



www.chinatag.com

CHINATAG

Microsoft 70-294

**Planning, Implementing and Maintaining a
Microsoft Windows Server 2003 Active
Directory Infrastructure**

Study Guide

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

TABLE OF CONTENTS

List of Tables

Introduction

1. Active Directory

- 1.1 Active Directory Overview
 - 1.1.1 Directory Services
 - 1.1.2 Active Directory Objects
 - 1.1.3 Active Directory Schema
 - 1.1.4 Active Directory Components
 - 1.1.4.1 Logical Structure
 - 1.1.4.1.1 Domains
 - 1.1.4.1.2 Organizational Units
 - 1.1.4.1.3 Trees
 - 1.1.4.1.4 Forests
 - 1.1.4.2 Physical Structures
 - 1.1.4.2.1 Sites
 - 1.1.4.2.2 Domain Controllers
 - 1.1.5 Catalog Services
 - 1.1.5.1 The Global Catalog
 - 1.1.5.2 Global Catalog Functions
- 1.2 Active Directory Replication
- 1.3 Trust Relationships
- 1.4 Configuration and Change Management
- 1.5 Group Policies
- 1.6 Planning the Active Directory Infrastructure Design
 - 1.6.1 The Active Directory Infrastructure Design
 - 1.6.2 The Design Process
- 1.7 Administering Active Directory Objects
 - 1.7.1 Locating Active Directory Objects
 - 1.7.2 Using Saved Queries
 - 1.7.3 Moving Active Directory Objects
 - 1.7.3.1 The MoveTree Utility
 - 1.7.3.2 The ClonePrincipal
 - 1.7.3.3 The Active Directory Migration Tool

- 1.7.4 Controlling Access to Active Directory Objects
- 1.7.5 Delegating Administrative Control
- 1.7.6 Publishing Resources
 - 1.7.6.1 Setting Up and Managing Published Printers
 - 1.7.6.2 Setting Up and Managing Published Shared Folders
- 1.7.7 Auditing Access to Active Directory Objects
 - 1.7.7.1 Monitoring User Access to Shared Folders
 - 1.7.7.2 Monitoring User Sessions
 - 1.7.7.3 Sending Administrative Messages to Users

2. Installing and Administering Active Directory

- 2.1 Active Directory Installation Prerequisites
 - 2.1.1 Determining the Domain Structure
 - 2.1.2 Determining the Domain Name
 - 2.1.3 Active Directory Files and Folders
 - 2.1.4 DNS Configuration
- 2.2 Installing Active Directory
 - 2.2.1 Installing Active Directory Using the Active Directory Installation Wizard
 - 2.2.1.1 Creating the First Domain Controller for a New Domain
 - 2.2.1.2 Adding a New Domain Controller to an Existing Domain
 - 2.2.2 Installing Active Directory Using an Answer File
 - 2.2.2.1 Installing Active Directory Using the Network or Backup Media
 - 2.2.2.2 Installing Active Directory Using the Configure Your Server Wizard
 - 2.2.3 Removing Active Directory Services
 - 2.2.4 Verifying DNS Configuration Settings
- 2.3 Verifying the Active Directory Installation
- 2.4 Troubleshooting the Active Directory Installation and Removal
 - 2.4.1 Using the Directory Service Log
 - 2.4.2 Using the Network Connectivity Tester
 - 2.4.3 Using the Domain Controller Diagnostic Tool
 - 2.4.4 Using the Dcpromo Log Files
 - 2.4.5 Using the Active Directory Diagnostic Tool
- 2.5 Administering Active Directory
 - 2.5.1 Active Directory Administrative Consoles
 - 2.5.1.1 Active Directory Domains And Trusts
 - 2.5.1.1.1 Domain Functional Levels
 - 2.5.1.1.2 Forest Functional Levels
 - 2.5.1.1.3 UPN Suffixes
 - 2.5.1.2 Active Directory Sites And Services
 - 2.5.1.3 Active Directory Users And Computers
 - 2.5.1.4 Active Directory Schema Snap-In

- 2.5.2 Active Directory-Specific Support Tools
- 2.5.3 Backing Up Active Directory
- 2.5.4 Restoring Active Directory
 - 2.5.4.1 The Impact of an Authoritative Restore

3. Installing and Managing Domains, Trees, and Forests

- 3.1 Creating Multiple Domains, Trees, and Forests
 - 3.1.1 Creating Multiple Domains
 - 3.1.2 Creating Multiple Trees
 - 3.1.3 Creating Multiple Forests
- 3.2 Renaming and Restructuring Domains
 - 3.2.1 Renaming and moving a Domain Controller
 - 3.2.2 Domain Controller Roles
 - 3.2.2.1 The Global Catalog
 - 3.2.2.2 Master Operation Roles
 - 3.2.2.3 PDC Emulator
 - 3.2.2.4 RID Master
 - 3.2.2.5 Infrastructure Master
 - 3.2.2.6 Domain Naming Master
 - 3.2.2.7 Schema Master
 - 3.2.2.8 Seizing a Role Master
 - 3.2.3 Planning Operations Master Locations
 - 3.2.3.1 Planning Operations Master Locations for a Domain
 - 3.2.3.2 Planning the Operations Master Roles for the Forest
- 3.3 Managing Trust Relationships
 - 3.3.1 Trust Relationships
 - 3.3.2 Trust Types
 - 3.3.2.1 Forest Trusts
 - 3.3.2.2 Tree-Root and Parent-Child Trusts
 - 3.3.2.3 Shortcut Trusts
 - 3.3.2.4 Realm Trusts
 - 3.3.2.5 External Trusts
 - 3.3.3 Creating and Administering Trusts Using the Command Line

4. Configuring Sites and Managing Replication

- 4.1 Replication
- 4.2 Configuring Sites
 - 4.2.1 Creating Sites
 - 4.2.2 Creating Subnets
 - 4.2.3 Creating, Moving, and Removing Domain Controller Objects in a Site
 - 4.2.4 Designating a Site License Server

- 4.2.5 Site Links
- 4.2.6 Site Link Bridges
- 4.2.7 Bridgehead Servers

4.3 Creating and Configuring Connection Objects

- 4.3.1 Connection Transport
- 4.3.2 Connection Schedule

4.4 Configuring Global Catalog Servers

- 4.4.1 Universal Group Membership Caching Feature
- 4.4.2 Creating or Removing a Global Catalog

4.5 Configuring Application Directory Partitions

- 4.5.1 Application Directory Partitions
 - 4.5.1.1 Application Directory Partition Naming
 - 4.5.1.2 Application Directory Partition Replication
 - 4.5.1.3 Application Directory Partitions and Domain Controller Demotion
- 4.5.2 Security Descriptor Reference Domain
- 4.5.3 Managing Application Directory Partitions
- 4.5.4 Adding or Removing an Application Directory Partition Replica
- 4.5.5 Displaying Application Directory Partition Information
- 4.5.6 Setting Replication Notification Delays
- 4.5.7 Setting the Application Directory Partition Reference Domain

4.6 Monitoring and Troubleshooting Replication

- 4.6.1 Active Directory Replication Monitor
- 4.6.2 Repadmin.exe: Replication Diagnostics Tool
- 4.6.3 Directory Services Utility
- 4.6.4 Common Active Directory Replication Problems

