Introduction to Windows 2000 Directory Services Administration

CERTIFICATION OBJECTIVES

1.01 What Is Windows 2000 Directory Services Administration?

1.02 Overview of Exam 70-217

1.03 What We’ll Cover in This Book

1.04 What You Should Already Know

✓ Two-Minute Drill

Q&A Self Test
Welcome to Windows 2000 and one of Microsoft’s most important core topics for the Windows 2000 Microsoft Certified Systems Engineer (MCSE) certification track. The Active Directory is one of the most exciting new features in Windows 2000. This new and improved, sophisticated directory service provides administrators with a flexible, powerful tool that simplifies many day-to-day activities.

The Active Directory (AD) is the “heart” of the Windows 2000 Server domain controller and of Windows 2000 networking. Creating and implementing an Active Directory infrastructure present the systems administrator with both a challenge and an opportunity. Knowledge of NT networking provides a good foundation for learning many aspects of Windows 2000, but when it comes to directory services, Windows 2000 is a whole new world and presents an entirely new way of accomplishing administrative tasks, as well as the ability to accomplish many tasks that simply were not possible to accomplish in Windows NT—at least, not without third-party add-on software.

The Windows 2000 Active Directory can support a huge scope of features and capabilities in an enterprise environment. Microsoft designed Windows 2000 and Active Directory with the enterprise network in mind. The company’s goal in developing the new operating system and directory service was scalability that would extend to large and complex network configurations.

This book will help prepare you to not only pass Microsoft certification exam 70-217, Implementing and Administering a Windows 2000 Directory Services Infrastructure, but it will also prepare you for the exciting experience of applying your knowledge and skills to your real-world network.

CERTIFICATION OBJECTIVE 1.01

What Is Windows 2000 Directory Services Administration?

In order to answer that question, let’s break the exam topic down into its component parts. First, and most basic: what do we really mean by implementing and administering? The American Heritage Dictionary defines implementing as
“putting into practical effect, or carrying out,” and it defines administering as “having charge of” or simply “managing.” (These definitions should appeal to the “control freak” side of your nature—and anyone who wants to manage an entire enterprise network must have at least a mild dose of that in his or her personality.)

What exactly is it, then, that we are “carrying out” and then “managing”? A directory, in this context, is a database that contains information about objects and their attributes. Most of us are already familiar with the basic directory concept; consider a telephone directory. The “objects” a telephone directory contains are names, and the attributes of each object include the phone number and address associated with that name. Directories utilized by network operating systems can, of course, be much more complex. The directory service is the component that organizes the objects into a logical and accessible structure and provides for a means of searching and locating objects within the directory. The directory service includes the entire directory and the method of storing it on the network.

Finally, let’s look at the word infrastructure. Returning again to our trusty dictionary, we find that an infrastructure is defined as “an underlying base or foundation for an organization or system.”

Putting it all together, we can conclude that exam 70-217 covers how to put into practice a plan that will provide a foundation for the use of a networkwide database holding information about objects on the network (such as user and computer accounts, resources, and network services) and make that information quickly and easily available to authorized users, applications, and operating system services. Furthermore, it will test you on the skills required to maintain, optimize, troubleshoot, and oversee the use of that database throughout your enterprise network.

The Active Directory includes the following specific features:

- A data store (another term for the directory), which stores information about Active Directory objects. Active Directory objects include shared resources such as servers, files, printers, and user and computer accounts.
- A set of rules, called the schema, which defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects, and the format of their names.
- The global catalog (GC) that contains information about all the objects in the directory. The GC allows users and administrators to find directory information without having to know which server or domain actually contains the data.
Chapter 1: Introduction to Windows 2000 Directory Services Administration

- A means of querying and indexing this information, so that objects and their properties can be published and found by network users (or by applications that need to access them).
- A replication service, which distributes directory data across the enterprise network. All domain controllers in a domain participate in replication and contain a complete copy of all directory information for their domain. Changes to directory data are automatically replicated to all domain controllers in the domain.
- A security subsystem that provides for a secure logon process to the network as well as access control on both directory data queries and data modifications.
- The ability to join domains into a domain tree and join trees in a forest, creating a trust relationship that allows for easy access by all users in the multidomain network to all resources for which their accounts have the appropriate access permissions.
- The means to exert granular control over entire sites, domains, or organizational units (OUs) through the use of Group Policy, making management of an enterprise-level network easier for the administrator.

