and group information to other applications or services, and populate Active Directory with data from other directory services.
Ntdsutil	General purpose Active Directory management tool. Use Ntdsutil to perform database maintenance of Active Directory, to manage single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.

Planning and Implementing User, Computer, and Group Strategies

Proper planning prevents poor performance. In this case, proper planning prevents users from whining. Proper placement of user accounts, computer accounts and the groups they belong too will not only enhance authentication but will ripple through the system when it comes to things like group policies and file replication.

Plan a security group strategy

Create groups of users or computers to make it easier to administer a large number of similar objects. It is easier to assign rights and permissions to large numbers of objects grouped together into a single group than it is to make the same assignments individually to each object.

Types of Security Groups

Depending on the functional level of the Windows Server 2003 Active Directory network, there can be four types of groups: Local Groups, Domain Local Groups, Global Groups and Universal Groups.

Local Groups
Local groups are not germane to this discussion. Created on the local computer, these groups include default groups like the Power Users group on a Windows Server 2003 computer and other groups as needed. While these groups provide permissions to those people who physically authenticate to the computer, these groups are not part of the Active Directory Design and Implementation.

Domain Local Group
As the name implies, these groups are created at the domain level. These groups can contain universal groups, global groups and accounts from any domain in the forest. These groups can also contain other domain local groups from its own domain. Domain local groups are assigned rights and permissions at the domain level.

Global Group
Global Groups can contain users, groups and computers from its own domain.
The global group, however, receives rights and permission for any resource in any domain in the forest.

Universal Group
Universal groups can contain users, groups and computers from any domain in its forest.
Rights and permissions are assigned to universal groups for any resource in any domain in the forest.
Universal groups are only available in the Windows Server 2003 domain functional level.
Use universal groups sparingly to decrease network traffic.

Group Nesting
In Windows 2000 domain and Windows 2003 interim domain:

- Create domain local groups and assign rights and permissions
- Add global groups to domain local groups

In Windows Server 2003 functional level

- Add global groups to Universal Groups

Remember **A-G-U-DL-P**

- User **a**ccounts are added to **g**lobal group accounts. Global groups are added to **u**niversal groups. Universal groups are added to **d**omain **l**ocal groups and resource **p**ermissions are assigned to the domain local groups.

Management
The management of groups depends on several factors, including:

- The group's location within Forest
- Administrative concerns

Have you delegated responsibility for the group or container? If so, do you want the delegated administrator to rule the group? If you do not, then place the group outside that person's area of responsibility.

Plan a user authentication strategy

Each user account has certain attributes that you can use to control the user's network access. Some of these user attributes include:

- **Account Expiration** - Use account expiration to terminate an account. For example, assume your company hired part time employees to fill in during a June, July and August rush. You could expire the account on September 1st so the temporary users would be locked out of the network starting on that date.
- **Logon hours** - You may have users scheduled to work Monday through Friday, from 8 am to 5 pm and have no reason for them being in the office on the weekend. You may want to limit their logon hours from 7 am - 6 pm on Monday to Friday for security reasons.
- **Logon To** - Use this attribute to limit the workstations a user can access.
- **Enable/Disable** - Use this attribute to enable or disable a user logon account. You might disable a user logon account when the person goes on an extended leave like a maternity leave. Disabling the account prevents logon's but maintains the Security Identifier (**SID**) and group membership.
- **Locked out** - You can define how many attempts a user can make to logon to the network. If the user attempts to logon a number of times with an incorrect password, the account is locked. You can define how many incorrect logon attempts are necessary in what time period before the account becomes locked.
- **Must change password** - Use this setting to make sure that a user changes their password during the next logon.
- **Cannot change password** - Use this setting to make sure a logon account's password does not change. This setting is useful for computers in a **kiosk** environment or for a guest account.

- **Password never expires** - Use this setting to make sure a logon account's password does not expire. This setting is useful for computers in a **kiosk** environment or for a guest account, or for Windows services requiring an account.

Use user attribute settings to prevent you from having to delete a user account and recreate it. When you delete a user account, the **SID** is deleted. Recreating the user account will require you to reset all the security permissions.

Plan a smart card authentication strategy

A smart card is a credit card like device, similar to an ATM card, which works with a personal identification number to enable certificate-based authentication and single sign-on. Smart Cards work by securely storing certificates, public and private keys, and passwords.

Implementing Smart Cards
When you implement smart cards, you need **Public Key Infrastructure** (**PKI**) and each computer needs a smart card reader. In addition, one computer is designated a smart card enrollment station and has a user assigned to operate it.

The **certificate authority** (**CA**) server issues certificates. These certificates are based on certificate templates that are stored in Active Directory, and the **ACL** on the templates determine which users and which computers can request or configure certificates. The templates are accessed through Active Directory Sites and Services.

In order for a user to be able to enroll a smart card certificate for someone else, the operator must be granted an **enrollment agent** certificate. As the enrollment agent, the designated user can create smart cards on behalf of others.

Deploying Smart Cards
The cost of administering the program depends on:

- The number of users
- The number of ways smart cards are issued
- What you do to users who lose cards

Create a password policy for domain users

Creating a password policy assures all users are following the password guidelines determined for your organization.

The password policy includes password settings like:

- **Enforce Password History -** Enforcing password history remembers the user's last 24 passwords and thus helps prevent the reuse of older, expired passwords.
- **Maximum Password Age -** Determines the amount of time that expires before a user must change a password.

- **Minimum Password Age -** Determines the amount of time that must pass before a user may change a password. This prevents a user from changing their password multiple times in a single day, in order to use the same password again (i.e., as a way to circumvent "Enforce Password History").
- **Minimum Password Length -** Determines how long a password must be to be effective.
- **Must meet complexity requirements -** Password**:**
    - Must be at least seven characters long.
    - Does not contain a user name, real name or company name.
    - Does not contain a complete dictionary word.
    - Is significantly different from previous passwords.
    - Contains upper and lower case letters, numerals and symbols.
    - Contains extended ASCII characters.
    - Example: Iwnf@8cPW – "I will never forget an eight character PassWord".

Plan an OU structure

Organizational Units are powerful tools in an Active Directory infrastructure. They can be used to delegate administration and for the association of group policy objects.

Analyze the administrative requirements for an OU

Organizational Unit's are created for several reasons including:

- For administration purposes.
- For political purposes.
- To ease the administration of group policies.

To analyze the administrative requirements of an organizational unit, determine the user accounts and the group accounts that are being placed in the OU.

Keep in mind the main reason for creating an OU is for administration. This can be based on location (i.e., another office in another community with an IT staff present) or because the head of a department may want to manage his or her department's own resources.

For example, the head of the Development Team wants to be able to manage her users, groups, printers, etc.

- Create the OU for the Development Team.
- Move or create appropriate objects in the OU.
- Delegate Responsibility to the manager of the team.

Analyze the Group Policy requirements for an OU structure.

Group Policies are collection of user and computer configuration settings that can be linked to sites, domains and OU's to specify behavior of desktop configurations or security.

To create a specific configuration for a particular group of users or computers, put users or computers in a particular OU and link the GPO to the OU.

For example, in a school, you may have an OU for the Science Department and all computers in the Science Department will be configured the same way.

Look at the example below in *Figure 15*:

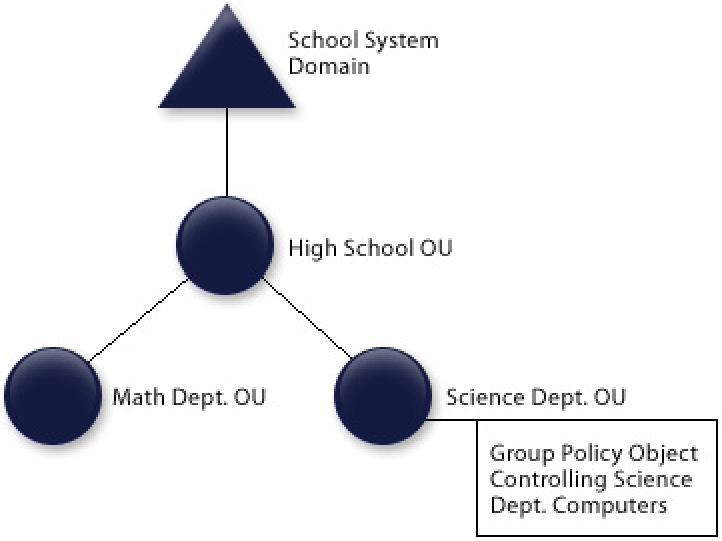


Figure 15 – Example OU Structure

Reminder – The Organizational Unit is the smallest scope that a GPO can be applied to. There is also a local GPO, created to control certain settings on the local computer. GPO's can be linked to sites, domains and organizational units.

GPO processing is done in the following order, with lower settings overwriting higher settings:

- **Local**
- **Site**
- **Domain**
- **Parent organizational unit**
- **Child** (or children) **organizational units**

- The **nested OU's** are processed in the order of the OU hierarchy

Implement an OU structure

Once the organizational unit structure is planned, it must be implemented. This includes creating the OU's, deciding who is going to manage each unit and delegating responsibility. Then comes the job of moving objects into the organizational units.

Create an OU

Organizational units are created in **Active Directory Users and Computers**.
To create an **OU**:

1. From Administrative tools, open Active Directory Users and Computers.
2. Right click on the location where you want to create the OU. This can be a domain or another OU. Choose **New**, and click **Organizational Unit**.
3. Type the name of the OU and click OK.

There are times when Organizational Units are created to **hide** objects. This can also be performed by users who have permission to modify the access control list (**ACL**). Here's how to accomplish this:

1. Create the OU.
2. Right click on the OU and choose **Properties**.
3. Click on the *Security tab*, remove all existing permissions from the OU and choose **Advanced.**
4. Clear the **Allow Inheritable Permissions From the Parent to Propagate to this Object and All Child Objects** check box.
5. In the *Security Message* box, click **Remove**.
6. You should now be back in the *Properties* dialog box, *Security* tab. Choose the group(s) you want to have **full** control of the OU. Grant the group(s) full control.
7. Choose the group(s) you want to have normal rights to the OU. Grant them **read** access.
8. Move the objects you want to hide into the OU.

Delegate permissions for an OU to a user or to a security group

You can delegate administrative control of:

- **Domains**
- **OU**

Delegation of control gives other users or groups the ability to manage the functions of the organizational unit according to their needs.