5. Administering User and Groups

5.1 User Account Types

5.2 Creating User Accounts

5.3 User Profiles and Home Folders

- 5.3.1 Creating User Profiles
- 5.3.2 Home Folders

5.4 Maintaining User Accounts

- 5.4.1 Unlocking User Accounts and Resetting Passwords

5.5 Administering Groups

- 5.5.1 Group Scopes
- 5.5.2 Default Groups

- 5.5.3 The Everyone Group and the Anonymous User Group
- 5.5.4 Built-In Local Groups

5.6 Implementing Groups

- 5.6.1 Group Nesting
- 5.6.2 Creating Groups
- 5.6.3 Adding a User to a Group

6. Group Policy and Group Policy Objects

6.1 Overview

- 6.1.1 Group Policy Settings
- 6.1.2 Group Policy Inheritance
- 6.1.3 Filtering GPO Scope
 - 6.1.3.1 Using Security Groups
 - 6.1.3.2 Using WMI Queries

6.2 Delegating Control of GPOs

6.3 Planning and Implementing Group Policy

- 6.3.1 Planning GPOs
- 6.3.2 Planning Administrative Control
- 6.3.3 Linking Group Policy Objects
- 6.3.4 Controlling the Processing of Group Policy
- 6.3.5 Refreshing Group Policy at Established Intervals
- 6.3.6 Resolving Conflicts Between Group Policy Settings
- 6.3.7 Delegating Control of a GPO

6.4 Resultant Set of Policy (RSoP)

- 6.4.1 Generating RSoP Queries
- 6.4.2 Delegating Control of RSoP

6.5 Folder Redirection and Offline Files

- 6.5.1 Folder Redirection
- 6.5.2 Setting Up Folder Redirection
- 6.5.3 Home Folders
- 6.5.4 Offline Files

6.6 Troubleshooting Group Policy

7. Software Deployment

7.1 Software Installation Extension

- 7.1.1 Assigning Applications
- 7.1.2 Publishing Applications
- 7.1.3 The Windows Installer Service

- 7.1.3.1 Windows Installer Packages
- 7.1.3.2 Application (.zap) Files

7.2 Software Deployment

- 7.2.1 Deploying Software with Group Policy
- 7.2.2 Using DFS to Manage SDPs

7.3 Maintaining Software Deployed with Group Policy

- 7.3.1 Redeploying Applications Deployed with Group Policy
- 7.3.2 Upgrading Applications Deployed with Group Policy
- 7.3.3 Removing Deployed Software

8. Administering Active Directory Security with Group Policy

8.1 Active Directory Security Provided by Group Policy

- 8.1.1 Security Settings
- 8.1.2 Auditing and Security Logging
- 8.1.3 Security Configuration And Analysis

8.2 Implementing Software Restriction Policies

8.3 Implementing an Audit Policy

- 8.3.1 Audit Policies
- 8.3.2 Configuring Objects for Auditing

8.4 The Security Log

- 8.4.1 Configuring the Security Log
- 8.4.2 Archiving the Security Log

8.5 Security Templates

- 8.5.1 Predefined Security Templates
 - 8.5.1.1 Default Security Templates
 - 8.5.1.2 Secure Security Templates
 - 8.5.1.3 High Security Templates
 - 8.5.1.4 Backward Compatible Security Templates
 - 8.5.1.5 Miscellaneous Security Templates
- 8.5.2 Managing Security Templates
- 8.5.3 Enforcing Default Security Settings on New Computers
- 8.5.4 Security Configuration And Analysis

9. Managing Active Directory Performance

9.1 Monitoring Performance

- 9.1.1 System Monitor
 - 9.1.1.1 Performance Objects and Performance Counters
 - 9.1.1.2 System Monitor Properties

9.1.1.3 Monitoring Active Directory Performance

9.2 Performance Logs And Alerts

9.2.1 Counter and Trace Logging Requirements

9.2.2 Creating a Counter Log

9.2.3 Alerts

9.3 Managing Active Directory Performance from the Command Line

9.4 Optimizing and Troubleshooting Active Directory Performance

9.4.1 Establishing a Baseline

9.4.2 Analyzing Performance-Monitoring Results

LIST OF TABLES

TABLE 1.1	Common Active Directory Objects
TABLE 1.2	Find Dialog Box Options
TABLE 1.3	Standard Active Directory Object Permissions
TABLE 2.1	Netdiag Command Line Switches
TABLE 2.2	Dcdiag Command Line Switches
TABLE 2.3	Active Directory-Specific Support Tools
TABLE 3.1	Netdom Trust Parameters
TABLE 4.1	Dsastat Parameters
TABLE 5.1	The Dsadd Command-line Parameters
TABLE 6.1	The Gpresult Command Parameters
TABLE 8.1	The SecEdit Command Parameters

Planning, Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure

Exam Code: 70-294

Certifications:

Microsoft Certified (MCP)

Microsoft Certified Systems Engineer (MCSE 2003)

Core

Prerequisites:

None

About This Study Guide

This Study Guide provides all the information required to pass the Microsoft 70-294 exam – Planning, Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure. It however, does not represent a complete reference work but is organized around the specific skills that are tested in the exam. Thus, the information contained in this Study Guide is specific to the 70-294 exam and not only to Planning, Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure. It includes the information required to answer questions related to the installation of Windows Server 2003, Windows 2000 Server, Windows XP Professional, Windows 2000 Professional, Windows NT, and Windows 98 that may be asked during the exam. Topics covered in this Study Guide include: Planning and Implementing an Active Directory Infrastructure; Planning a Strategy for Placing Global Catalog Servers; Network Traffic Considerations when Placing Global Catalog Servers; Evaluating the Need to Enable Universal Group Caching; Planning Flexible Operations Master Role Placement; Planning for Business Continuity of Operations Master Roles; Identifying Operations Master Role Dependencies; Implement an Active Directory Directory Service Forest and Domain Structure; Creating the Forest Root Domain; Creating a Child Domain; Creating and Configuring Application Data Partitions; Installing and Configuring an Active Directory Domain Controller; Setting an Active Directory Forest and Domain Functional Level based on Requirements; Establishing Trust Relationships, including External Trusts, Shortcut Trusts, and Cross-Forest Trusts; Implementing an Active Directory site topology; Configuring Site Links; Configuring Preferred Bridgehead Servers; Planning an Administrative Delegation Strategy; Planning an Organizational Unit (OU) Structure and a Security Group Hierarchy based on Delegation Requirements; Managing and Maintaining an Active Directory Infrastructure; Managing an Active Directory Forest and Domain Structure; Managing Trust Relationships; Managing Schema Modifications; Adding or Removing a UPN Suffix; Managing an Active Directory site; Configuring Replication Schedules; Configuring Site Link Costs; Configuring Site Boundaries; Monitoring Active Directory Replication Failures with Replication Monitor, Event Viewer, and Support Tools; Monitoring Active Directory Replication and File Replication Service (FRS) Replication; Restoring Active Directory Directory Services; Performing an Authoritative and Nonauthoritative Restore Operation; Troubleshoot Active Directory; Diagnosing and resolving

issues related to Active Directory Replication, Operations Master Role Failure, and the Active Directory Database; Planning and Implementing User, Computer, and Group Strategies; Planning a Security Group Strategy and a User Authentication Strategy; Creating a Password Policy for Domain Users; Planning an OU Structure; Analyzing the Administrative Requirements and Group Policy Requirements for an OU; Implementing an OU Structure; Creating an OU; Delegating Permissions for an OU to a User or a Security Group; Moving Objects within an OU Hierarchy; Planning and Implementing Group Policy; Planning Group Policy strategy using Resultant Set of Policy (RSOP) Planning Mode; Planning a Strategy for Configuring the User and Computer Environment using Group Policy; Configuring the User Environment using Group Policy; Distributing Software using Group Policy; Redirecting Folders using Group Policy; Configuring User Security Settings using Group Policy; Deploying a Computer Environment by Using Group Policy; Managing and Maintaining Group Policy; Troubleshooting Issues related to Group Policy Application Deployment; Maintaining Installed Software using Group Policy; Distributing Updates to Software Distributed by Group Policy; Configuring Automatic Updates for Network Clients using Group Policy; and Troubleshooting the Application of Group Policy Security Settings.