### SCENARIO & SOLUTION

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does the Active Directory namespace differ from the NT domain namespace?</td>
<td>The NT namespace is flat—that is, all domains are on an equal “level.” The Active Directory namespace is hierarchical; domains exist in a “tree” structure in which a root domain spawns “child” domains, which can in turn have children of their own. The name of the child includes the name of the parent; thus a domain named training.tacteam.net is the child of a parent domain named tacteam.net.</td>
</tr>
<tr>
<td>How do Active Directory trust relationships between domains differ from NT trusts?</td>
<td>Active Directory trusts use Kerberos authentication, an industry standard, to provide for explicit two-way transitive trust relationships between all domains in a tree or a forest of trees. NT trusts are one way, and each must be created explicitly.</td>
</tr>
<tr>
<td>How does Active Directory achieve compatibility with other directory services?</td>
<td>Active Directory is compatible with the LDAP standards, which makes it compatible with other LDAP directory services such as Novell’s directory services.</td>
</tr>
</tbody>
</table>
What Is Windows 2000 Directory Services Administration?

The Role of a Directory Service

Directory services are good—in fact, they are necessary components of any complex networking system. In an object-oriented operating system such as Windows, there must be some means of keeping track of all the system's objects (users, groups, computers, printers, folders, and files and other network resources) and an easy way to locate and access them when you need to use them.

Directory Services in Windows NT

One thing that we should clarify: The directory service itself is not a new thing in Windows 2000. NT uses directory services, too. In fact, NT uses a multiplicity of directory services: DNS, with its database of host names and IP addresses; WINS, with its own database of NetBIOS names and IP addresses; the browse service, to keep up with shared network resources; and the Security Accounts Manager (SAM)
database that handles information about security objects (users and groups) and permissions. NT uses NT Directory Services (NTDS) to manage users and groups. It is a flat database and is not extensible, but it does offer such features as single sign-on to access network resources across the enterprise.

The databases used by NT were not well integrated to work together, and locating particular objects could be difficult. For instance, if you needed to access a particular shared folder, you needed to know which server that folder resided on in order to access it. With the Active Directory, objects can be published and will appear in the directory; users can access a shared folder without ever knowing—or needing to know—on what computer’s hard disk the folder is physically located.

Long-time network administrators who have worked with Novell’s network operating systems will quickly see the parallel here: The difference between the NT Directory Services and Active Directory is like the difference between the NetWare 3x bindery, which was a flat database, and the NetWare 4x and 5x hierarchically structured NDS tree. Furthermore, just as Novell designated moving from NetWare 3x to version 4 as a “migration” as opposed to an “upgrade,” the switch from NT to Windows 2000 should be viewed in the same light.

Advantage of Active Directory

Unfortunately, NT’s ways of storing information had some serious limitations. For instance, the number of security objects that could be contained in the SAM database was restricted by the fact that the entire database had to fit into the domain controller’s RAM. This resulted in a Microsoft-recommended maximum of about 40,000 accounts in a domain. In contrast, one of the biggest advantages of Active Directory is its scalability; because security accounts information, along with information about many other types of objects, is stored in the Active Directory and stored on a partition on the domain controllers’ hard disks, there is no such limit on the number of accounts. One domain can contain literally millions of objects.
Interoperability of Directory Services
Along with the Active Directory, Microsoft introduced the Active Directory Services Interface (ADSI), a set of COM interfaces supplied as a Software Development Kit (SDK) that allows developers to enable their applications to use directory services. This structure gives users a single point of access to one or more directories, which can be based on LDAP, NDS, or NTDS.

Microsoft designed Active Directory to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies have and use in their networks. Toward that end, migration tools are provided to allow administrators to more easily migrate from other directory services, such as NTDS or NDS, to the Active Directory. Third-party programs are also available to assist in migration and/or allow for integration with multiple operating systems and services such as Banyan Vines and NDS.

Replication of Directory Information
The directory information is stored in a file named NTDS.DIT. This file must be located on an NTFS-formatted partition or volume on the Windows 2000 domain controller. The directory data can be divided into two categories: private and public. Public data is stored on a shared system volume. This volume is replicated to all domain controllers within the domain.