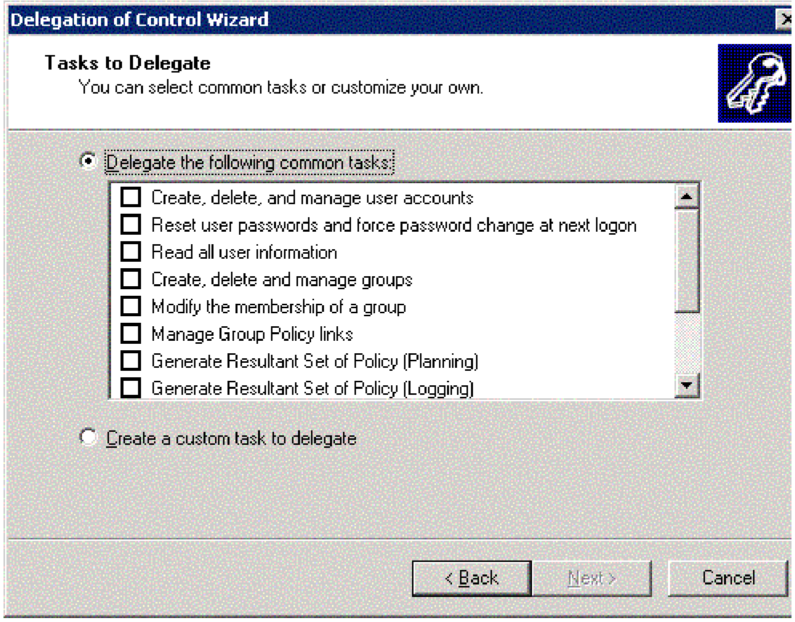
Why would you delegate authority?

Here's an example. You create an OU for the accounting department and the manager wants control over the resources in her department. To give the manager control, you can use the Delegation of Control Wizard.

You can delegate control to users or groups. You must choose the user or group accounts to which you want delegate control. You can run the **Delegation of Control Wizard** to assign the appropriate permissions at the domain or Organizational Unit level.

If other permissions for other objects are necessary, these must be manually set using individual permissions and special permissions from the *Security* tab on the object.

With the **Delegation of Control Wizard** you can choose tasks to delegate. See *Figure 16* below.



Delegation of Control Wizard
Tasks to Delegate
You can select common tasks or customize your own.
< Back
Next >
Cancel

● Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)
- □ Generate Resultant Set of Policy (Logging)

○ Create a custom task to delegate

Figure 16 - Tasks to Delegate from Delegation of Control wizard

If you choose to create a custom task to delegate, you can use **advanced** permissions. Select the permission to delegate.

Move objects within an OU hierarchy

When you move objects between OU's in the same domain, any permission assigned directly to the object will remain the same and the objects will also inherit permissions from the target OU. Permissions inherited from the source or old OU are lost.

There are three ways of moving Active Directory objects between Organizational Units:

- Drag and Drop
- **Move** option from Active Directory Users and Computers console
- **DsMove** command line tool

Planning and Implementing Group Policy

Group policies require careful planning before implementation. GPO's can limit access to services with one mouse click. Improperly applying GPO's can lead to an extended period of network problems!

Plan Group Policy Strategy

Planning a group policy strategy happens both at installation of Active Directory and is an ongoing response to alterations on the network.

Part of the planning process involves understanding how the current configuration is functioning. One of the tools available to help that understanding is the **Resultant Set of Policies (RSoP)**.

Plan a Group Policy strategy by using Resultant Set of Policy (RSoP) Planning mode

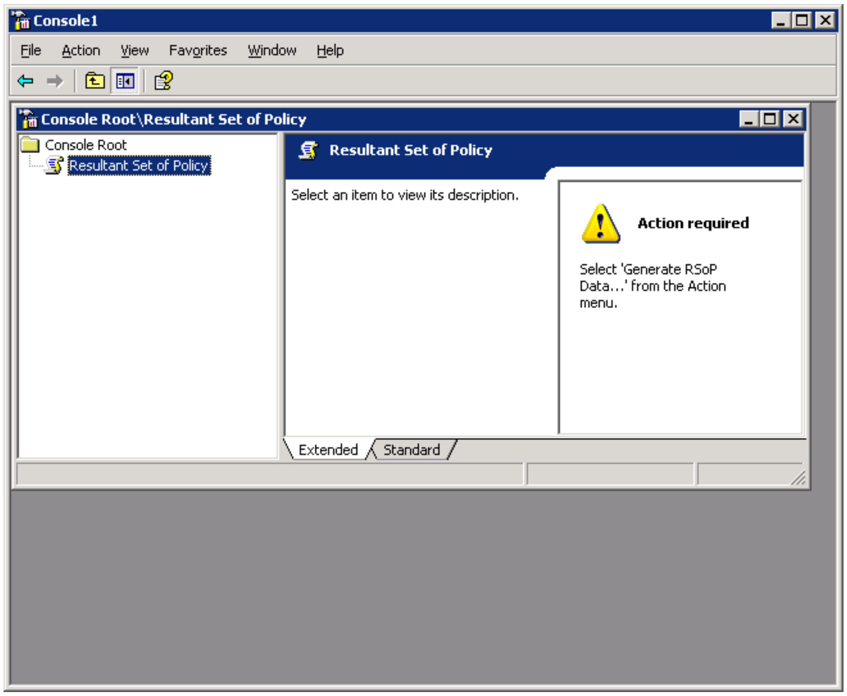
RSoP is a tool that can help plan for changes to your Group Policy strategy.
Here are some of the RSoP characteristics:

- RSoP operates in two modes, *Logging and Planning*.
- RSoP **Logging** is for troubleshooting existing policies.
- RSoP in **Planning** mode helps an Administrator review existing policies and test a new set of policies.

To access **RSoP** in the Microsoft Management Console, do the following:

1. Open MMC.
2. From the File Menu, click **Add/Remove SnapIn**.
3. On the Standalone Tab click **Add**.
4. Choose **Resultant Set of Policies** from the Available Standalone SnapIn menu.

It should look like this:



Select an item to view its description.

Action required

Select 'Generate RSoP Data...' from the Action menu.

Figure 17 – Resultant Set of Policy

During the planning process, you can run **RSoP** to check a query against an existing user or against computer objects to see the effects of **group policy**, no matter where the policy is applied.

When you plan group policies, you have to decide how you are going to use these powerful tools. **Group policies** can be used for things like:

- Distributing software.
- Modifying the registry.
- Implementing security settings.
- Providing scripts for execution at startup, shutdown, logon or logoff.
- Locking down a desktop configuration or how an application will execute.

Every group policy contains a **User Configuration** Node and a **Computer configuration** node. When a user logs on, the user receives group policies in the user configuration node of all group policies that lead from a site, to a domain, through all levels of organizational units.

When a computer starts up, that computer receives the group policies from the same locations. This means that a user can logon to two computers in two locations and get two completely different configurations.

Group policy administration can be carried out by using single setting GPO's, multiple setting GPO's, and dedicated setting GPO's.

Single Setting GPO

- Contains a single type of Group Policy setting; i.e., contains only security settings.
- Best suited for task-based administration and delegated among several individuals.

Multiple Setting GPO

- Contains multiple types of GPO settings; i.e., software settings and application deployment.
- Model best suited for an organization with centralized responsibilities and a head administrator to perform all type of GPO administration.

Dedicated Setting GPO

- Contains computer configurations or user configuration Group Policy settings, but not both.
- Increases the number of GPOs applied.
- Lengthens logon time, but can aid troubleshooting.

When planning for GPO deployment, there are two philosophies, Decentralized GPO designs or Centralized GPO designs.

Decentralized GPO Design

- Goal is to include specific settings in as few GPO's as possible.
- Create a base GPO to be applied to the domain that contains policy settings for as many OU's as possible.
- Next create additional GPO's tailored to the common requirements of an OU and apply them to appropriate OU's.
- This model is best suited for environments where different groups in the organization have common security concerns and changes are frequent.

Centralized GPO approach

- Goal is to use only one GPO for any given user or computer. All policy settings should be implemented in a single GPO.
- If the site, domain or OU has need for different policies, consider subdividing the container into OU's.

Plan a strategy for configuring the user environment by using Group Policy

Planning the user environment involves a wide array of tasks. It includes tasks like:

- Planning for network authentication.
- Planning for network security via passwords and limiting logon times.
- Planning for data management needs, including deciding which folders need to be available to the user from any point in the network or offline.
- You will also need to plan for software deployment. Which software needs to follow the user around the network, and which software can be statically assigned to a computer.
- Setting up authentication using PKI or certificates.

Plan a strategy for configuring the computer environment by using Group Policy

Use Group policies to manage a computer environment by:

- Deploying software, revisions, patches or updates.
- Automatically enrolling certificates.
- Configuring security settings.
- Locking down a desktop.
- Making a user environment safe from end users making changes.
- Deploying or using roaming user profiles.

Configure the user environment by using Group Policy

A problem for every network administrator is how to manage his or her users. When a new software application is released, how can you install it without having to touch each workstation? How can you manage security certificates across the enterprise? Is there a way to make sure that folders are redirected for security purposes? Group Policies can help in each of these areas.

Distribute software by using Group Policy

Why would you want to use a GPO for software deployment? By using a GPO, users can have access to the applications they need, no matter where they log on. In addition, you can configure computers to insure each machine will have the applications required. Applications can also be updated, maintained and removed to meet the needs of the organization

Software distribution is done with the Software Installation Extension to the Microsoft Management Console and with the Control Panel Add or Remove Programs option if GPO's are published and users need to manage their own applications.

Assigning Applications

When a user is assigned an application, the application appears on the Start Menu the next time the user logs in. The application will follow the user wherever the user logs on. The local registry is updated, but the application is actually installed the first time the user accesses it.

If an application is assigned to a computer, the application is listed on the Start Menu and the application is actually installed when the computer can safely perform the operation without endangering other running processes. Assigning applications is used for mandatory company applications that all users must have.

Publishing Applications

When an application is published, the application does not appear as installed on the user's computer. That means no shortcuts are visible, and no updates are made to the registry. The application is listed in the Add/Remove programs Applet in the Control Panel and the user must explicitly select it to install it.

The application advertisement attributes are stored in Active Directory and the application shows up in the Active Directory container. Publishing applications is used for applications that some users, but not all users, need.

Windows Installer Package

The Windows Installer package is a file that has instructions on how to install and remove a specific program. If there are several programs in the suite, each program can be individually installed, removed or modified without affecting the other applications.

Native Windows Installer packages have an .MSI extension, so these files are referred to as MSI files. MSI files have been developed as part of the application development process and are therefore Windows Installer aware.