Intended Audience

This Study Guide is targeted specifically at people who wish to take the Microsoft MCSE exam 70-294 exam – Planning, Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure. This information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex and require an understanding of material provided for the CompTIA A+, Network+ and Server+ exams. Study Guides for these exams are available from TestKing.com.

Note: There is a fair amount of overlap between the 70-294 and the 70-293 and 70-290, exams. Don't skim over the information that seems familiar. Read over it again to refresh your memory.

How To Use This Study Guide

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work.
- If possible, perform all the walk-throughs that are included in this Study Guide to gain practical experience, referring back to the text so that you understand the information better. Remember, it is easier to understand how tasks are performed by practicing those tasks rather than trying to memorize each step.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Note: Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

1. Active Directory

1.1 Active Directory Overview

1.1.1 Directory Services

On a computer network, many objects are stored in a directory. Users must be able to find and use these objects. Administrators must be able to manage the use of these objects. A **directory service** stores all the information needed to use and manage these objects in a centralized location and simplifies the locating and managing process. It is the central authority that manages the identities and relationships between resources, enabling them to work together. A directory service supplies fundamental operating system functions and must be coupled with the management and security mechanisms of the operating system to protect the privacy of the network. It also forms an integral part of an organization's ability to maintain the network infrastructure, perform system administration, and control the user experience of a company's information systems.

Active Directory is the directory service in Windows Server 2003. It includes the following features:

- **Centralized** data store in a single, distributed data store, allowing users easy access to the information from any location. This needs less administration and improves the organization of data.
- **Scalability**, allowing you to meet network requirements through the configuration of domains and the placement of domain controllers. Active Directory allows millions of objects per domain and uses indexing and replication techniques to speed performance.
- **Extensibility** of the Active Directory database (the schema) allows for customized information.
- **Manageability** through hierarchical organizational structures that make it easier to control administrative and other security settings, and for users to locate network resources.
- Integration with the **Domain Name System (DNS)**, which enables replication to other Active Directory domain controllers.
- **Client configuration management.**
- **Policy-based administration.**
- **Replication** of information which enables you to update the directory at any domain controller and replicates directory changes. Because multiple controllers are used, replication continues.
- Active Directory **authentication and authorization** services, which provide protection for data while minimizing barriers to doing business over the Internet.
- **Directory-enabled applications**, which makes it easier to manage applications. It also provides a development environment through Active Directory Service Interfaces (ADSI).
- **Interoperability** with other directory services.
- Signed and encrypted **LDAP** traffic. Active Directory tools in Windows Server 2003 sign and encrypt all including Lightweight Directory Access Protocol (LDAP) version 3 traffic by default. This guarantees that the data comes from a reliable source.

1.1.2 Active Directory Objects

Active Directory is organized into objects, which are named sets of attributes that represent a network resource. Object attributes are characteristics of objects in the directory. Objects known as **containers** can contain other objects.

Every object in Active Directory has a name, and LDAP standards determine how the objects are named. Active Directory uses a variety of object naming conventions: distinguished names, relative distinguished names, globally unique identifiers, and user principal names.

- Every object in Active Directory has a **distinguished name (DN)** that identifies the object and contains enough information for a client to retrieve the object from the directory. The DN includes the name of the domain holding the object and the complete path through the container hierarchy to the object. DNs must be unique because Active Directory does not allow duplicate DNs.
- Active Directory supports querying by attributes, so an object may be located even if the exact DN is unknown. The **relative distinguished name (RDN)** of an object is the part of the name that is an attribute of the object itself.
- A **globally unique identifier (GUID)** is a 128-bit hexadecimal number that is guaranteed to be unique within the enterprise. GUIDs are assigned to objects when the objects are created. The GUID never changes. Applications can store the GUID of an object and use it to retrieve that object regardless of its DN. A GUID is unique across all domains, so you can move objects from domain to domain and they will still have a unique identifier.
- Each user account has a **user principal name (UPN)**. The UPN consists of a user account name and a domain name identifying the domain in which the user account is located.

Some common Active Directory objects and the information pertaining to it that is stored in Active Directory are listed in Table 1.1.

TABLE 1.1: *Common Active Directory Objects*

Object Type	Description
User account	Information, such as user logon name, that allows a user to log on to a Windows Server 2003 domain. This information has optional fields including first name, last name, display name, telephone number, e-mail, and home page.
Contact	Information about a person with a connection to the organization. This information also has optional fields including telephone number, e-mail, address, and home page.
Group	A collection of user accounts, groups, or computers that you can create and use to simplify administration.
Shared folder	A pointer, i.e., the address, to the shared folder.
Printer	A pointer to a printer.
Computer	The information about a computer that is a member of the domain.
Domain controllers	The information about a domain controller. This can include optional descriptions for the Domain Controller; the Domain

	Name System (DNS) name; the pre-Windows 2000 name; the operating system version on the domain controller; the location; and the user account name of the user responsible for managing the domain controller.
Organizational Unit (OU)	Containers which contains other objects, including other OUs, and are used to organize Active Directory objects.

1.1.3 Active Directory Schema

The Active Directory schema defines objects that may be stored in Active Directory. A Schema definition can be administered in the same manner as the rest of the objects in Active Directory. The schema is defined by two types of objects: schema class objects and schema attribute objects. Class objects and attribute objects, which are collectively referred to as **schema objects** or **metadata**, are defined in separate lists within the schema.

- **Schema class objects** describe the Active Directory objects that can be created.
- **Schema attribute objects** define the schema class objects they are associated with.

You can extend the schema by defining new classes and attributes for existing classes. Extending the schema is an advanced operation. Because schema cannot be deleted, and is replicated automatically, you must plan and prepare carefully before extending it.

1.1.4 Active Directory Components

Active Directory components are used to form a directory structure that meets the needs of your organization. It represents logical and physical structures in an organization. Domains, organizational units (OUs), trees, and forests are logical structures while sites and domain controllers are physical structures. Active Directory separates the logical structure from the physical structure.

1.1.4.1 Logical Structure

In Active Directory, you group resources in a logical structure using domains, OUs, trees, and forests. Grouping resources allows a user to find a resource by its name, making the network's physical structure transparent to users.

1.1.4.1.1 Domains

Domains are core units of logical structure in Active Directory. A domain comprises computer systems and network resources that share a logical security boundary. Although a domain can cross physical locations, all domains maintain their own security policies and security relationships with other domains. They can be created to define functional boundaries such as those between administrative units, or to group of resources or servers that use a common domain namespace.

The **first domain** that is created in Windows Server 2003 network is called the **forest root domain**. When other domains are created on the network, they added to the root domain to form the tree structure or the forest structure, depending on the domain name requirements.

A **tree** is a hierarchical arrangement of Windows Server 2003 domains that share a **contiguous namespace**. In such an arrangement the root domain name is attached as a suffix to the new domain names. The new domain is called a child domain of an existing parent domain and has a **two-way, transitive trust relationship** with its parent domain. Thus, a domain tree structure is formed by adding child domains to the root domain. The root domain contains the configuration and schema data for the tree. As child domains are added to the domain tree, Active Directory partitions are replicated to one or more domain controllers within each of the domains.