The data that is replicated includes domain data, configuration data, and schema data. Domain data is what we generally think of as directory information—that is, information about domain objects. Examples are user and computer account attributes, published shared folders, printers, and other resources. The configuration data is information about the directory structure, such as the names of domains and trees and where the domain controllers and global catalog servers are located in the domain. Schema data refers to the definitions of classes, object types, and attributes that you can store in the directory.
Chapter 1: Introduction to Windows 2000 Directory Services Administration

Windows 2000 provides for the means to modify or extend the schema, but it is not a task for the timid. Microsoft refers to schema modification as “an advanced and complex operation best handled programmatically.” In other words, the usual way for the schema to be modified is for developers to write applications that will modify it. Unfortunately, when an application changes the schema incorrectly, the administrator may have to perform schema modification as part of the troubleshooting process.

It is a good practice to disconnect the domain controller serving as the schema operations master from the network prior to making the changes; that way, you can test the change before the schema update is replicated to the other domain controllers. Remember, the schema master’s role is forestwide, so changes to the schema impact every domain in every tree in the forest. In fact, because a change to the schema constitutes such serious business, it is recommended that they always be tested in a lab environment first, so that any unexpected effects will be isolated from your production network.

Features of a Global Directory Service

What do we mean by a global directory service? Microsoft uses the term to refer to a directory service that is scalable to the enterprise level, compatible with Internet and industry standards, and integrated fully with the operating system. Some features of Active Directory that have been incorporated to ensure that it meets these criteria include:

- Support for major standards such as the Dynamic Domain Name System (DDNS), Dynamic Host Configuration Protocol (DHCP), LDAP, and Kerberos
- Open programming interfaces and protocols such as Active Directory Service Interfaces (ADSI) and the Security Support Provider Interface (SSPI)
- Centralized management using a consistent management interface
- Customization and control of the user desktop and environment
- Directory-enabled applications and easier application deployment and configuration
- Integration of security services, based on standardized authentication protocols

Let’s take a brief look at what each of these features means.
Support for Major Standards
Windows 2000 Server and the Active Directory support and work together with Internet and industry standards, including:

- Dynamic Domain Name System (DDNS)
- Dynamic Host Configuration Protocol (DHCP)
- Lightweight Directory Access Protocol (LDAP)
- Transmission Control Protocol/Internet Protocol (TCP/IP)

Dynamic Domain Name System  DDNS support and integration in the Active Directory allows for the creation of a global naming structure compatible with standard DNS conventions, while including the benefits of the “dynamic” aspect of this improved version of DNS. The DNS dynamic update protocol is a new specification to the DNS standard that permits hosts that store name information in DNS to dynamically register and update their records. This applies to DNS zones maintained by DNS servers that are able to accept and process dynamic update messages. Note that DDNS is supported only by Berkeley Internet Name Domain (BIND) versions 8.x and above. BIND is an implementation of DNS distributed with UNIX.

Dynamic Host Configuration Protocol  DHCP’s new integration with Active Directory provides a means of authorizing DHCP servers in the directory, so that “rogue” (unauthorized) DHCP servers can be detected and prevented from allocating IP addresses on the network.

Lightweight Directory Access Protocol  LDAP compatibility translates into better interoperability between applications and directory services. Microsoft provides LDAP support in client products such as Microsoft Outlook, NetMeeting, and Internet Explorer and in server products such as Site Server and Exchange Server.

LDAP will also be the method used by Microsoft Exchange Server for directory migration and synchronization with Windows 2000 Server. You can also use the Active Directory Connector to replicate directory objects between a Microsoft Exchange Server directory (version 5.5 or later) and the AD directory service.
Transmission Control Protocol/Internet Protocol  
TCP/IP is, of course, the standard set of protocols required for computers to communicate on the Internet. TCP/IP works on a huge diversity of operating systems and platforms and enables connectivity between dissimilar systems all over the world. The Windows 2000 implementation of TCP/IP has added several enhancements, such as support for large TCP receive windows and Selective Acknowledgements, both of which can improve the performance of this powerful, flexible, but relatively slow protocol stack.

Open Programming Interfaces and Protocols  
True global status and interoperability require open interfaces and protocols that enable third parties to more easily develop applications that work in the Active Directory environment. These include:

- The Active Directory Services Interface (ADSI)
- The Security Services Provider Interface (SSPI)

Active Directory Services Interface  
ADSI consists of a set of high-level, language-independent directory service programming interfaces, which support the ability to work with resources provided by Windows NT Server 4.0, Novell NetWare 3.x, and NetWare 4.x (including the Novell Directory Services). ADSI is the primary application programming interface (API) to be used for developing applications for the Windows 2000 Server Active Directory. ADSI’s purpose is to provide software developers with a standardized, easy-to-use, object-oriented way to write application programs using tools such as Java, C, C++, or Visual Basic that can access information from multiple directories and synchronize data between directories.