Repacked Applications

Repackaged applications are used to install applications without a native .msi file

Repackaged applications contain a single product with all the components and applications associated with that product installed as a single feature.

Native applications give you more options.

Transform files

A transform file has an extension of .mst. These files are used to customize the installation of applications.

Patch files

These files have an extension of .msp. MSP files are used to update an existing msi file for the application of patches and service packs.

Application (ZAP) files

ZAP files are third party text files that contain instructions on how to install the related program. These files provide input that is usually taken from an existing Setup program. They have a .zap extension, and do not support the Windows Installer features. The installation process will begin using the original setup.exe or install.exe. These applications can only be published, not assigned, and are installed using the Add/Remove program wizard from Control panel.

Software Distribution Point

No matter what type of application is used, access to the files must be assured. This is done by using a software distribution point. The software distribution point is a location for users or workstations to access the software files.

It is up to the administrator to create the folders for the software on the server and make these folders sharable. When defining the share, the administrator should use the UNC path to the share \\<servername>\share where <servername> is the name of the server and share is the shared folder name.

After the share is created, the administrator copies appropriate files to the software distribution point and then assign the appropriate permissions:

- Administrators should have full control.
- Users only need to view (READ permission).

Software Deployment Process
Once the software distribution point setup is complete, create a GPO and define the deployment properties, including:

- Path to software distribution point.
- Whether to display information while the installation is taking place.
- Whether the application will be published, or assigned.
- User interface options
    - Basic – few messages displayed.
    - Maximum – all messages displayed.

Advanced Tab

- Used to uninstall an application.
- Include OLE information when deploying applications.
- Make 32 bit x86 Windows Installer applications available to 64 bit machines.
- Make 32 bit x86 Down-Level ZAP applications Available to 64 bit machines.
- Set file extension and application precedence to define which files you want automatically installed and the order you are going to install them.

In the **GPO**, the administrator designates the deployment method of publish, assign or advanced. Advanced sets properties with Windows Installer packages including published/assigned options and changes.

In addition, the administrator can set Windows Installer Package properties to:

- Fine tune deployment.
- Set the name for the package and designate a support URL.
- Designate deployment type, options and the user interface options.
- Designate if this is an upgrade to an existing installation.

The *Modifications* tab gives you the ability to add patches or service packs.

The *Advanced* tab gives you the ability to Ignore Language settings and makes the application available to 64 bit machines as well as includes OLE class and product information.

Security Tab
Click security group on which to set permissions.

For the deployment of applications, you have two choices. If all workstations are running Windows 2000 or later, deploy applications using a Group Policy. For those workstations still not running Windows 2000 or greater, down-level clients, use Microsoft Storage Management Services (**SMS**).

Best Practices

- Assign or publish just one application per GPO.
- Assign or publish close to the root in the Active Directory hierarchy.
- Make sure Windows Installer packages include modifications before they are published or assigned.
- Specify application categories for your organization.
- Repackage existing software.
- Set GPO properties to give widely scoped control.
- Set properties on Windows Installer package for fine control.
- Know when to use a GPO versus SMS.

Automatically enroll user certificates by using Group Policy

Notice that this section appears twice, once for users and once for computers. Certificates verify the authentication of users and computers. Group Policy helps network administrators manage these certificates at both levels.

Public Key Policies and Certificate Auto-Enrollment
Public Key Policy rolls out a **Public Key Infrastructure** (**PKI**). The PKI is a set of laws, policies, standards and software used to enhance authentication.

Public Key Policy controls:

- Encrypting File system
  - Add encrypted data recovery agents.
  - Handles changes to the encrypted data recovery policy settings.
- Automatic Certificate Request
  - Enables computers to automatically submit a certificate request to an enterprise certification authority to install the certificate.

Trusted Root Certificate Authorities
The trusted root certificate authority is responsible for establishing public keys belonging to subjects (users or computers) or to other certificate authorities.

- Setting is used to establish common **Trusted Roots.**
- Use policy setting to establish trust in a root certification authority that is not part of your organization.

Enterprise Trust
Used to create and distribute **certificate trust list** (**CTL**).

- CTL is a signed list of root certification authority certificates that are considered viable.

Autoenrollment
In the Auto enrollment settings property box:

- You can enable or disable the automatic enrollment of computer and user certificates by using GPO.
- You can also use Auto Enrollment to manage certificates and to request certificates based on certificate templates.

Auto Enrollment is available for both computers and users.

Redirect folders by using Group Policy

Redirect folders using a Folder Redirection Group Policy Object. This option is available only on the *User* Configuration Node.

You redirect folders to provide centralized locations for XP Professional folders on a server or on servers. This means the data is more likely to get backed up. It is called a sharepoint and allows users an access point and administrators a way of managing information.

Only certain folders can be redirected to network locations including:

- My documents
- My pictures
- Application Data
- Desktop
- Start Menu

Advantages

- Documents are available no matter where a user logs in.
- If **roaming profiles** are used, the network path to My Documents is part of the roaming user profile, not the My Documents folder itself.
- **Offline files** will give users access to My Documents when not connected to the network.

- Data on the network will be backed up.
- Administrators can use a Group Policy to set **disk quotas**, limiting the amount of disk space the special folders can take up.
- Data specific to a user can be redirected to a different hard disk on the user's local computer from the computer holding the OS.

Set up

- Redirect special folders to one location for everyone in a site, domain or OU.
- Redirect special folders to a location according to security group membership.

Configure user security settings by using Group Policy

Security policies are rules you can configure on a computer or several computers for protecting resources on a network. Security policies can control:

- How a user authenticates to the network or computer
- What resources a user is allowed to use
- Whether event logging is turned on or not
- Group Membership

Areas that can be configured using Security policies include:

- Account Policies
    - Password Policy
    - Account lockout policy
- Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security options
- Event Log
- System Services
- Registry
- File System
- Wireless Network Policies
- Public Key Policies
- Software Restriction Policy

- IP Security Policy
- Account Lockout Policy
- Event Logging Policy
- Wireless Networking Policy

Deploy a computer environment by using Group Policy

Does your company use a standard desktop configuration? This can include things like having standard wallpaper, certain applications installed on computers in certain areas or allowing computers to authenticate to other trees or forests. Each of these tasks can be simplified by using group policies.

Distribute software by using Group Policy

You can deploy software via group policy to either computers or users. Deploy to users if you want the software to follow the user no matter where they access the network. Deploy software to computer when you want the software to be available to whoever uses that computer.

Why would you want to use a GPO for software deployment? By using a GPO, computers can have applications automatically installed. Applications can also be updated, maintained and removed to meet the needs of the organization

Software distribution is done with the Software Installation Extension to the Microsoft Management Console and with the Control Panel Add or Remove Programs option if users need to manage their own applications.

Assigning Applications
If an application is assigned to a computer, the application is installed on the Start Menu and the application is actually installed automatically when the process will not conflict with other running applications.

Publishing Applications
When an application is published, the application does not appear as installed on the user's computer. That means no shortcuts are visible, and no updates are made to the registry. The application is listed in the Add/Remove programs Applet in the Control Panel and the user must explicitly select it to install it.

The application advertisement attributes are stored in Active Directory and the application shows up in the Active Directory container.

Windows Installer Package
The Windows Installer package is a file that has instructions on how to install and remove a specific program. If there are several programs in the suite, each program can be individually installed, removed or modified without affecting the other applications.

The **native** Windows Installer packages have an .MSI extension, so these files are referred to as MSI files. MSI files have been developed as part of the application development process and are therefore Windows Installer aware.

Repacked applications
Repackaged applications are used for applications without a native .msi file

Repackaged applications contain a single product with all the components and applications associated with that product installed as a single feature.

Native applications give you more options.

Transform files
A transform file has an extension of **.mst**. These files customize the installation of applications.

Patch files
These files have an extension of .msp. MSP files are used to update an existing msi file for the application of patches and service packs.

Application (ZAP) files
ZAP files are third party text files that contain instructions on how to install the related program. These files provide input that is usually taken from an existing Setup program. They have a .zap extension, and do not support the Windows Installer features. The installation process will begin using the original setup.exe or install.exe. These applications can only be published, not assigned, and are installed using the Add/Remove program wizard from Control panel.

Software Distribution Point
No matter what type of application is used, access to the files must be assured. This is done with a software distribution point. The software distribution point is a location for users or workstations to access the software files.

It is up to the administrator to create the folders for the software on the server and make these folders sharable. When defining the share, the administrator should use the UNC path to the share \\<servername>\share where <servername> is the name of the server and share is the shared folder name.

After the share is created, the administrator copies appropriate files to the software distribution point and then assign the appropriate permissions:

- Administrators should have full control.
- Users only need to view (READ permission).

Software Deployment Process
Once the software distribution point setup is complete, create a GPO and define the deployment properties, including:

- Path to software distribution point.
- Whether to display information while the installation is taking place.
- Whether the application will be published, or assigned.
- User interface options
    - Basic – minimal information presented.
    - Maximum – all messages displayed.

Advanced Tab

- Used to uninstall an application.
- Include OLE information when deploying applications.

- Make 32 bit x86 Windows Installer applications available to 64 bit machines.
- Make 32 bit x86 Down-Level ZAP applications available to 64 bit machines.
- Set file extension and application precedence to define which files you want automatically installed and the order you are going to install them.

In GPO, the administrator designates the deployment method of publish, assign or advanced. Advanced sets properties with Windows Installer packages including published/assigned options and changes.
In addition, the administrator can set Windows Installer Package properties to:

- Fine tune deployment.
- Set the name for the package and designate a support URL.
- Designate deployment type, options and the user interface options.
- Designate if this is an upgrade to an existing installation.

The *Modifications* tab gives you the ability to add patches or service packs.

The *Advanced* tab provides you with the ability to Ignore Language settings and makes the application available to 64 bit machines as well as includes OLE class and product information.

Security Tab
Click security group on which to set permissions.

For the deployment of applications, you have two choices. If all workstations are running Windows 2000 or later, deploy applications using a Group Policy. For those workstations still not running Windows 2000 or greater (down-level clients), use Microsoft Storage Management Services (**SMS**).

Best Practices

- Assign or publish just once per GPO.
- Assign or publish close to the root in the Active Directory hierarchy.
- Make sure Windows Installer packages include modifications before they are published or assigned.
- Specify application categories for your organization.
- Repackage existing software.
- Set GPO properties to give widely scoped control.
- Set properties on Windows Installer package for fine control.
- Know when to use a GPO versus SMS.