A **forest** can either consist of a **single tree** or **number of trees** that do not share a contiguous namespace but do share a common **schema** and **global catalog**. In this arrangement, every tree root domain has a **transitive trust relationship** with the root domain. A single tree that is not related to any other tree constitutes a **forest of one tree**. The root domain contains the configuration and schema data for all trees in the forest.

Both a tree and a forest are namespaces, which is a bounded area in which a name can be resolved. Using a common namespace allows you to unify and manage multiple hardware and software environments in your network. There are two types of namespaces:

- **Contiguous namespace.** The name of the child object in an object hierarchy always contains the name of the parent domain. A tree is a contiguous namespace because the name of any child object in a tree always contains the name of the parent tree.
- **Disjointed namespace.** The names of a parent object and of a child of the same parent object are not directly related to one another. A forest is a disjointed namespace because all trees in a forest do not share a common naming structure.

1.1.4.1.2 Organizational Units

An **OU** is a container that contains objects such as user accounts, groups, computers, printers, applications, file shares, and other OUs from the same domain. OUs allow administrators to group domains and child domains with similar administrative and security characteristics into administrative. A domain usually comprises one or more OUs arranged hierarchically. OUs provide levels of administrative authority for applying **Group Policy** settings and delegating administrative control. The latter allows an administrator to delegate administrative duties for certain Active Directory objects to non-administrative users while Group Policy is used to allow administrators to specify Group Policy settings for a site, domain, or organizational unit. Active Directory then enforces these Group Policy settings for all users and computers in the container.

Your OU structure can model the physical organizational, geopolitical, or administrative structure of your company. You can combine objects into a logical hierarchy of OUs that represent:

- Your company's **organizational model**, in which case it is based on departmental or geographical boundaries; or
- Your company's **administrative model**, in which case it is based on which administrators are responsible for managing specific users and resources across the network.

To create an OU within a domain or child domain, do the following:

- Click on the **START** button to display the **Start Menu**.
- Point to **ALL PROGRAMS**.

- Click on **ADMINISTRATIVE TOOLS**.
- Click **ACTIVE DIRECTORY USES AND COMPUTERS**.
- Right-click the **Domain**.
- Click **NEW**.
- Then select **ORGANIZATIONAL UNIT**.
- In the **OU** dialog box, type the name of the new Organizational unit in the **Name** box.
- Then click **OK**.

The primary reason for defining an OU is to delegate administration. Delegating administration is the assignment of information technology (IT) management responsibility for a portion of the namespace, such as an OU, to an administrator, a user, or a group of administrators or users. In the Windows Server 2003 operating system, you can delegate administration for the contents of an OU (all users, computers, or resource objects in the OU) by granting administrators specific permissions for an OU on the OU's access control list. An access control list (ACL) is the mechanism for limiting access to certain items of information or certain controls based on users' identity and their membership in various groups.

Once you determine the OUs needed for your organization, you can add OUs to other OUs to form a hierarchy of administrative control. Hierarchies consist of one layer of OUs, called top-level OUs, under which are arranged various layers of second-level OUs. Hierarchies for delegating administration can reflect location, business function, object type and combination.

There are two types of administrative responsibility you can delegate for an OU: **Full control** and **Control for object classes**. By default, only domain administrators have full control over all objects in a domain. Domain administrators are responsible for creating the initial OU structure, repairing mistakes, and creating additional domain controllers. It is usually sufficient to allow only domain administrators full control over objects in a domain. However, if there are units in the organization that need to determine their own OU structure and administrative models, you can provide them with this permission by delegating full control. When determining whether to delegate full control for an OU, you must determine which areas in the organization need to be allowed to change OU properties and to create, delete, or modify any objects in the OU. If more restrictive control is appropriate, you can accomplish this by delegating control of specific object classes for an OU. Although there are many object classes in the schema, you need to consider only the object classes in which administrators will create objects. Such object classes typically include user account objects, computer account objects, group objects, and OU objects. When determining whether to delegate control of object classes, for each object class that your administrators will create in Active Directory you must determine which areas in the organization should be granted full control over objects of this class in the OU; which should be allowed to create objects of this class and thus have full control over these objects and which should be allowed to modify only specific attributes for or perform specific tasks pertaining to existing objects of this class.

1.1.4.1.3 Trees

A tree is a grouping of one or more Windows Server 2003 domains that is created by adding one or more child domains to a parent domain. Domains in a tree share a contiguous namespace and a hierarchical naming structure. By creating a hierarchy of domains in a tree, you can retain security and allow for administration within an OU or within a single domain of a tree. The tree structure allows for organizational changes.

1.1.4.1.4 Forests

A forest is a grouping or hierarchical arrangement of one or more separate and independent domain trees. All domains in a forest share a common schema. All domains in a forest share a common global catalog. All domains in a forest are linked by two-way transitive trusts. Trees in a forest have different naming structures. Domains operate independently, but communication is possible across the entire organization

The forest functional level provides a way to enable forest-wide Active Directory features within your network environment. Three forest functional levels are available: Windows 2000 (default), Windows Server 2003 interim, and Windows Server 2003. You can only raise the functional level of a forest if the domain controllers are running the appropriate version of Windows.

1.1.4.2 Physical Structures

The physical components of Active Directory are sites and domain controllers. These components are used to develop a directory structure that reflects the physical structure of your organization.

1.1.4.2.1 Sites

A site is a combination of one or more IP subnets connected by a highly reliable and fast link to localize network traffic as much as possible. Typically, a site has the same boundaries as a local area network (LAN). An available bandwidth, i.e., the average amount of bandwidth that is available for use after normal network traffic is handled, of 128 Kbps is sufficient for a site.

With Active Directory, sites are not part of the namespace as sites only contain computer and connection objects used to configure replication between sites.

1.1.4.2.2 Domain Controllers

A domain controller is a computer running Windows Server 2003 that stores a replica of the domain directory (local domain database). The functions of domain controllers are as follows:

- Each domain controller stores and manages a copy of all Active Directory information for that domain.
- Domain controllers automatically replicate directory information in the domain to each other and immediately replicate important updates. **Operations master roles** are special roles assigned to one or more domain controllers in a domain to perform single-master replication.
- Domain controllers detect collisions
- Having more than one domain controller provides fault tolerance
- Domain controllers manage all aspects of users' domain interaction.

You must place domain controllers in sites which reflect your organization's physical structure and optimize replication and authentication.

1.1.5 Catalog Services

1.1.5.1 The Global Catalog

Active Directory allows users and administrators to find objects only in their domain. Finding objects outside the domain requires a mechanism that allows the domains to act as one entity. A catalog service contains selected information about all objects of all the domains in the directory, which is useful in doing searches outside the domain. The global catalog is the catalog service provided by Active Directory.

The **global catalog** is the central repository of information about objects in a tree or forest. A global catalog is created automatically on the initial domain controller in the forest. A domain controller that holds a copy of the global catalog is called a **global catalog server**. You can designate any domain controller in the forest as a global catalog server. It stores a full replica of all object attributes in the directory for its host domain and a partial replica of all object attributes contained in the directory for every domain in the forest. The partial replica stores attributes frequently used in search operations. Attributes are marked for replication in the global catalog when they are defined in the Active Directory schema. Object attributes replicated to the global catalog inherit the same permissions as in source domains which ensures the data is secure.