Security Services Provider Interface  
SSPI allows developers to utilize the integrated security benefits of Windows 2000, such as single sign-on and authentication. SSPI is used to access the security features of the Active Directory.

SSPI is the component of the security subsystem that reduces the amount of code needed at the application level to support multiple security protocols by providing a generic interface for the authentication mechanisms that are based on shared-secret or public key protocols.
Centralized Management and a Consistent Management Interface

The Active Directory serves as a central repository for all information about system configuration, user profiles, and applications. This repository allows administrators to manage distributed desktops, network services, and directory-enabled applications from one central location, using a consistent management interface: the Microsoft Management Console (MMC). It also provides network administrators with a consistent way to monitor and manage network devices, such as routers, through system profiles provided by the Active Directory.

The MMC is a tool that is used to create, save, and open collections of administrative tools, called consoles. Consoles contain snap-ins, wizards, and documentation that are used for managing hardware, software, and networking components in Windows 2000. See Figure 1-1 for an example of an MMC—in this case, the AD Sites and Services console.

All MMC snap-ins present this same common interface, with the console tree shown on the left and the details pane on the right. This Windows Explorer-like
interface makes it easier for administrators to perform management tasks, without being required to learn to navigate a different interface for each administrative tool.

**Customization and Control of the User Environment**

The Windows 2000 Active Directory supports customization and personalization of the user desktop and environment. Features in Windows 2000 Server and Windows 2000 Professional use information stored in Active Directory to determine where users store their documents, where their personal settings are saved, and the general configuration of their environments.

Through application of Group Policies, administrators can control the environments of users to whatever extent is desired, all the way to “locking down” the desktop. Group Policy for a site, domain, or organizational unit is implemented through the Active Directory, and the Group Policy settings define the components of the user’s desktop environment that a systems administrator needs to manage.

**Directory-Enabled Applications and Easier Deployment and Configuration**

Applications can be written to use the Active Directory to locate services that are published to the directory and to centrally store application configuration and installation information.

**Integration of Security Services**

In Windows 2000, strong security features, such as Kerberos authentication and public key certificates, are directly integrated with the directory services. Let’s briefly examine how this differs from the NT model.

In NT 4.0, the SAM database and the characteristics of the NTLM trust relationship combined to limit security to three levels within the domain: global groups, local groups, and individual users. With Active Directory, the database is distributed throughout the enterprise. This means security can be administered with much more granularity and flexibility. One example is the ability to delegate administrative authority at the OU level.

The Windows 2000 Distributed Security Services use the Active Directory as the central repository for account information and domain security policy. This is a big improvement over registry-based implementation in terms of both performance
and scalability. It is also easier to manage because the Active Directory provides replication and availability of account information to multiple domain controllers and can be administered remotely.

**Active Directory Structure**

The Active Directory has both a *physical structure*, defined by sites for purposes of optimizing replication and logon authentication traffic, and a *logical structure*, defined by domains, which can be joined into trees, and trees combined to create forests. If you are not familiar with these terms, see the section on directory services terminology later in this chapter.

**Active Directory Physical Structure**

The physical structure of the Active Directory is based on Active Directory sites. A *site* is a group of computers in an IP subnet or group of subnets that have a high-performance connection. Sites are completely independent of domains; that is, a site can span more than one domain, and a domain can span multiple sites.

**Using Sites to Optimize Logon Authentication Traffic**

The Active Directory uses sites to optimize the flow of network traffic across slow wide area network (WAN) links. In other words, if you have two sites, connected by a 56Kbps link, it is more efficient for a user logon to be authenticated by a domain controller at the same site as the computer from which the user is logging on, because the traffic will not have to travel over the slow link.