Automatically enroll computer certificates by using Group Policy

Public Key Policies and Certificate Auto-Enrollment
Public Key Policy rolls out a **Public Key Infrastructure** (**PKI**). The PKI is a set of laws, policies, standards and software used to enhance authentication.

Public Key Policy controls:

- Encrypting File system
    - Add encrypted data recovery agents.
    - Handles changes to the encrypted data recovery policy settings.
- Automatic Certificate Request
    - Enables computers to automatically submit a certificate request to an enterprise certification authority and install the certificate.

Trusted Root Certificate Authorities
The trusted root certificate authority is responsible for establishing public keys belonging to subjects (users or computers) or to other certificate authorities.

- Setting is used to establish common **Trusted Roots.**
- Use policy setting to establish trust in a root certification authority that is not part of you organization.

Enterprise Trust
Used to create and distribute **certificate trust list** (CTL).

- **CTL** is a signed list of root certification authority certificates that are considered viable.

Autoenrollment
In the Auto enrollment settings property box:

- You can enable or disable the automatic enrollment of computer and user certificates by using GP.
- You can also use Auto Enrollment to manage certificates and to request certificates based on certificate templates.
- Auto Enrollment is available for both computers and users.

Configure computer security settings by using Group Policy

You can use Group Policy to control security for all the computers on your network from your workstation. By using the Group Policy Management console, you can create and change policies that manage workstations, servers and domain controllers throughout the organization

You can either use some of the default security templates provided by Microsoft or you can use the **GPMC** to create your own standards.

You can modify the following from the Account Policies:

- Password Policy
- Account Lockout Policy
- **Kerberos Policies**

From the local computer policy, you can set

- Audit Policy
- User Rights Assignments
- **Security Options**

In addition, you can define security policies for Wireless networking and IPSec.

Managing and Maintaining Group Policy

Troubleshoot issues related to Group Policy application deployment. Tools might include RSoP and the gpresult command

It is easy to get in trouble when you use multiple group policies objects. GPO's may contain the same group policy with a different configuration, meaning that one group policy will block, overwrite, alter or otherwise screw up another group policy. In any case, the result you receive is not the result you expect. This can be especially frustrating when trying to figure out why an application is not deploying, or is deploying improperly.

Troubleshooting 101 says before you can figure out what it wrong, you have to know what is currently happening. In troubleshooting group policies, you have to first figure out which group policies are being applied, the order they are being applied, and whether the inheritance of a group policy is forced on another container, or if it is blocked. Next, you could start by examining each and every group policy, but that would be the hard way. The easier way is to use the **Resulting Set of Policy** (**RSoP**) tool and the command **gpresult**.

As mentioned previously, RSoP runs in either *planning* mode or *logging* mode. For troubleshooting, use logging mode to get exact information for either a computer or user account. RSoP discovers results of the group policy settings applied when a user logs onto a computer in a different OU.

Gpresult is a command line tool that lets you create and display a RSoP –type request from the command line. It also gives you general information about the operating system, the user and the computer.

In addition, if *Verbose Logging* is turned on the Windows Package Installer, you will have the opportunity to use the Advanced Deployment Options. The **Advanced Deployment Option** dialog box will give you the opportunity to view these items:

- Product Code
- Deployment Count
- Script Name

To view the advanced diagnostic information, do the following:

1. Start the **GPO Editor** and open the appropriate **Software Settings.**
2. Click the *Software Installation Node*.
3. From the details area, use the right mouse button to highlight the package, and then click **Properties.**
4. Click the *Deployment* tab and then click **Advanced**.

Maintain installed software by using Group Policy

By its very nature, software is outdated when it is installed. In addition, you install software so users can access it, and we all know how creative users can be when it comes to screwing things up. Software must also be maintained. In an effort to keep you from actually having to deal with people, some of the maintenance tasks can be automated with Group Policies.

When you need to redeploy an application that has previously been deployed with a group policy, you can make small changes to the original deployment. This would be helpful if you were to add Microsoft Access to a previous deployment of Word, Excel and Powerpoint. As long as you make the changes to the original package deployed with a group policy, you can deploy the application over the network.

To redeploy the application:

1. Open the **GPO Editor** console and open the appropriate Software Settings.
2. Click the *Software Installation Node*
3. From the details pane, right click the package to remove, click **All Tasks** and then click **Redeploy** Application.
4. In the dialog box, click **Yes** to redeploy the application to all the computers on which it is currently deployed.

Distribute updates to software distributed by Group Policy.

Updates or upgrades can occur for a variety of reasons including:

- New versions are available.
- Your organization may switch to a different developer of the software.

Major updates and upgrades include new files to be deployed, new version numbers, new directories and other substantial changes. If you are going to upgrade, you will first have to create a new Windows Installer package that contains the upgrade and then configure the upgrade in the *Upgrade* tab in the properties dialog box for the package.

To upgrade the package:

1. Start the **GPO Editor**. In the *Computer Configuration* or *User Configuration* node, open the software settings.
2. Choose the **Software Installation node.**
3. Create a new Windows Installer package for the upgrade and either *assign* the package or *publish* it.

4. From the details pane, right click the *Windows Installer package* that will be the upgrade and then click **properties**.
5. In the *Upgrade* tab of the Properties dialog box, click **Add** to generate the Add Upgrade Dialog box.
6. In the *Add Upgrade* Dialog, chose either:
   - **Current Group Policy Object**
   - **A different GPO**
7. Select the package you want to upgrade in the Packages to Upgrade list.
8. Select from:
   - **Uninstall the existing package.**
   - **Package can upgrade over the existing package.**
9. Click OK.
10. From the *Upgrades* tab in the Properties dialog for the package, choose the **Required Upgrade for Existing Packages** check box if you want the upgrade to be *mandatory* and click OK.

Software Removal
When software outlives its usefulness, it should be removed. There are two methods for removing software that has been deployed using Group Policies:

- Immediately Uninstall or *forced* removal.
- Allow current users to continue using the software but not allow any other new users access to it. This is known as an *optional* removal.

With a forced removal, the following happens:

- If the software is assigned to a computer, it is deleted from the computer the next time the computer is rebooted or turned on.
- If the computer is not attached to the network, it is deleted the next time the computer is attached to the network.
- Software assigned or published to users is deleted from the computer the next time the user logs on.
- Software assigned or published to users on computers that are not attached to the network is deleted the next time the computer attaches to the network.

To remove software:

1. Open the **GPO Editor** console and open the appropriate *Software Settings*.
2. Choose the **Software Installation Node**.
3. From the details pane, right click the package to be removed, click **All Tasks** and click **Remove**.
4. From the Remove dialog box choose to **Immediately Uninstall** or **Allow Users to Continue to use software**.

Configure automatic updates for network clients by using Group Policy

As a network administrator, you are in a position to make sure the workstations on your network remain up-to-date on the latest patches and security updates. In a large environment, this can be a daunting task. Using a GPO and linking the GPO to an OU or to a domain can simplify it.

To setup the behavior of Automatic Updates clients by using a Group Policy:

1. Open the **Group Policy Management Console** and create a *new* **GPO**.
2. Click **Computer Configuration** to expand your choices and chose **Administrative Templates**, then expand **Windows Components** and click **Windows Update**.
3. From the *Windows Update* template, select **Configure Automatic Updates**.
4. Select from the following options:
    - Notify for download and notify for install.
    - Auto download and notify for install.
    - Auto download and schedule the install.

This process can also be *redirected* to a server running **Software Update Services** (**SUS**) by:

1. Open the Group Policy MMC and from the details pane, click Specify Windows Update Server.
2. In the text box, type in the name of the server that runs SUS.

Note: SUS is an optional component that is available from Microsoft's Web site. SUS works with both Windows Server 2003 and Windows 2000 Server. For more information on SUS including a link to download it visit: Software Update Services

Troubleshoot the application of Group Policy security settings. Tools might include RSoP and the gpresult command

It is easy to get in trouble when you use multiple group policies objects. GPO's may contain the same group policy with a different configuration, meaning that one group policy will block, overwrite, alter or otherwise screw up another group policy. In any case, the result you receive is not the result you expect.

Troubleshooting 101 says before you can figure out what it wrong, you have to know what is currently happening. In troubleshooting group policies, you have to first figure out which group policies are being applied, the order they are being applied, and whether the inheritance of a group policy is forced on another container, or if it is blocked. Now, you could start by examining each and every group policy, but that would be the hard way. The easier way is to use the **Resulting Set of Policy** (**RSoP**) tool and the command gpresult.

As mentioned previously, RSoP runs in either *planning* mode or *logging* mode. For troubleshooting, go with logging mode to get exact information for either a computer or user account. RSoP discovers results of the group policy settings applied when a user logs onto a computer in a different OU.

Gpresult is a command line tool that lets you create and display a RSoP –type request from the command line. It also gives you general information about the operating system, the user and the computer.

Practice Questions

Chapter 1 Planning and Implementing an Active Directory Infrastructure

1. Tom has created a customized program that needs to store data on domain controllers so that it will be replicated to several domains in his company's Active Directory forest. What should he do?

   Select the best answer.

   ○ A. Add an additional application programming interface (API) that enables the application to store its data in the Active Directory configuration partition.
   ○ B. Use the ntdsutil tool to create an application partition.
   ○ C. Use Active Directory Users and Computers to create an application partition.
   ○ D. Use Active Directory Sites and Services to create an access for the application to store its data in the Active Directory configuration partition.

2. Freda is a domain administrator who is responsible for ensuring the proper management of servers and client computers in her company, which operates a single Active Directory domain with a series of OUs representing various departments and office locations. She needs to assign junior administrators to take care of the various departments and offices, including the specification of multiple configuration and permission changes.

   Which management tool should Freda use to most efficiently specify multiple configuration and permission changes at the same time?

   Select the best answer.

   ○ A. Delegation of Control Wizard
   ○ B. Authorization Manager
   ○ C. Group Policy Object Editor
   ○ D. Access Control List (ACL) Editor

3. John is the network administrator for a wholesale distributor that has experienced large growth in the past two years. He has become aware that a user named Norma has taken several advanced computer courses and acquired basic knowledge of the workings of Active Directory. After talking with his supervisor and interviewing Norma, John has decided to provide Norma with the ability to create and manage user accounts in the Accounting OU.

   Which of the following tasks should John do to provide Norma with this ability, without granting her excessive control? Each answer represents a complete solution to the problem.

   Choose two answers.

   ○ A. Grant Norma's account the appropriate permissions in Active Directory.
   ○ B. Grant the Accounting OU the appropriate permissions in Active Directory.
   ○ C. Add Norma's account to the Account Operators group.
   ○ D. Use the Delegation of Control Wizard.