1.1.5.2 Global Catalog Functions

The global catalog (GC) allows a user to log on to a network by providing **universal group membership information** to a domain controller when a logon process is initiated and it enables finding directory information regardless of which domain in the forest actually contains the data.

When a user logs on to the network, the GC provides universal account group membership information for the account to the domain controller processing the information. The GC server role is held if there is only one domain controller. If there are many domain controllers, one is assigned the GC. If a GC is unavailable, the user can only log on to the local computer unless the site has been configured to **cache universal group membership lookups** when processing user logon attempts.

The GC responds to user and programmatic queries anywhere in the tree or forest with maximum speed and minimum network traffic. A single GC contains information about all objects in all domains in the forest, thus, a query about an object that is not contained in the local domain can be resolved by a GC server in the domain in which the query is initiated.

1.2 Active Directory Replication

Replication enables changes to a domain controller to be reflected in all domain controllers. Directory information is replicated to domain controllers within and among sites.

The information stored in the directory is logically partitioned into four categories. Each of these is referred to as a directory partition or a naming context, and is a unit of replication. The directory contains the following partitions:

The Query Process

A query is a request made by a user to the global catalog (GC) in order to retrieve, modify, or delete Active Directory data.

The query process is as follows:

1. The client queries its DNS server for the location of the GC server.
2. The DNS server returns the IP address of the domain controller assigned as the GC server.
3. The client queries the IP address of the GC server to port 3268 on the GC server.
4. The GC server processes the query.
5. If the GC contains the attribute of the object being searched for, it provides a response to the client. If the GC does not contain the attribute of the object being searched for, the query is referred to Active Directory.

- **Schema partition**, which defines the objects that **can be created** in the directory and the attributes those objects may have. This data is common to all domains in a forest and is replicated to all of them.
- **Configuration partition**, which describes the **logical structure** of the deployment, including data such as domain structure or replication topology. This data is also common to all domains in a forest and is replicated to all of them.
- **Domain partition**, which describes all the objects in a domain. This data is **domain-specific** and is not replicated to other domains.
- **Application Directory partition**, which stores dynamic **application-specific data** in Active Directory. It allows you to control the scope of replication and the placement of replicas without adversely affecting network performance. This partition can contain any type of object except **security principals**.

A **domain controller** stores and replicates the schema partition data and the configuration partition data for a forest, as well as the domain partition data for its domain.

A **global catalog** stores and replicates the schema partition data and the configuration partition data for a forest, as well as a partial replica containing commonly used attributes for all directory objects in the forest. It also has a full replica containing all attributes for all directory objects in the domain where the global catalog is located

Active Directory replicates information either within a site, in which case it is called intrasite replication; or between sites, which is called intersite replication.

- In **Intrasite Replication**, the Windows Server 2003 **knowledge consistency checker (KCC)** generates a topology for replication among domain controllers in the same domain. The topology defines the path for directory updates to pass between domain controllers. The KCC determines which servers replicate with each other and designates certain domain controllers as replication partners. Domain controllers can have more than one replication partner. The KCC then builds connection objects that represent replication connections between the replication partners.

The KCC analyzes the replication topology within a site every 15 minutes. If you add or remove a domain controller from the network or site the KCC reconfigures the topology.

When more than seven domain controllers are added to a site, the KCC creates more connection objects so that if a change occurs at a domain controller, replication partners can ensure that no domain controller is more than three replication hops from another domain controller.

- In **Intersite Replication** between sites, a single KCC generates all connections between the sites. Active Directory uses the network connection information to generate connection objects that provide efficient replication.

1.3 Trust Relationships

A trust relationship is a link between two domains in which the trusting domain honors the logon authentication of the trusted domain.

Trusts have a **method of creation**, which means a trust relation can be created manually (explicitly) and/or automatically (implicitly); **transitivity**, which means a trust relation can either not be bound by the domains in

the trust relationship (transitive), or they can be bound by the domains in the trust relationship (non-transitive); and **direction**, which means a trust relation be one-way or two-way. A one-way trust is a single trust relationship.

Active Directory supports the following forms of trust relationships:

- **Tree-root trust**, which is implicitly established when you add a **tree root domain** to a forest. A tree-root trust can only be set up between the roots of two trees in the same forest. The trust is **transitive** and **two-way**.
- **Parent-child trust**, which is implicitly established when you create a **child domain** in a tree. This trust relationship makes all objects in the domains of the tree available to all other domains in the tree. The trust is also **transitive** and **two-way**.
- **Shortcut trust**, which you must explicitly create between **two domains in a forest** and can be used to improve user logon times. The trust is **transitive** and can be **one-way or two-way**.
- **External**, which you must explicitly create between Windows Server 2003 domains that are in different forests, or between a Windows Server 2003 domain and a domain that has a domain controller running Windows NT 4 or earlier. This trust is used when users need access to resources in a Windows NT 4 domain or a domain within a separate forest, which cannot be joined by a forest trust. The trust is **nontransitive** and can be **one-way or two-way**.
- **Forest trust**, which you must explicitly create between **two forest root domains**. This trust allows all domains in one forest to **transitively** trust all domains in the other forest. The trust is **transitive** and can be **one-way or two-way** but is available only when the forests are at the Windows Server 2003 **functional level**.
- **Realm trust**, which you must be explicitly create between a **non-Windows Kerberos realm and a Windows Server 2003 domain**. This trust provides **interoperability** between the Windows Server 2003 domain and any realm used in Kerberos version 5 implementations and can be **transitive or nontransitive** and **one-way or two-way**.

1.4 Configuration and Change Management

Configuration and change management is a set of Windows Server 2003 features that simplify computer management tasks. It includes the User Data Management, Software Installation and Maintenance, User Settings Management, and Computer Settings Management features, (collectively called the IntelliMirror management technologies). Change and configuration management also includes the Remote Operating System (OS) Installation technologies.

- In **User Data Management**, data and documents follow the users so they can access the data they need.
- In **Software Installation and Maintenance**, software follows the users so they have the software they need.
- In **User Settings Management**, user settings follow users and they can see their preferred desktop arrangements.
- In **Computer Settings Management**, administrators can define how computers customization and restriction on the network.
- In **Remote Installation Services**, administrators can enable remote installation of Windows XP; Windows Server 2003; Windows 2000 Professional; and Windows 2000 Server on new or replacement computers without pre-installation or on-site technical support.

1.5 Group Policies

Group policies are collections of user and computer configuration settings that can be linked to computers, sites, domains, and OUs to specify the behavior of users' desktops. To create a specific desktop configuration for a specific group of users, you create Group Policy Objects (GPOs), which are collections of Group Policy settings. All computers running Windows Server 2003 has one local GPO and might be subject to Active Directory–based GPOs. Local GPOs are overridden by nonlocal GPOs. Active Directory–based GPOs can apply to users or computers. They are applied hierarchically from the least restrictive group (site) to the most restrictive group (OU) and are cumulative.

GPOs are applied in the following order:

- Each server running Windows Server 2003 has one GPO stored **locally**. These are applied first.
- Any GPOs that have been linked to the **site** are applied next. GPO application is synchronous; the administrator specifies the order of GPOs linked to a site.
- The next GPOs to be applied are the **Domain**-linked GPOs, which are applied synchronously; the administrator specifies the order of GPOs linked to a domain.
- Finally, GPOs linked to **OUs** are applied. GPOs linked to the OU highest in the Active Directory hierarchy are applied first, followed by GPOs linked to its child OU, and so on. Finally, the GPOs linked to the OU that contains the user or computer is applied. One, many, or no GPOs can be linked at the level of each OU in the Active Directory hierarchy. If many group policies are linked to an OU, they are applied in an order specified by the administrator.