**Using Sites to Optimize Directory Replication Traffic**

Sites are also used in optimizing directory replication. The traffic generated by the replication of directory information from one domain controller to another can have a major impact on network bandwidth if those domain controllers are separated by a slow link. Thus replication between separate sites (*intersite replication*) is handled differently from replication traffic within the same site (*intrasite replication*). For instance, you can schedule intersite replication to take place after business hours or increase the interval between instances of replication to reduce the load on the network at peak usage times.
Active Directory Logical Structure

The logical structure of the Active Directory is based on domains. NT administrators are already familiar with the term, but Windows 2000 Active Directory domains differ in many ways from NT domains. NT domains are all “peers” on the network, and they operate independently. Users who belong to one NT domain cannot access the resources of a different domain unless the administrator explicitly creates a trust relationship between the two domains. Even then, the trust is not two way; the trusting domain’s resources are available to users in the trusted domain, but the opposite is not true. Another separate trust must be established for that to happen.

Trees and Forests  An important feature of the Windows 2000 domain structure is the ability to join domains in trees. A tree is a group of domains that share a contiguous namespace and all of which have a two-way transitive trust with one another.

Multiple trees can be joined into a forest. The root domains of each tree also share two-way transitive trusts with those of every other trust in the forest. All domains in a forest share a common schema, configuration, and global catalog.

The Nature of Trusts  A transitive trust is one in which the trust relationship is transferred through intermediary domains. In other words, if Domain A trusts Domain B, and Domain B trusts Domain C, then Domain also trusts Domain C in a transitive relationship. Kerberos trusts, used by Active Directory, are transitive, while NTLM trusts, used in NT-based networks, are nontransitive.

The Hierarchy of Domains  The way in which domains are arranged within a tree is hierarchical. A hierarchy is a way of organizing objects in such a way that there is a single “root” object from which others branch off and in which each object “belongs to” the object above it. The object to which it belongs is called its parent object, and each object directly beneath another in the hierarchy is called a child object. See Figure 1-2 for an illustration of a domain hierarchy.

Note that the name of each child domain also includes the full name of its parent. This is what is meant by a contiguous namespace.
CERTIFICATION OBJECTIVE 1.02

Overview of Exam 70-217

The Windows 2000 certification exams can be divided into two groups: the core implementing and administering exams and the design electives. Each category has a different focus; the design exams are concerned with planning issues, whereas the cores deal with the “nitty gritty” of everyday work with the network and the operating system.
and its components. It might seem logical (or chronological) to learn design first, since after all a directory services infrastructure (or other network infrastructure) must be designed before it can be implemented and administered. However, you will almost certainly find it easier to study and test on the core topics first. The design exam questions are more complex, requiring a higher level of cognition and the ability to dissect, analyze, evaluate, and then devise a plan based on multiple sources of information. You will find that studying for this exam, Implementing and Administering a Directory Services Infrastructure, will lay the foundation needed to prepare for 70-221, the directory services infrastructure design exam.

This exam, 70-217, covers an amazing number of complex topics. Not only must you be able to demonstrate your ability to install, configure, and troubleshoot the Windows 2000 Active Directory components as well as DNS for Active Directory; you must also be able to implement Active Directory security solutions and deploy Windows 2000 via the Remote Installation Service (RIS). Finally, you should be able to manage, monitor, and optimize the desktop environment by using Group Policy, and you must be able to use Group Policy to deploy application software.

Exam Objectives

The objectives stated by Microsoft for this exam involve many skills, most of which will be new to experienced NT administrators (although the concepts won’t necessarily be). In this section we break the objectives down into broad categories and discuss a little about each.

Installing, Configuring, and Troubleshooting the Active Directory

It is recommended that you practice installing the Active Directory in various situations (for example, on a domain controller for a new domain, on a new domain controller for an existing domain, on a new domain controller that is to become the root of a new tree in an existing forest).

In order to meet this objective, you must know much more than simply how to run the Active Directory Installation Wizard (see Figure 1-3).
To start the Active Directory installation process, type **DCPROMO** at the command line. Remember that installing Active Directory on a server makes that server a Windows 2000 domain controller. The DCPROMO command is also used when you want to demote a domain controller to a member or standalone server and remove Active Directory from its hard disk. Expect questions on installation issues on the exam, and be sure you also understand how to verify the installation of Active Directory once it's done.

**Sites and Subnets** In addition to demonstrating your ability to install the Active Directory, the first objective requires that you be able to create active sites and subnets and then make site links, site link bridges, and connection objects to establish a replication topology between those sites. You must also know how to move server objects from one site to another.
Special Domain Controller Roles  

Domain controllers can take on several different, special roles in a Windows 2000 forest or domain. You must understand these specialized roles and their impact on the network. Particularly, you should know how to create and use global catalog servers and operations masters and how to transfer operations master roles from one DC to another.