4. Molly is a systems engineer for a company that operates a single domain Active Directory ne work with six sites.

   After checking the output of Replmon, she realizes the need to optimize intersite replication, so she opens Active Directory Sites and Services. More specifically, she needs to modify the cost of several site links. Which steps does she need to follow to configure the site link cost?

   To answer, select and move the correct steps to the right and put them in the correct order.

   A. Expand the Inter-Site Transports folder, and right-click the transport (IP or SMTP) that you want to modify.
   B. In the details pane of Active Directory Sites and Services, right-click a site link whose cost you want to modify, and choose Properties.
   C. Right-click the Inter-Site Transports folder and choose Properties.
   D. In the Replicate every text box, enter a value for the number of minutes between replication events.
   E. Enter a cost value in the Cost text box or use the up/down arrows to select a value.

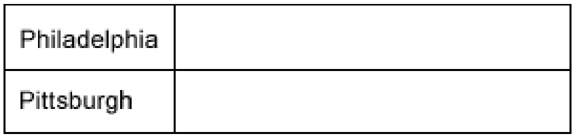
5. Pauline is an enterprise administrator for an engineering company that has an Active Directory forest containing an empty root domain plus two child domains.

   The company operates two offices, which are connected by a slow WAN link and both of which contain users from both child domains. The offices are configured as separate sites in Active Directory. One office in Philadelphia contains 500 users. The other office, located in Pittsburgh, contains 75 users. The security group structure of the forest contains several universal groups that facilitate resource access between the child domains.

   How should Pauline employ global catalog servers and universal group caching in the two offices?

   To answer, drag the correct implementation to the correct office location.

   A. Global catalog server B. Universal group caching



Philadelphia	
Pittsburgh	

Chapter 2 Managing and Maintaining an Active Directory Infrastructure

1. Ruth needs to optimize Active Directory replication in her company's single domain network that includes a single site with three Windows Server 2003 domain controllers. The company is a small one and changes to Active Directory occur only at infrequent intervals. For this reason, Ruth wants to extend the Active Directory replication interval to a longer time that releases bandwidth for other network operations. Which of the following does Ruth need to do to accomplish this objective?

Select the best answer.

○ A. Modify the NTDS Settings object in Active Directory.
○ B. Modify the DEFAULTIPSITELINK object.
○ C. Modify the Registry at each domain controller.
○ D. Modify the schema.

2. Carl is a systems administrator for a company that hosts an Active Directory domain with eight sites representing cities throughout North America in which his company does business. He has received messages from administrators on the West Coast that Active Directory replication has not always taken place as expected. Carl has decided that he needs to monitor Active Directory replic tion more consistently so that he can locate and troubleshoot any problems that might occur. Which of the following activities should he undertake? Each answer presents part of the solution.

Choose three.

□ A. Check the Directory Service log and the File Replication Service log for replication failure messages.
□ B. Check the DNS log for DNS name registration failures.
□ C. Use Replmon to monitor replication partners and link replication status, and check repliction topology.
□ D. Use Replmon to monitor for DNS name registration failures.
□ E. Use Netdiag to monitor replication failures.
□ F. Use Netdiag to monitor network and DNS registration failures.

3. Gerry is the network administrator for his company, which operates a single domain Active Directory network that includes seven Windows Server 2003 computers and 100 client computers that run a mix of Windows 2000 Professional and Windows XP Professional.

Four of the servers, named SRV1, SRV2, SRV3, and SRV4, function as domain controllers, with SRV1 and SRV2 also functioning as operations masters.

Every Friday, Gerry runs a full backup of each server, and every Tuesday, he runs an incremental backup of each server. One Thursday, SRV3 experiences a total hard disk failure. Gerry installs a new hard disk, and reinstalls Windows Server 2003 and Active Directory on the computer. He then runs the Disk Management snap-in to recreate a volume structure similar to the previous one and restores data files that had been on the server from the total and incremental backups. What else does Gerry need to do to completely restore SRV3 as a domain controller? Each answer represents part of the solution.

Choose all that apply.

□ A. Start the computer in Safe Mode.
□ B. Start the computer in Directory Services Restore mode.
□ C. Nonauthoritatively restore system state data from backup.
□ D. Authoritatively restore system state data from backup.
□ E. Manually restore the File Replication Service (FRS).

4. Kelly is a systems administrator for a company that operates an Active Directory domain with a mixture of Windows NT 4.0, Windows 2000, and Windows Server 2003 domain controllers. One Windows NT 4.0 BDC runs a proprietary application that will not be updated to Windows 2000/2003 in the foreseeable future.

One Monday, Kelly received several complaints from users in the same office as this BDC that they were unable to log on. Checking the BDC, she realized that it had not received replication updates from other domain controllers. What should she check first?

Select the best answer.

○ A. Use replmon to check the replication topology on the network.
○ B. Raise the domain functional level to Windows 2000 native.
○ C. Roll the domain functional level back to Windows 2000 mixed.
○ D. Ensure that the PDC emulator is functioning and accessible to the BDC.

5. You are an enterprise administrator for a company that operates an Active Directory forest containing six domains in two domain trees.

   Your company has recently signed a cooperative deal with another company that requires you to set up a forest trust between the two companies' Active Directory forests. However, the other company is using a UPN suffix that conflicts with one in use by your company; consequently, you have to remove the conflicting suffix in your company.

   Working from Active Directory Domains and Trusts, which of the following steps should you perform to accomplish this objective?

   To answer, drag the correct steps to the right and place them in the proper order.

   A. Select the UPN suffix to be removed and click Disable. ______
   B. Select the UPN suffix to be removed and click Remove. ______
   C. Select the UPN suffix to be removed and press the Delete key. ______
   D. Select the Name Suffix Routing tab. ______
   E. Right-click Active Directory Domains and Trusts and choose Properties. ______
   F. Right-click the forest root domain and choose Properties.

Chapter 3 Planning and Implementing User, Computer, and Group Strategies

1. Dan is a systems administrator for a company that operates a Windows Server 2003 domain. He is planning an OU structure that will parallel the company's departmental organization. After Dan has specified initial user permissions, departmental administrators will configure additional permissions. Dan needs to assign permissions for resources, such as files, folders, and printers. Which of the following Active Directory objects should Dan use for the initial permissions assignment?

   Select the best answer.

   ○ A. Organizational units
   ○ B. Individual users
   ○ C. Distribution groups
   ○ D. Security groups

2. Murray is designing a plan for upgrading his company's multiple domain Windows NT 4.0 enterprise to Active Directory in Windows Server 2003. He is reading about the new feature of OUs that he can use when he is consolidating several Windows NT domains into a single Active Directory domain. Which of the following represent actions he can perform by creating a system of OUs?

   Choose all that apply.

   □ A. Deploy group policies that regulate user desktops, software installation, and security settings.
   □ B. Deploy account policies including password policies.
   □ C. Configure replication of Active Directory.
   □ D. Create e-mail distribution lists.
   □ E. Delegate administrative authority to departmental administrator groups.

3. Jennifer is a domain administrator for a research firm that recently had some secrets stolen by a spy who was posing as an office-cleaning contractor. To increase the security of the network, her manager has approved a system of smart card authentication, and has purchased the appropriate hardware. Jennifer is already aware of the benefits provided by smart card authentication, including a higher security of logons and secure e-mail. Which of the following represents an additional benefit of using smart cards for authentication?

Select the best answer.

○ A. Smart cards can sign documents.
○ B. Smart cards can encrypt documents.
○ C. Smart cards store public key infrastructure (PKI) information.
○ D. Smart cards store digital signatures.

4. Frank is a systems engineer who works for a mining company. The company operates a single domain Active Directory network with sites representing each office and field operation. Business functions include mineral exploration, extraction, processing, and marketing.

Frank needs to design an OU structure that will enable the local administration of users and resources at every location by a user situated at that location. What type of model should Frank use when designing the company's OU structure?

Select the best answer.

○ A. A model based on business functions
○ B. A geographical model
○ C. A model based on types of resource objects
○ D. A hierarchical model

5. Doug is the systems administrator of a company that operates an Active Directory forest that contains a parent domain called tech.com and two child domains named east.tech.com and west.tech.com. A user named Kristin in the east.tech.com domain has been promoted to supervisor of a work group that is headquartered within the west.tech.com domain. Doug needs to move her account from the east.tech.com domain to the west.tech.com domain so that she can access the proper resources required for her to do her new job.

Which of the following tasks should Doug perform in order to move her account?

○ A. Use the ADMT MMC snap-in tool.
○ B. Use the Movetree command utility.
○ C. Copy her user account from the east.tech.com domain to the west.tech.com domain. Then delete the old account from the east.tech.com domain.
○ D. In Active Directory Users and Computers, right-click her account and select Move. Then enter the new domain name.

Chapter 4 Planning and Implementing Group Policy

1. You are responsible for ensuring that all computers in your company meet minimum standards. In doing so, you must analyze the security settings on a series of computers and then apply updated settings if you find any discrepancies. Which of the following tools can you use to accomplish this task? Each answer represents a complete solution.

   Choose two.

   □ A. Security Templates
   □ B. Security Configuration and Analysis
   □ C. Security Settings Extension to Group Policy
   □ D. IPSec Security Policies
   □ E. The Secedit command line tool

2. Adam is a systems administrator for a company that operates a single domain Active Directory network. The company has three divisions, corresponding to major business operations. Each division is further divided into two or more sections. There is an OU for each division and a child OU for each section, and GPOs exist for each OU in the company. The company's Engineering division consists of Design and Construction sections. A domain-wide GPO contains corporate settings including a prescribed desktop configuration.

   The manager of the Design section wants users in that section to have a different desktop configuration applied to only the computers in that section.

   Adam has created a GPO that applies these configurations, and needs to ensure that computers in the design section receive only the settings defined in that GPO. Computers in all other departments must receive the corporate settings. What should he do?

   Select the best answer.

   ○ A. Specify Block Policy Inheritance on the Design OU.
   ○ B. Specify Block Policy Inheritance on the Engineering OU.
   ○ C. Specify No Override on the GPO linked to the Design OU.
   ○ D. Specify No Override on the GPO linked to the Engineering OU.

3. Greg is responsible for enrollment of certificates for users on his company's Active Directory network. He needs to configure autoenrollment of user certificates.

   What should he do to require users who request certificates to sign the request with a private key from a valid certificate in their certificate store?

   Choose all that apply.

   □ A. Select the Prompt the user during enrollment option.
   □ B. Set the This number of authorized signatures option to 1.
   □ C. Set the This number of authorized signatures option to a value higher than 1.
   □ D. Select the Valid existing certificate option.
   □ E. Select the Prompt the user during enrollment and require user input when the private key is used option.