The default order of processing Group Policy settings may have exceptions if the computer is a member of a workgroup or if any of the **No Override**, **Block Policy Inheritance**, or **Loopback** settings invoke for a GPO.

The **Resultant Set of Policy (RSOP) Wizard** is provided to make policy implementation and troubleshooting easier. It is a query engine working in two modes: logging mode and planning mode. In logging mode, the wizard polls existing policies and any applications associated with a particular user or computer and reports the results of the query. In planning mode, the wizard questions a planned policy implementation and reports the query results.

Note: Group Policy applies only to **Windows 2000, Windows Server 2003** and **Windows XP Professional**, but not to earlier versions of the Windows operating system.

1.6 Planning the Active Directory Infrastructure Design

1.6.1 The Active Directory Infrastructure Design

An Active Directory infrastructure design should represent your organization's network infrastructure. Your Active Directory infrastructure design is used to determine how you will configure Active Directory to store information about objects on your network and make the information available to users and network administrators. It is the key to the success of your Windows Server 2003.

To develop an effective Active Directory infrastructure design, you must assemble the design team, the business and technical analyses, and a test environment.

When **assembling the design team**, you must identify the people in your organization that should be involved in the design process and form them into team. You may decide to employ a multi-level team design to ensure that all aspects of your organization are addressed in your Active Directory implementation. The design team members selected for each panel should commit their time and talents throughout the design process to ensure that the infrastructure design meets the requirements of their organization. The three panels are:

- **Infrastructure designers**, which should include the personnel involved in designing your Active Directory infrastructure
- **Staff**, which should include the personnel throughout the organization who carry out daily operations
- **Management**, which should include the management level personnel who approve business decisions within the organization

After a design team is assembled, the next design tools needed are analyses of your organization's **business and technical environments**. These analyses define how it organizes and manages its non-technical resources as well as its technical resources.

After you complete your infrastructure design you should **test** it in a test environment. A test environment is a simulation of your production environment that allows you to test parts of your Windows Server 2003 deployment without risk to your organization's network.

1.6.2 The Design Process

The Active Directory infrastructure design process consists of four stages: creating a forest plan; creating a domain plan; creating an OU plan; and creating a site topology plan. During each of these stages, you consult your business and technical analysis documents, assess your organization's requirements and evaluate any changes planned to address growth and scalability issues.

- In the **forest plan**, you analyze your organization's requirements to determine the number of Active Directory forests it requires. You should strive to create only one forest for your organization, but you might need to use multiple forests in situations where network administration is separated into autonomous groups with no trust relationships; where business units are politically separated into autonomous groups; where business units must be maintained separately; where there is a need to isolate the schema, configuration container, or global catalog; and/or where there is a need to limit the scope of the trust relationship between domains or domain trees.
- In the **domain plan**, you analyze your organization's requirements to determine the number of domains it requires. You should minimize the number of domains. Once you've created a domain, the domain cannot be easily moved or renamed. You might need to consider using multiple domains to meet security policy settings; to meet special administrative requirements (legal or privacy concerns); to optimize replication traffic; to retain Windows NT domains; and/or to establish a distinct namespace.

The second step in creating a domain plan is to define the forest root domain. You can choose an existing domain for the forest root or designate a new domain to serve as a forest root domain. Define your forest root domain with caution, because you cannot change it without renaming and reworking the entire Active Directory tree.

The third step in creating a domain plan is to define a domain hierarchy and name domains. To define the domain hierarchy, you must determine the number of domain trees; designate tree root domains for each tree; and arrange the remaining subdomains in a hierarchy under the root domains.

Finally, determine the placement of DNS servers. Additional zones must also be planned, the existing DNS services employed on DNS servers and the zone replication method to use must be determined. The end result of a domain plan is a domain hierarchy diagram including domain names and planned zones.

- To create an **OU plan** you must define an OU structure. The three reasons for defining an OU are: to delegate administration; to hide objects; and to administer Group Policy. The primary reason for defining an OU is to delegate administration. This is the assignment of IT management responsibility for a portion of the namespace.

After you've determined the OU structure, user accounts must be placed in the appropriate OUs. The end result of an OU plan is a diagram of OU structures for each domain and a list of users in each OU.

- The first step in creating a **site topology plan** is to define sites. The main concern of a site is to physically group computers to optimize network traffic. In Active Directory, site structure reflects the location of user communities. You must define a site for each LAN or set of LANs that are connected by a high-speed backbone; and/or each location that does not have direct connectivity to the rest of the network and is reachable only by using SMTP mail.

The second step in creating a site topology plan is to place domain controllers. The availability of Active Directory depends on the availability of domain controllers; a domain controller must always be available. For optimum network response time and application availability, you must place one domain controller in each site, and two domain controllers in each domain. You might need to place additional domain controllers in a site if there are a large number of users in a site and the link to the site is slow, and/or the link to a site is historically unreliable or only intermittently available.

The third step in creating a site topology plan is to define a replication strategy. An effective replication strategy ensures efficient replication and fault tolerance. In this step you configure site links. You also have the option to specify preferred bridgehead servers.

The final step in creating a site topology plan is to place global catalog servers and operations masters within a forest. The end result of a site topology plan is a site diagram that includes site links and a site link table that provides details about site link configurations, as well as locations of domain controllers and operations masters' roles.

1.7 Administering Active Directory Objects

1.7.1 Locating Active Directory Objects

You can use **FIND** in the **Active Directory Users and Computers** snap-in in the **Administrative Tools** folder to locate Active Directory objects. You can open **FIND** by doing the following:

- Click on the **START** button
- Open the **CONTROL PANNEL**
- Double-click on **ADMINISTRATIVE TOOLS**

- Open the **ACTIVE DIRECTORY USERS AND COMPUTERS** console
- Right-click a **domain or a container** in the console tree
- Then click **FIND**

The Find dialog box provides options that allow you to search the global catalog to locate Active Directory objects. Table 1.2 lists the options in the Find dialog box.

TABLE 1.2: *Find Dialog Box Options*

Option	Function
Find	Lists the object types for which you can search.
In	Lists the locations in which you can run the search.
Browse	Allows you to select the path of your search.
Advanced (tab)	Allows you to define the search criteria to locate the object that you need. The Advanced tab contains these additional options: <ul style="list-style-type: none"> • Field Lists the attributes for which you can search on the object type that you select. • Condition Lists the methods available to further define the search for an attribute. • Value Allows you to enter the value for the condition of the field or attribute that you are using to search the Directory. • Search Criteria Lists each search criteria that you have defined.
Find Now	Used to begin a search after you have defined the search criteria.
Stop	Used to stop a search.
Clear All	Used to clear the specified search criteria.
Results	Displays the results of your search once the search has been completed or stopped.

You can also use the **dsquery** command-line tool find computers, contacts, subnets, groups, OUs, sites, servers, and users in Active Directory according to criteria you specify.

- To find computers that have been inactive for the last four weeks, type: `dsquery computer -inactive 4`
- To find all users in an OU of a domain, type: `dsquery user OU=<OU_name>,DC=<domain_name>,DC=Com`
- To find all users with names starting with “Magd,” type: `dsquery user -name Magd*`

1.7.2 Using Saved Queries

Windows Server 2003 has a new saved queries feature that allows you to create, edit, save, organize, and e-mail saved queries. This allows you to access a specified set of directory objects in order to monitor or perform a specific task on them.