Global Catalog Servers  

The *global catalog server* is a domain controller that contains a partial replica of every domain in Active Directory. The global catalog holds a replica of every object in Active Directory, but it includes only some of the objects’ attributes—those most often used in search operations.

A domain controller can be enabled or disabled as a global catalog server via the Active Directory Sites and Services MMC, by double-clicking the server name, right-clicking NTDS Settings | Properties, and checking the Global Catalog checkbox, as shown in Figure 1-4. (Later in the book, you will go...
through all the steps involved in making a domain controller a global catalog server.

A user must generally have access to a global catalog server to successfully log onto the network, because the global catalog is needed to determine to what groups the user belongs.

*Network performance is increased if the domain controller at a site is also a global catalog server, so it can fulfill queries about all the objects in the entire forest. The down side is that if you make too many domain controllers global catalog servers, the replication traffic on your network could be increased.*

**Operations Masters**  
Active Directory “levels the playing field” by making domain controllers more equal—doing away with the roles of Primary Domain Controller (PDC) and Backup Domain Controller (BDC). Windows 2000 introduces *multimaster replication*, wherein a read/write copy of the directory is kept on all DCs. Nonetheless, there are still some tasks that must be performed in a *single-master* fashion. This means one domain controller must be designated as the one “in charge” of that particular operation (at least, for a period of time). These tasks are referred to as *single-master operations* and the domain controllers that take on the role of handling them are called *operations masters*.

---

**Flexible Single-Master Operations**

You may hear the term *flexible single-master operations* or simply *FSMO* (pronounced *fiz-mo*). This was the term used to describe the operations masters in the beta versions of Windows 2000. The roles were described as “flexible” because they could be transferred from one domain controller to another within the domain or forest. (Some operations master roles are domainwide and others are forestwide.)

—*Debra Littlejohn Shinder, MCSE, MCP+I, MCT*
The operations master roles are as follows:

- Schema master
- Domain-naming master
- Infrastructure master
- Relative ID (RID) master
- PDC emulator

### SCENARIO & SOLUTION

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What does the schema master do?</td>
<td>The DC designated as schema master controls updates and modifications to the schema. This role is forestwide because a common schema is shared by all domains in a forest. There can be only one schema master in the forest, and changes to the schema can be made only through that machine.</td>
</tr>
<tr>
<td>What does the domain-naming master do?</td>
<td>The domain-naming master is the domain controller that oversees the addition or removal of domains within the forest. Like the schema master, this is a forestwide role.</td>
</tr>
<tr>
<td>What does the infrastructure master do?</td>
<td>There is an infrastructure master for each domain, and it updates the group-to-user references when group members are changed.</td>
</tr>
<tr>
<td>What does the RID master do?</td>
<td>The RID master, a domainwide role, is a DC that allocates relative ID sequences to the DCs in its domain. A RID is a unique security identifier assigned each time a user, group, or computer object is created.</td>
</tr>
<tr>
<td>What does the PDC emulator do?</td>
<td>This domain controller emulates a Windows NT PDC if there are Windows NT BDCs in the domain, processing password changes and replicating the information to the BDCs. If the domain operates in native mode, with only Windows 2000 DCs, the PDC emulator receives preferential replication of password changes performed by other DCs, serving as a sort of clearinghouse for password authentication.</td>
</tr>
<tr>
<td>Can one domain controller serve more than one operations master role at a time?</td>
<td>Yes. One domain controller can perform two or more operations master roles simultaneously. This would obviously be necessary in a small network that had fewer than five domain controllers.</td>
</tr>
</tbody>
</table>
The Organizational Unit Structure  The next part of this first objective specifies that you be able to implement an OU structure. Organizational units are container objects in the Active Directory that can be created within a domain for purposes of administrative boundaries. OUs can contain users, groups, computers, printers, and even other OUs.

In Windows NT, the smallest administrative boundary was the domain. This meant that if you gave a user administrative authority, he or she had administrative privileges for the entire domain. It was difficult to delegate authority this way, and this difficulty resulted in the creation of multiple domains on a network that otherwise would have needed only one or two. Having all these separate domains was made an even greater headache because of the nature of trust relationships in NT.

Windows 2000 OUs solve this problem. Now it is simple to create an OU, place in it those resources over which you want an individual to have authority, and assign the user administrative privileges for that OU only. Organizational units function as both administrative and security boundaries because Group Policy can be applied to an OU as well.