4. Sheila is the administrator of the corporate.com domain. She has created several Active Directory containers, as follows:

- An OU named Marketing.
- An OU named Management.
- A child domain named research.corporate.com.
- An OU named Development, located in the research.corporate.com domain.

In which of the following containers can Sheila create a Group Policy Object?

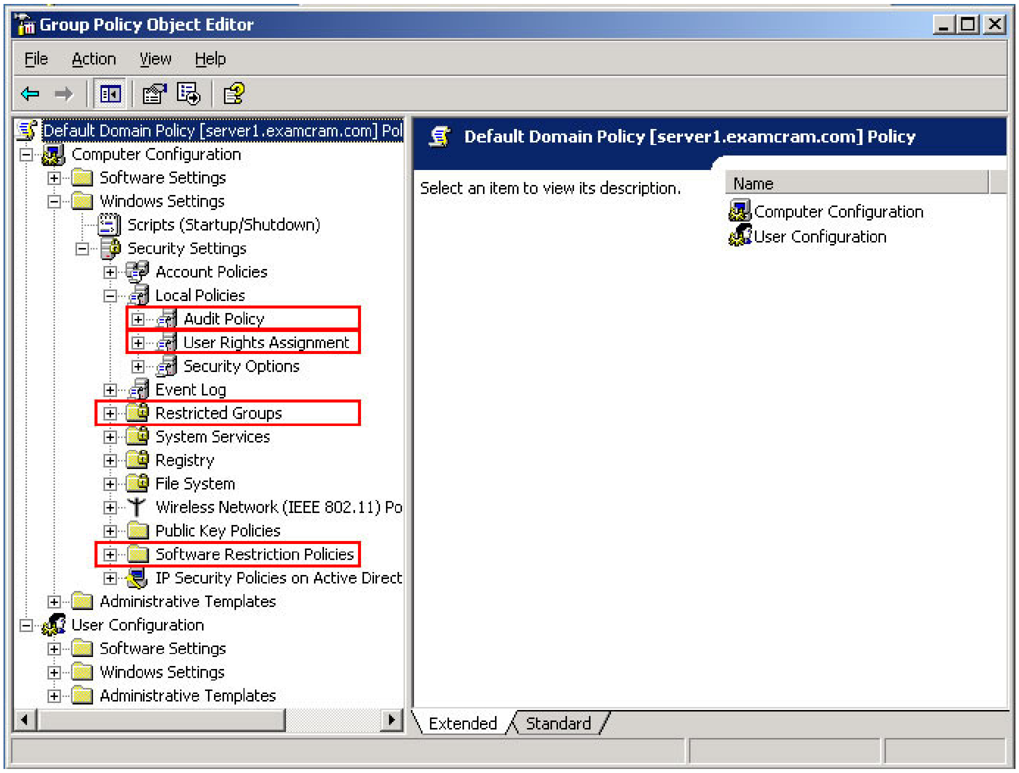
Choose all that apply.

□ A. Management OU
□ B. Computers
□ C. Marketing OU
□ D. Development OU
□ E. The research.corporate.com domain
□ F. Builtin

5. Judy is the systems administrator of a small company that operates an Active Directory network. She has been plagued with incidents of users installing unauthorized software that has resulted in lost productivity and help desk calls to clean up corrupted computers. When checking several of these computers, she realized that users were adding their domain accounts to the local Administrators group to grant them the capability to install software.

Judy needs to configure a node in the Group Policy Object Editor console to prevent users from adding themselves to the local Administrators group. Which node should she configure?

To answer, select the appropriate node in the exhibit.



Chapter 5 Managing and Maintaining Group Policy

1. You are the network administrator for your company. A user named Sharon reports that she ca not access Internet Explorer to connect to a Web site containing information vital to performing her job. You just finished creating a GPO linked to the Data Entry OU that hides Internet Explorer from members of this OU.

You need to find out why Sharon appears to be receiving this policy despite the fact that her user account is located in the Research OU. What should you do? Each answer represents a complete solution.

Choose two.

❑ A. Use Resultant Set of Policy (RSoP) in logging mode, specifying Sharon's user account and the computer that she regularly uses.
❑ B. Use Resultant Set of Policy (RSoP) in planning mode, specifying Sharon's user account and the computer that she regularly uses.
❑ C. Use the gpotool command, and specify Sharon's user account and the computer that she regularly uses.
❑ D. Use the gpresult command, and specify Sharon's user account and the computer that she regularly uses.

2. You are a systems engineer for your company, which operates an Active Directory forest with three domains. The company has hired Priscilla as a new design specialist. Priscilla attempts to install a published application from the Add or Remove Programs applet in Control Panel, but receives an error message.

To determine what caused this error to occur, you start the RSoP snap-in. Which of the following steps should you take to obtain troubleshooting information? Each answer presents part of the solution.

Choose three.

❑ A. Perform an RSoP planning mode query for Priscilla.
❑ B. Perform an RSoP logging mode query for Priscilla.
❑ C. Set the Software Installation folder's view to Installed Applications.
❑ D. Set the Software Installation folder's view to Available Applications.
❑ E. Check the information displayed on the Error Information tab of the software pac age's Properties dialog box.
❑ F. Check the information displayed on the Precedence tab of the software package's
❑ G. Properties dialog box.

3. Tiffany is a departmental administrator for a large company that operates a single domain Active Directory infrastructure with four sites representing the cities in which the company does business. Each department is represented by one or more OUs. Tiffany administers users and computers in the Accounting department. Within this department is an Accounting Users OU and an Accounting Computers OU. These OUs contain the user and computer accounts for this department, respectively.

Tiffany is planning to install Microsoft Software Update Services on a server in the Accounting department. She wants users in this department to download updates only from this server, regardless of the location of the computer they are using. Employees of other departments should be able to connect directly to Windows Update from all computers, even those in the Accounting department. How should Tiffany configure a GPO to accomplish these objectives?

Select the best answer.

○ A. Use the Computer Configuration node of a GPO linked to the Accounting Computers OU.
○ B. Use the User Configuration node of a GPO linked to the Accounting Computers OU.
○ C. Use the User Configuration node of a GPO linked to the Accounting Users OU.
○ D. Use the Computer Configuration node of a GPO linked to the Accounting Users OU.

4. Sophie is responsible for maintaining software on client computers in her company's Active Directory network. An application vendor has provided an upgrade that Sophie needs to distribute to users who have the software installed on their computers. The upgrade is to be installed over the existing version and should retain the user's application preferences and document type associations.

Sophie accesses the User ConfigurationSoftware SettingsSoftware Installation node in the Group Policy Object Editor console focused on the GPO that originally deployed the software. What should Sophie do next?

Select the best answer.

○ A. Deploy the upgraded version of the software. Right-click the upgraded application and choose Properties. Select the Upgrades tab, and then click Add. In the Add Upgrade Package dialog box, select the application package to upgrade. Select the Package can upgrade over the existing package option.
○ B. Deploy the upgraded version of the software. Right-click the upgraded application and choose Properties. Select the Upgrades tab, and then click Add. In the Add Upgrade Package dialog box, select the application package to upgrade. Select the Uninstall the existing package, then install the upgrade package option.
○ C. Right-click the existing application and choose Properties. Select the Upgrades tab, and then click Add. In the Add Upgrade Package dialog box, specify the upgraded application package. Select the Package can upgrade over the existing package option.
○ D. Right-click the existing application and choose Properties. Select the Upgrades tab, and then click Add. In the Add Upgrade Package dialog box, specify the upgraded application package. Select the Package can upgrade over the existing package option.

5. Charles is a network administrator for a medium-sized engineering company that hires a large number of college students during the summer months. The company operates a single domain Windows Server 2003 network with two sites corresponding to its San Jose and Los Angeles offices. Among the students hired at these offices are several computer science students who are entering their senior year and have been given the responsibility of maintaining user and group accounts.

One September morning, Charles needed to delete the user accounts of several students who had recently returned to college. However, he discovered that one of these accounts had already been deleted. Earlier in the summer, he had appropriately configured the network to audit all objects in Active Directory. He now wants to verify the proper deletion of the student's account, and find out who has deleted the account. What should Charles do to accomplish this task with the least amount of administrative effort?

Select the best answer.

○ A. He should look for Directory Service Access events in each domain controller's Security log.

○ B. He should look for Account Management events in each domain controller's Security log.

○ C. He should look for Object Access events in each domain controller's Security log.

○ D. He should look for Process Tracking events in each domain controller's Security log.

Answers and Explanations

Chapter 1

1. Answer: B

Explanation A. The configuration partition contains information about the structure of Active Directory in the forest, including domains, sites, and services. It is not possible to add application-specific data to this partition.

Explanation B. An application partition is a new feature of Windows Server 2003 that contains application-specific data that needs to be replicated only to specific domain controllers in one or more domains of the Active Directory forest. Tom can use the ntdsutil tool to create an application partition.

Explanation C. Active Directory Users and Computers does not contain any tools that would enable the creation of an application partition.

Explanation D. The configuration partition contains information about the structure of Active Directory in the forest, including domains, sites, and services. It is not possible to add application-specific data to this partition. Furthermore, you cannot use Active Directory Sites and Services in this manner.

Answer: B

Explanation A. Although you can configure multiple permissions automatically using the Delegation of Control Wizard, Authorization Manager provides additional scope and options for configuration using role-supporting applications.

Explanation B. The Authorization Manager is a very effective tool for managing administrative rights and privileges. In particular, you can implement multiple configuration and permission changes at once. It enables you to use role-based access control for managing the various OUs in the network.

Explanation C. You can configure a large number of policies using the Group Policy Object Editor but you cannot implement configuration and permission changes required for this scenario using this tool.

Explanation D. You can use the ACL editor to configure permissions that enable junior administrators to perform their tasks, but its use takes far more administrative effort and you may not know exactly which permissions you need to specify to enable the
delegation of the proper level of authority.

3. Answer: A, D

Explanation A. The Delegation of Control Wizard provides John with the ability to delegate partial control of an OU to a user such as Norma. He can also grant her account specific permissions on the Active Directory objects (in this case, user accounts), assuming her user account is in the same OU.

Explanation B. It is not possible to grant her this type of control by assigning permissions to the OU.

Explanation C. John could add Norma's account to the Account Operators group, but this would grant her control over all user accounts in the domain, which is too much authority.