Saved queries are stored in the **Saved Queries** container in the **Active Directory Users And Computers** console. These queries are preserved within the **Active Directory Users And Computers** console file (*Dsa.msc*) and are restored every time the console is opened. Once you have successfully created a customized set of queries, you can copy the console file to other Windows Server 2003 domain controllers in the same domain. You can also easily export saved queries to an *.xml* file and import them into other **Active Directory Users And Computers** consoles located on Windows Server 2003 domain controllers in the same domain.

1.7.3 Moving Active Directory Objects

You can move Active Directory objects within a domain through the use of the **Active Directory Users and Computers** snap-in by pointing to the object, and selecting a target container for the **Move** operation. Moving objects between domains is a more complicated. The process of moving Active Directory objects between domains that belong to different forests is migrating objects.

In Windows Server 2003, Active Directory supports a number of tools that can be used for the purposes of object migration. These tools include: the **MoveTree** command-line utility; the **ClonePrincipal**; and the **Active Directory Migration Tool (ADMT)**. All of the utilities are included in the */Support/Tools* folder on the Windows Server 2003 Installation CD, except the ADMT, which is available in the */i386/ADMT* folder. All three tools add the original objects' SIDs to the **sidHistory** attribute of target objects if the domains are in the Windows 2000 native domains functional level.

1.7.3.1 The MoveTree Utility

You can use the **MoveTree** command-line utility (*MoveTree.exe*) to move the user, group, and OU objects within an Active Directory-based forest. The **MoveTree** command-line utility allows administrators to reconstruct Active Directory-based domains which belong to the same forest. This tool can move both single Active Directory objects, such as user accounts; empty domain local and global groups; universal groups; and entire containers, such as OUs, from one domain to another and are removed from their original location. In such an **intra-forest migration**, the user accounts retain their passwords after being moved, while membership to Universal groups is preserved. The **MoveTree** command-line utility cannot be used to move computer accounts, system objects, or domain controllers. Microsoft, however, recommends that you use the ADMT instead of the **MoveTree** command-line utility, except for moving contracts which cannot be handled by the ADMT.

1.7.3.2 The ClonePrincipal

The **ClonePrincipal** is a set of scripts that allows administrators to perform inter-forest migration, such as when incrementally migrating accounts from an existing Windows NT 4.0 domain to an Active Directory domain. The **ClonePrincipal** can also be used to reorganize Active Directory forests. Microsoft, however, recommends that you use the ADMT instead of the **ClonePrincipal**.

The **ClonePrincipal** can be used to duplicate user accounts; and security group accounts, which include local groups, global groups, domain local groups and universal groups. However, the **ClonePrincipal** cannot be used to duplicate computer accounts; inter-domain trusts; and accounts with well-known SIDs since these accounts have identical SIDs in every domain. Accounts with well-known SIDs are: Account Operators; Administrators; Backup Operators; Guests; Power Users; Print Operators; Replicator; Server Operators; and Users.

1.7.3.3 The Active Directory Migration Tool

The **ADMT** is a Microsoft Management Console snap-in that should be installed in the target domain only by running the *Admigration.msi* file in the */i386/ADMT* folder on the Windows Server 2003 Installation CD. It can be used to perform the same functions as the **MoveTree** utility and the **ClonePrincipal** through the help of wizards. It can be used to migrate user accounts, groups, and computer accounts:

- From Windows NT 4.0 domains to an Active Directory domain environment;
- Between Active Directory domains in different forests; and
- Between Active Directory domains in the same forest.

When you perform inter-forest migrations, you must run ADMT on a domain controller that belongs to the target domain. When you perform intra-forest migrations, you must run ADMT on the RID Master in the target domain.

The ADMT also supports a log file for each operation. These files are located in the *Logs* folder that resides in the ADMT installation folder and can be used to analyze failed migration operations.

1.7.4 Controlling Access to Active Directory Objects

Windows Server 2003 uses an **object-based security** model, that is similar to the one used to implement NTFS security, to implement access control to all Active Directory objects. Each Active Directory object has a security descriptor that defines the permissions to the object and the type of access that is allowed. Windows Server 2003 uses these security descriptors to control access to the Active Directory objects. An administrator or the object owner must assign permissions to the object before users can gain access to the object. Windows Server 2003 stores a list of these assigned user access permissions for every Active Directory object in the **access control list (ACL)**. This allows you to assign permissions or administrative privileges to a specific user or group for an OU, a hierarchy of OUs, or a single object, without assigning administrative permissions for controlling other Active Directory objects.

In addition, you can allow or deny permissions to Active Directory objects. The **Deny** permission takes precedence over any permission that you otherwise allow for user accounts and groups. You can also set standard permissions and special permissions on objects. Standard permissions are the most frequently assigned permissions and are composed of special permissions. Special permissions provide you with a finer degree of control for assigning access to objects. Table 1.3 lists standard object permissions that are available for most objects and the type of access that each standard permission allows.

TABLE 1.3: *Standard Active Directory Object Permissions*

Object Permission	Description
Read	Allows the user to view objects and object attributes, the object owner, and Active Directory permissions.
Write	Allows the user to change object attributes.
Create All Child Objects	Allows the user to add any type of child object to an OU.
Delete All Child Objects	Allows the user to remove any type of object from an OU.

Full Control

Allows the user to change permissions and take ownership and to perform all the tasks that are allowed by the above standard permissions.

You can use the **Active Directory Users and Computers** console to set standard permissions for objects and attributes of objects and you can use the **Security** tab of the **Properties** dialog box for the object to assign permissions. In addition, you can either allow permission inheritance to have permissions to propagate from a parent object to child objects or you can prevent permissions inheritance.

1.7.5 Delegating Administrative Control

Active Directory allows you to assign permissions and grant user rights in specific ways. You can assign permissions and grant user rights so as to delegate administrative privileges for certain objects to appropriate individuals in an organization. You can delegate:

- Permissions for specific organizational units to different administrators.
- The permissions to modify specific attributes of an object in a single organizational unit.
- The permissions to perform particular tasks in all organizational units of a domain.

1.7.6 Publishing Resources

Publishing resources is the process of **creating objects** in Active Directory that either directly contain the information that you want to make available, or provide a reference to that information. This will make it easier for users to locate network resources. Resources should be published in Active Directory when the information contained in them is useful to a user or when it must be highly accessible. However, you do not need to publish resources, such as user accounts, that already exist in Active Directory. Though, you must publish resources that do not exist in Active Directory such as printers on a pre-Windows 2000 computer, and shared folders.

Note: You should only publish information that is relatively static and does not change frequently in Active Directory. This will prevent excessive **replication traffic** across a network.

The object that is published in the directory is completely **separate** from the shared resource that it represents. The published object contains a reference to the location of the shared resource. When a user accesses the published object, Windows Server 2003 redirects the user to the shared resource. Therefore, by publishing resources in Active Directory you can allow users to locate resources even if the physical location of the resources changes. Furthermore, because a shared resource and the published object that refers to the shared resource are two different objects, each of these objects has its own **discretionary access control list (DACL)**, which is used to control access to that shared resource. A user requires Read permission on the DACL of a published object to view the published object in the results list when searching for a published resource but may not be able to access the shared resource, depending on the DACL on the shared resource.