Creating an effective OU structure requires that you analyze carefully the administrative functions in your organization’s network and use the ability to nest OUs (place one inside another) to accomplish your purpose(s).

Organizational units are created and managed via the Active Directory Users and Computers management console (see Figure 1-5).

Back Up and Restore Active Directory  The last part of this exam objective deals with backing up the Active Directory information and restoring the Active Directory from backup.

- **Authoritative Restore**  You should know how to perform an authoritative restore. This is a type of restoration operation performed on a Windows 2000 domain controller in which the objects that are in the restored directory replace all existing copies of those objects via replication. Only replicated *system state data*—that is, Active Directory data and File Replication Service data—is authoritatively restored. The NTDSUTIL.EXE tool is used to perform an authoritative restore, which can be done only by an administrator.

- **System Failure Recovery**  You should also know how to recover from a system failure. This means being able to demonstrate your ability to back up
the Windows 2000 Registry and restore it to recover from a system failure. The Registry can be backed up using the Windows 2000 Backup utility to back up the system state data.

**You should know how to create and use an Emergency Repair Disk (ERD) to recover from a failure when you are unable to open the Backup utility to restore the Registry. The ERD is created using the Backup utility and contains information about your current system configuration that is used to repair the system when the computer will not start and/or when system files are damaged.**

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

The next objectives deal with DNS and how to integrate Active Directory DNS zones with non-AD zones. The DNS Server service is designed to interoperate with the Active Directory in Windows 2000; by integrating DNS zones with the Active Directory, you can benefit from new features in Windows 2000 DNS—in particular, dynamic updates and record aging and scavenging features. DNS updates can be conducted via multimaster replication in the same way other directory information is replicated between domain controllers.
Directory-integrated DNS zones are stored in the Active Directory tree under the domain object container, and each zone is located in a DNS zone container labeled with the name of the zone. Integration optimizes replication planning for the network and provides for secure updates of DNS zone files.

**Zone Configuration**  The exam objectives require that you be familiar with the process of configuring DNS zones, using both standard zone storage (which relies on a text-based file with the .DNS extension located in the `<systemroot>\System32\Dns` folder on each DNS server) and directory-integrated zone storage using the Active Directory database.

**Managing, Monitoring, and Troubleshooting DNS**  Furthermore, you should be able to manage, monitor, and troubleshoot Windows 2000 DNS. You should know that DNS is configured through the Computer Management console, accessible as a node in the Services and Applications section of the console tree (see Figure 1-6) or through the DNS administrative tool, which will bring up only the DNS console.
Be sure you understand the basics of Windows 2000 DNS, such as:

- How to install and configure a Windows 2000 DNS server
- How the DNS query process works when a client wants to resolve a fully qualified domain name (FQDN)
- How reverse lookups work and how to add a reverse-lookup zone
- How to use the DNS server log, viewed via Event Viewer, to monitor DNS events
- How to trace logging to a text-based file of DNS server activity
- How to use DNS counters in the System Monitor (accessed via Performance in the Administrative Tools menu)
- How to use DNS Notify for notifying a select set of secondary servers for a zone when it is updated

You should know the purpose of the various DNS resource records, including:

- **Host (A)** For mapping a DNS domain name to an IP address used by a computer.
- **Alias (CNAME)** For mapping an alias DNS domain name to another primary or canonical name.
- **Mail Exchanger (MX)** For mapping a DNS domain name to the name of a computer that exchanges or forwards mail.
- **Pointer (PTR)** For mapping a reverse DNS domain name based on the IP address of a computer that points to the forward DNS domain name of that computer.
- **Service location (SRV)** For mapping a DNS domain name to a specified list of DNS host computers that offer a specific type of service, such as Active Directory domain controllers.

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

This next series of exam objectives revolves around Windows 2000 Group Policy, an integral feature of Active Directory. *Group Policy* serves some of the same functions
as Windows NT’s system policies, but it does much more. You can think of Group Policy as “System Policy on steroids.”

For exam 70-217, it is vitally important that you know all aspects of installing, configuring, managing, optimizing, monitoring, and troubleshooting Group Policy; you should expect several questions on the exam that come from this broad objective.

Group Policy is a complex topic; entire books could be written about it (and no doubt will be). You will benefit greatly from actually working with this feature until you become comfortable with its many exciting features.