Explanation D. The Delegation of Control Wizard provides John with the ability to delegate partial control of an OU to a user such as Norma. He can also grant her account specific permissions on the Active Directory objects (in this case, user accounts), assuming her user account is in the same OU.

4. Answer:

A. Expand the Inter-Site Transports folder, and right-click the transport (IP or SMTP) that you want to modify.
B. In the details pane of Active Directory Sites and Services, right-click a site link whose cost you want to modify, and choose Properties.
C. Right-click the Inter-Site Transports folder and choose Properties.
D. In the Replicate every text box, enter a value for the number of minutes between replication events.
E. Enter a cost value in the Cost text box or use the up/down arrows to select a value.

B.
E.

Explanation: Site link costs are defined separately for each site link. Molly needs to perform this step to reach the Properties dialog box for the site she is configuring. The value in the Cost text box determines the site link cost, with lower site link costs defining preferred replication paths. The default cost is 100.

The Properties dialog box of the Inter-Site Transports folder does not contain site link cost information.

The Properties dialog box of an intersite transport protocol does not contain site link cost information.

Molly would enter a value for the number of minutes between replication events in the Replicate every text box, if she needed to modify the replication interval, but not the site link cost.

5. Answer:

Philadelphia	A. Global catalog server
Pittsburgh	B. Universal group caching

Explanation: Because the Philadelphia office contains the largest majority of users, situating the global catalog servers at this office makes the most sense. These servers facilitate authentication and resource access across the domain boundary. Each domain should contain at least one global catalog server, including the empty root domain. Universal group caching is best suited for the office with the smaller amount of employees (Pittsburgh). Its use enables users in this office to log on to a local domain controller without the need to cross the slow WAN link to obtain universal group information.

Locating the global catalog servers in the Pittsburgh office would result in a large amount of network traffic across the slow link. Locating the global catalog servers in both offices would result in a large amount of network traffic across the slow link. No need exists for both global catalog servers and universal group caching at the same office.

Chapter 2

1. Answer: C

Explanation A. Ruth would modify this object if she needed to modify site links or force intersite replication. She does not need to modify this object in a single site network.

Explanation B. Ruth would modify this object if she needed to configure the scheduling of intersite replication. She does not need to modify this object in a single site network.

Explanation C. To modify the default intersite replication interval, Ruth must modify the Registry. She needs to go to the HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesNTDSParameters key and modify the Replicator notify pause after modify (secs) value. By default, this value is set to 300 seconds, but Ruth can increase it to any desired amount. This action modifies the delay between the time a change is made to Active Directory and the first notification of replication partners.

Explanation D. The Active Directory schema does not contain any objects that influence replication schedules, either intrasite or intersite.

2. Answers: A, C, F

Explanation A. The Directory Service log records events related to Active Directory replication, whereas the File Replication Service log records events related to FRS replication. FRS replication is used to replicate the SYSVOL folder among domain controllers.

Explanation B. Carl should check the output of the Netdiag command for DNS name registration failures.

Explanation C. Replmon enables Carl to monitor the status of Active Directory replication and display the Active Directory replication topology in a graphical format. He can check the consistency of replication between selected pairs of domain controllers. If replication has failed between a selected pair of domain controllers, DNS name registration problems may have occurred.

Explanation D. Replmon does not monitor DNS name registration failures.

Explanation E. Although Netdiag monitors network problems, it does not monitor replication failures.

Explanation F. Netdiag tests the condition and functionality of network clients, and verifies DNS name registrations. Its output assists Carl in insolating and troubleshooting network and connectivity problems.

3. Answers: B, C

Explanation A. To perform any type of restore operation on a domain controller, Gerry must restart the computer in Directory Services Restore mode, not Safe Mode.

Explanation B. Gerry needs to start the computer in Directory Services Restore mode and nonauthoritatively restore System State data from backup by using ntbackup.exe. After Gerry has brought SRV3 back online, the most recent Active Directory data is automatically replicated from the other domain controllers.

Explanation C. Gerry needs to start the computer in Directory Services Restore mode and nonauthoritatively restore system state data from backup by using ntbackup.exe. After Gerry has brought SRV3 back online, the most recent Active Directory data is automatically replicated from the other domain controllers.

Explanation D. If Gerry were to authoritatively restore system state data, then this restored data would be replicated to the other domain controllers, erasing any updates to Active Directory that had occurred since Tuesday.

Explanation E. FRS is automatically restored when the System State data is restored, and does not need to be restored manually.

4. Answer: D

Explanation A. Kelly should ensure that the replication topology includes the BDC; however, she should first make sure that the PDC emulator is operating and accessible to the BDC. If this is true, checking the replication topology should be the next step that she takes to resolve the problem.

Explanation B. For the BDC to function properly in the domain, the domain functional level should remain at Windows 2000 mixed. Only Windows 2000 and Windows Server 2003 domain controllers can operate at the Windows 2000 native functional level.

Explanation C. For the BDC to function properly in the domain, the domain functional level should remain at Windows 2000 mixed. However, you cannot roll the domain functional level back after it has been raised; Kelly would need to reinstall the entire domain if the domain functional level has been raised and it was essential to have the Windows NT 4.0 BDC remain online.

Explanation D. The BDC cannot receive updates to the Active Directory database if the PDC emulator is not functioning properly. Kelly may need to seize this role if the domain controller holding the role has failed and cannot be simply restarted. If the PDC emulator is functioning properly, she should try to ping this computer from the BDC and ensure that network connectivity is functioning properly.

5. Answer:

A. Select the UPN suffix to be removed and click Disable. E.
B. Select the UPN suffix to be removed and click Remove. B.
C. Select the UPN suffix to be removed and press the Delete key.
D. Select the Name Suffix Routing tab.
E. Right-click Active Directory Domains and Trusts and choose Properties.
F. Right-click the forest root domain and choose Properties.

Explanation: The Properties dialog box of Active Directory Domains and Trusts lists additional UPN suffixes that are available throughout the Active Directory forest. From this dialog box you can add new alternative UPN suffixes or remove those you do not need. You can remove UPN suffixes by selecting the required suffix and clicking the Remove button (but not press the Delete key).

The Trusts tab of the domain's Properties dialog box allows you to manage forest trusts. You can disable, but not delete, alternative UPN suffixes from the Name Suffix Routing tab of the trust's Properties dialog box. The Disable command is available from the Name Suffix Routing tab of a trust's Properties dialog box. This command allows you to disable, but not delete, a UPN suffix.

Chapter 3

1. Answer: D

Explanation A. It is not possible to assign permissions on files, folders, and printers directly to an OU. You can assign these permissions only to users or security groups.

Explanation B. Although Dan could complete this task by assigning permissions to individual users, this is not the best way to solve the problem, because it requires far more administrative effort (and is more prone to error) than assigning the permissions go a security group.

Explanation C. Dan would use a distribution group for creating an e-mail distribution list. This enables him to send e-mail messages to group members by simply sending the message to the group. He cannot use a distribution group to assign permissions.

Explanation D. The best way to assign permissions for Active Directory objects, such as files, folders, and printers, is to use security groups for the permissions assignment and add the required users to these groups.

2. Answers: A, E

Explanation A. Murray can use OUs to perform tasks such as deployment of most Group Policy settings and delegation of administrative control.

Explanation B. Although Murray can deploy most Group Policy settings to OUs, account policies are an exception because they can be configured only at the domain level.

Explanation C. Replication of Active Directory is configured only for domains (in the case of the domain partition), the entire forest (in the case of the configuration and schema partitions), or a specified subset of all domain controllers (in the case of application partitions).

Explanation D. Murray would use a distribution group to create e-mail distribution lists. He can also use a security group for this purpose, but he cannot use an OU.

Explanation E. Murray can use OUs to perform tasks such as deployment of most Group Policy settings and delegation of administrative control.

3. Answer: A

Explanation A. Smart cards provide security-critical computations that include digital signatures that can be used to verify the authenticity of documents.

Explanation B. Smart cards do not have the ability to encrypt documents. Jennifer needs to employ a solution such as Encrypting File System (EFS) for documents on servers or IPSec for documents and other files being transmitted across the network.

Explanation C. Smart cards do not store PKI information; this is the function of the Certification Authority (CA) servers used in conjunction with the smart card enrollment procedure.

Explanation D. Smart cards do not store digital signatures; however, they can store the private keys used to decrypt them.

4. Answer: B

Explanation A. In this scenario, Frank wants to have the ability to delegate administrative control at each location to a local user. This need points to the use of a geographical model of OU design. The scenario does not call for management according to business functions.

Explanation B. In this scenario, Frank wants to have the ability to delegate administrative control at each location to a local user. This need points to the use of a geographical model of OU design.

Explanation C. In this scenario, Frank wants to have the ability to delegate administrative control at each location to a local user. This need points to the use of a geographical model of OU design. The scenario does not call for management according to resource objects.

Explanation D. In this scenario, Frank wants to have the ability to delegate administrative control at each location to a local user. This need points to the use of a geographical model of OU design. No need exists for more than one level of OU, as would exist in a hierarchical model.

5. Answer: B

Explanation A. The ADMT tool is used to migrate accounts from a Windows NT 4.0 domain to an Active Directory domain, but not from one Active Directory domain or another.

Explanation B. To move a user account from one domain to another, Doug needs to use the Movetree command utility. This utility modifies the user account's security identifier (SID) to fit the new domain, but does not change its globally unique identifier (GUID).

Explanation C. The Copy command can be used only to create a copy of a user account with a new name but existing within the same container (domain, OU, etc.).

Explanation D. The Move command from the right-click menu in Active Directory Users and Computers can be used to move an account only within the domain in which it is located, and not between domains.

Chapter 4

1. Answers: B, E

Explanation A. The Security Templates snap-in allows you to define a custom security template that you can then use to analyze and configure security settings on computers. It does not perform the actual analysis.

Explanation B. You can use the Security Configuration and Analysis snap-in to analyze and configure computer security settings. This snap-in displays a list of discrepancies that it finds and allows you to upgrade a computer's security settings to those in a stored database.

Explanation C. These extensions enable you to modify the security policy of a site, domain, or OU. They do not compare computer security settings to a template.

Explanation D. IPSec Security Policies is a subnode in the Computer ConfigurationWindows Settings Security Settings node of Group Policy Object Editor that enables you to set the security level of network communication.

Explanation E. You can use the secedit /analyze command to analyze the security settings of a computer and then the secedit /configure command to configure security settings by applying settings from a template. You can script these tools to analyze and configure a series of computers.