1.7.6.1 Setting Up and Managing Published Printers

All printers shared on Windows 2000 or Windows Server 2003–based print servers that are members of either a domain or a domain controller are automatically published in Active Directory. However, you must publish printers that run on pre-Windows 2000 computers by using Active Directory Users and Computers. When you publish a printer, it is the print queue is published, and the object in Active Directory is called a **printQueue**. You only need to manage printers if you change the default behaviour of the printer.

Note: When you publish a printer, the printer object is placed in the print server's computer object in Active Directory. You can view printer objects in Active Directory. To view printer objects, you enable the option in Active Directory Users and Computers to view objects as containers.

By default any printer shared on a Windows 2000 and Windows Server 2003 print server that has an account in an Active Directory domain is published in Active Directory. When a print server is removed from the network, its published printers are automatically removed from Active Directory. When you configure or modify a printer's properties, Windows Server 2003 automatically updates the appropriate published printer object's attributes in Active Directory.

Note: To prevent users from viewing or using a particular printer, you must prevent the automatic publishing of printers in Active Directory. You can control the automatic publishing of a printer by using the List in the directory check box on the printer's Sharing tab. The List in the Directory check box is selected by default; therefore, the printers that are added by using the Add Printer Wizard are automatically published. You can use Group Policy to control the default behavior of published printers. You configure the **Automatically publish new printers in Active Directory** Group Policy setting in Computer Configuration\Administrative Templates\Printers in Group Policy to disable or enable automatic publishing of printers.

Managing printers includes tasks such as moving printers, connecting to printers on the network, and modifying properties of the print queue objects. After you publish printers in Active Directory, user and organization printing needs may change. This change may require you to configure printer settings so that your printing resources better fit these needs.

To **organize published printers**, you can move related published printers that are installed on multiple computers into a single organizational unit. By moving printers into a single organizational unit, you can perform administrative functions on all of the printers in the organizational unit. To move printers in a domain:

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTRATIVE TOOLS**
- Click on **ACTIVE DIRECTORY USERS AND COMPUTERS**
- Right-click the published printers you want to move
- Click **MOVE**
- In the **Move** dialog box that appears, expand the domain tree

- Click the organizational unit to which you want to move the selected printers
- Click **OK**

To use a print device the operating system on each computer that must connect to the print server requires a different version of the printer driver that is written for that operating system. Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP Professional and Windows Server 2003 client computers will automatically download the appropriate **printer driver** if a copy of the driver on the print server. To install a driver for a different operating system:

- Click on the **START** button
- Point to **SETTINGS**
- Click on **PRINTER**
- In the Printers folder that appears, right-click the printer that the clients will use
- Click **PROPERTIES**
- Click the **SHARING** tab
- Click the **ADDITIONAL DRIVERS** button
- Select the appropriate check boxes in the **ENVIRONMENT** column

For clients running Windows 3.11 non-Microsoft operating systems, such as **Macintosh** or **UNIX**, you must manually install a printer driver on the client computers. You must also install a print service on the print server for these clients.

1.7.6.2 Setting Up and Managing Published Shared Folders

You can publish any shared folder that can be accessed by using a **UNC name**, in Active Directory. A computer running Windows 2000 or Windows Server 2003 can use Active Directory to locate and connect to the shared folder. You can also define keywords and a description for the shared folders in Active Directory and you can move shared folders to related organizational units. You publish shared folders by using Active Directory Users and Computers but you must first share the folder, and then publish the shared folder in Active Directory. To publish a shared folder:

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTRATIVE TOOLS**
- Click on **ACTIVE DIRECTORY USERS AND COMPUTERS**
- Right-click the **ORGANIZATIONAL UNIT** where you want to publish the shared folder
- Point to **NEW**
- Click **SHARED FOLDER**
- In the **SHARED FOLDER NAME** box, type the name of the folder
- In the **UNC PATH** box, type the UNC path of the shared folder that you want to publish in Active Directory

Note: The UNC path is the complete Windows Server 2003 name of a network resource that conforms to the `\\servername\sharename` syntax.

After you publish a shared folder, you can add a description, which can provide more information about the shared folder, and keywords, which are a list of words that you can define for the shared folder object, to make it easier for users to locate the folder. To add a description and keywords to the shared folder objects:

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTRATIVE TOOLS**
- Click on **ACTIVE DIRECTORY USERS AND COMPUTERS**
- Right-click the **SHARED FOLDER**
- Click on **PROPERTIES**
- In the **DESCRIPTION** box, type the description for the shared folder
- Click **KEYWORDS**
- In the **KEYWORDS** box, type keywords that facilitates searching for this folder
- Click **ADD**
- Click **CLOSE**

Once a shared folder has been published, you can move the published folder to another container or organizational unit by moving the shared folder object, which contains information or references the shared folder, in Active Directory. The physical location of the shared folder does not change.

1.7.7 Auditing Access to Active Directory Objects

The procedure of enabling auditing consists of two steps: enabling the appropriate auditing policy and specify events to audit. Auditing access to Active Directory objects relates to operations performed on the domain controller. Therefore, the most appropriate place to enable audit is the **Default Domain Controllers Policy** or a GPO linked to the **Domain Controllers OU**.

1.7.7.1 Monitoring User Access to Shared Folders

Computer Management in Windows Server 2003 allows you to **monitor and administer shared resources** on local and remote computers. With Computer Management you can view information about shared resources, and perform administrative tasks, such as modifying permissions for a shared resource and determining the number of users who are currently gaining access to a shared resource. You would want to monitor access to:

- Check which users have access to which shared folders;
- Check which users are currently using a shared folder so that you can notify them before making the folder temporarily or permanently unavailable; and
- Check which shared folders are being used, how many users are using the folder and how often, so that you can plan for future system growth.

1.7.7.2 Monitoring User Sessions

You can monitor users who have a connection to open files on a server and the files to which they have a connection and use this information to determine which users you must contact when you must stop sharing a folder or shut down the server. You can also disconnect one or more users to free idle connections to the shared folder, prepare for a backup or restore operation, shut down a server, and change group membership and

permissions for the shared folder. After you disconnect a user, the user can immediately gain access to a shared folder unless you change the permissions or stop sharing the folder.

Note: Disconnecting users from open files can result in **data loss**. To prevent data loss you should **notify** users that are connected to shared folders or files that there will be a disruption to the computer or resource availability.

1.7.7.3 Sending Administrative Messages to Users

It is thus recommended that you send administrative messages to users when there will be a disruption to the availability of computers or resources to which they are a currently connected. You would send administrative messages to notify users when you intend to:

- Perform a backup or restore operation.
- Disconnect users from a resource.
- Upgrade software or hardware.
- Shut down the server.

You can use the **Shared Folders snap-in** to send administrative messages to users. By default, all currently connected computers appear in the list of recipients to which you can send a message. You can add other users or computers to this list even if they do not have a current connection to resources on the computer. To send administrative messages:

Note: Administrative messages will only be sent to computers running Windows NT, Windows 2000, Windows XP Professional and Windows Server 2003 if they are running the **Windows Messenger**. For Windows 95, Windows 98, and Windows ME, you must use *Winpopup.exe*.

When you combine NTFS permissions, the effective permission is a combination of all permissions, and when you combine shared folder permissions, the effective permission is a combination of all permissions. However, when you combine NTFS permissions with shared folder permissions, the effective permission is the most restrictive permissions of the effective permissions. Thus, if a user cannot gain the appropriate access to a resource, you must first determine the shared folder permissions that the user has. Then you must determine the NTFS permissions on the resource that the user is trying to access. Finally, you must determine which of these effective permissions are the most restrictive.