2. Answer: A

Explanation A. By specifying Block Policy Inheritance on the Design OU, all GPOs applied at higher levels of the Group Policy hierarchy (site, domain, and Engineering OU) are blocked from applying to users and computers located in the Design OU. Note that if Adam needed to apply any policies from higher levels to the Design OU, he can specify No Override for these policies (or link them again to the Design OU).

Explanation B. If Adam were to specify Block Policy Inheritance on the Engineering OU, all GPOs applied at higher levels would be blocked from applying at the Engineering and lower level OUs. This would prevent the domain desktop policy from applying to users and computers in the Construction OU as well as the Design OU, which is not what is intended in this scenario.

Explanation C. Adam would use No Override if he wanted to prevent settings in a child OU from overwriting policy settings in the GPO on which it is applied. In this scenario, this specification would have no effect.

Explanation D. Adam would use No Override if he wanted to prevent settings in a child OU from overwriting policy settings in the GPO on which it is applied. In this scenario, this specification would prevent settings in the Design and Construction OUs from overwriting those in the Engineering OU, which is not what is intended.

3. Answers: B, E

Explanation A. This option prompts the user only during enrollment and not during use of the private key. It is intended for enrollment of smart card certificates, and provides a prompt for entering a PIN number.

Explanation B. By setting the This number of authorized signatures option to 1, the user is required to sign the request with a private key from a valid certificate in their certificate store. If this number is set to a value higher than 1, autoenrollment based on the template is disabled. This option is found on the Issuance Requirements tab of the certificate template's Properties dialog box.

Explanation C. By setting the This number of authorized signatures option to 1, the user is required to sign the request with a private key from a valid certificate in their certificate store. If this number is set to a value higher than 1, autoenrollment based on the template is disabled. This option is found on the Issuance Requirements tab of the certificate template's Properties dialog box.

Explanation D. The Valid existing certificate option allows the renewal of a valid certificate without the subject needing to meet issuance requirements at renewal time. It does not require users to provide signatures at issuance time.

Explanation E. The Prompt the user during enrollment and require user input when the private key is used option asks for user input during enrollment and use of the private key. This option is found on the Request Handling tab of the certificate template's Properties dialog box.

4. Answers: A, C, D, E

Explanation A. You can create GPOs that are linked to any site, domain, or OU within your Active Directory structure. This includes child domains and child OUs.

Explanation B. The Computers and Builtin containers are not OUs and you cannot create GPOs linked to these containers.

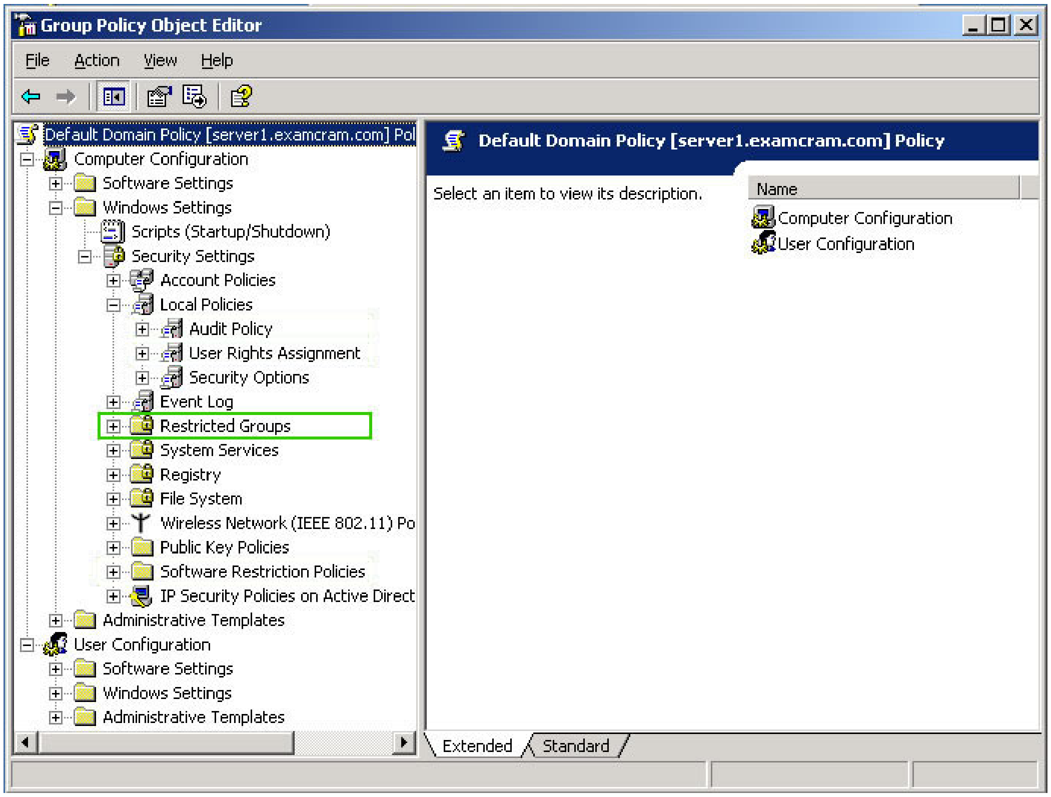
Explanation C. You can create GPOs that are linked to any site, domain, or OU within your Active Directory structure. This includes child domains and child OUs.

Explanation D. You can create GPOs that are linked to any site, domain, or OU within your Active Directory structure. This includes child domains and child OUs.

Explanation E. You can create GPOs that are linked to any site, domain, or OU within your Active Directory structure. This includes child domains and child OUs.

Explanation F. The Computers and Builtin containers are not OUs and you cannot create GPOs linked to these containers.

5. Answer:



Select an item to view its description.

Explanation: Restricted Groups is a new security option policy that allows you to determine who can be a member of a group, and what groups the group can be a member of. You can use this feature to define the membership of local groups such as the local Administrators group.

An audit policy would tell you who has added themselves to the local Administrators group but would not stop such additions from occurring. A software restriction policy would stop unapproved software from running and prevent many instances of viruses and corruption, but this was not what the question specified. There is no user rights policy that would deny local administrators the right to install software.

Chapter 5

1. Answers: A, D

Explanation A. RSoP in logging mode and the Gpresult command enable you to view the actual application of GPOs to a specified user and computer combination.

Explanation B. RSoP in planning mode allows you to simulate the proposed application of GPOs to users and/or computers.

Explanation C. Gpotool is used to monitor the health of GPOs on Windows 2000 domain controllers. It does not monitor the application of GPOs to specific users or groups, and is not available on servers running Windows Server 2003.

Explanation D. RSoP in logging mode and the gpresult command enable you to view the actual application of GPOs to a specified user and computer combination.

2. Answers: B, C, E

Explanation A. Planning mode enables you to simulate the proposed application of Group Policy. It does not provide error information with regard to failed policy application.

Explanation B. Logging mode enables you to determine which policies were applied successfully and which policies failed.

Explanation C. The RSoP Software Settings results in the details pane of the RSoP snap-in includes options for adding additional columns of information. By right-clicking in the details pane and selecting View, Add/Remove Columns, you can select additional columns. The Installed applications option lists information on applications that installed or failed to install.

Explanation D. This option from the View, Add/Remove Columns context menu does not provide the information you need to solve this problem. You need to select Installed Applications instead.

Explanation E. The Error Information tab provides information related to the reason why the package failed to install.

Explanation F. The Precedence tab provides information on which GPOs were applied and in what sequence for the policy whose properties you are viewing. It does not provide error information.

3. Answer: D

Explanation A. Tiffany should not link the GPO to the Accounting Computers GPO. Doing so would apply the policy to all users of the Accounting department when they are using computers located in this department. It would also not apply the policy to Accounting users when they are using computers located in other departments.

Explanation B. Tiffany should not link the GPO to the Accounting Computers GPO. Doing so would apply the policy to all users of the Accounting department when they are using computers located in this department. It would also not apply the policy to Accounting users when they are using computers located in other departments. In addition, the User Configuration node does not allow her to specify the server that hosts Software Update Services.

Explanation C. Although Tiffany should link the GPO to the Accounting Users OU, she cannot configure the policy from the User Configuration node. This node enables her to restrict access to the Windows Update Web site, but it does not allow her to specify the server that hosts Software Update Services.

Explanation D. By linking the GPO to the Accounting Users GPO, Tiffany ensures that settings in the GPO apply to all users in the Accounting department, regardless of the location of the computer they are using. And by using the Computer Configuration node, she can specify the server that hosts Software Update Services.

4. Answer: A

Explanation A. Sophie needs to follow these steps to upgrade the application. The Add Upgrade Package dialog box allows her to specify which package is being upgraded by the newly deployed version. The Package can upgrade over the existing package option retains the user's application preferences, document type associations, and so on.

Explanation B. These steps would upgrade the existing package as intended. However,
the Uninstall the existing package, then install the upgrade package option does not retain application preferences, document type associations, and so on. She should use this option if you are replacing the application with a completely different one, such as from a new vendor.

Explanation C. Sophie cannot upgrade an existing application by simply right-clicking this application and proceeding from its Properties dialog box. She must first deploy the upgraded application and then specify that it upgrades the existing one.

Explanation D. Sophie cannot upgrade an existing application by simply right-clicking this application and proceeding from its Properties dialog box. She must first deploy the upgraded application and then specify that it upgrades the existing one.

5. Answer: B

Explanation A. Charles can configure an audit policy by accessing the Group Policy Object Editor snap-in for the appropriate GPO and navigating to the Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy node. This node contains a series of events that can be audited for either success or failure. In this case, he needs Account Management events, which include items such as the creation, change, or deletion of a user or group account, and also the renaming, disabling, or enabling of a user account or change of password.

Explanation B. Charles can configure an audit policy by accessing the Group Policy Object Editor snap-in for the appropriate GPO and navigating to the Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy node. This node contains a series of events that can be audited for either success or failure. In this case, he needs Account Management events, which include items such as the creation, change, or deletion of a user or group account, and also the renaming, disabling, or enabling of a user account or change of password.

Explanation C. Charles can configure an audit policy by accessing the Group Policy Object Editor snap-in for the appropriate GPO and navigating to the Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy node. This node contains a series of events that can be audited for either success or failure. In this case, he needs Account Management events, which include items such as the creation, change, or deletion of a user or group account, and also the renaming, disabling, or enabling of a user account or change of password.

Explanation D. Charles can configure an audit policy by accessing the Group Policy Object Editor snap-in for the appropriate GPO and navigating to the Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy node. This node contains a series of events that can be audited for either success or failure. In this case, he needs Account Management events, which include items such as the creation, change, or deletion of a user or group account, and also the renaming, disabling, or enabling of a user account or change of password.