**Group Policy Objects**  
A group policy object (GPO) is a collection of policy settings. Local GPOs are stored on all Windows 2000 computers; nonlocal GPOs are stored on domain controllers and managed via the Group Policy MMC that you create for each GPO (see Figure 1-7).

As shown in Figure 1-7, user rights, audit policies, and security policies are just a few of the many policies implemented via the Group Policy management console.

![Group Policy Objects](image-url)
Group Policy can be applied to sites, domains, or OUs, and you can filter the policy application by associating security groups with GPOs.

For this exam, you should know how to create a new GPO and how to link an existing GPO as well as how to modify Group Policy. Acquaint yourself with the default GPOs and their components, and practice working with Group Policy, both local and otherwise.

Delegation of Control Another important area in which to practice is delegation of administrative authority, which can be done easily using the Delegation of Control wizard. There are basically three ways to define the delegation of administration responsibilities:

- You can delegate permissions to change properties on a particular container.
- You can delegate permissions to create and delete objects of a specific type under an organizational unit, such as users, groups, or printers.
- You can delegate permissions to update specific properties on objects of a specific type under an organizational unit.

You can delegate administration of particular resources to a specific individual or group. This technique does away with the need for multiple administrators to have authority over an entire domain or site. The user or group who has been granted the appropriate permissions can even turn around and delegate administration of a subset of his, her, or their accounts and resources to someone else. This makes for a flexible and granular means of assigning administrative responsibilities—particularly useful in large, enterprise-level organizations.

Group Policy Inheritance Group Policy is generally inherited by child containers from their parent containers. This means that if you have assigned a specific Group Policy to a high-level parent container, that Group Policy applies to all containers beneath the parent container, including the user and computer objects in each container. On the other hand, if you explicitly specify a Group Policy setting for a child container, the child container’s Group Policy setting overrides the parent container’s setting.
Blocking Inheritance  You can modify the behavior of Group Policy inheritance. For example, inheritance can be blocked at the site, domain, or OU level.

Enforcing Inheritance  Another way in which you can modify default Group Policy behavior is to enforce inheritance using the No Override option. This option forces all child containers to inherit the policies of the parent container, even if Block Inheritance is in effect.

Implementing and Troubleshooting Group Policy
This objective requires that you understand the basics of using Group Policy to control various aspects of the user environment, including software deployment and management.

Using Group Policy to Manage the User Environment  For the exam, you must be able to use Group Policy to control and manage users' environments and troubleshoot problems that may arise as a result of Group Policy conflicts or misapplication.

You should be familiar with using administrative templates, which are ASCII files that provide a source for Group Policy to generate user interface settings. You should also be able to assign script policies to users and computers. Group Policy can be used to specify four types of scripts: logon, logoff, startup, and shutdown. Group Policy includes extensions for deployment of these script types.

Windows 2000 also includes the Windows Scripting Host (WSH), used to run Visual Basic Script and JavaScript without the need to embed the scripts in a HyperText Markup Language (HTML) document.

Managing Software via Group Policy  The Software Installation component of Group Policy is used to deploy and manage application software throughout the organization. Applications that include Windows Installer files can be assigned to a user or computer or published (made available for installation) to users.

Exam 70-217 requires that you be familiar with deploying application software in each of these three ways and that you understand how to maintain and deploy software upgrades and configure your deployment options. You should also be able to demonstrate your ability to troubleshoot common problems that can occur during software deployment.
Chapter 1: Introduction to Windows 2000 Directory Services Administration

Using Remote Installation Services
The Windows 2000 Remote Installation Services (RIS) are designed to allow administrators to set up unattended installations on multiple client machines. These services are part of the IntelliMirror Technology.

Windows 2000 provides the Remote Installation Preparation (RIPrep) wizard to prepare an existing installation of Windows 2000 Professional and then replicate the image to a designated remote installation server.

Installing and Configuring Remote Installation Services
For this exam, you should be familiar with RIS installation and configuration issues and know how to install the RIS, including the prerequisites for installation, such as:

- Hardware requirements for both server and client
- A DNS server on the network
- An authorized DHCP server on the network
- Active Directory installed on the network

Troubleshooting Remote Installation Services
Be familiar with common RIS-related problems and know how to use the RIS troubleshooter included in the Windows 2000 Server Help component.

RIS Security Issues
Be sure you understand the security features incorporated into RIS, including authorization of RIS servers. When a remote installation server attempts to start on the network, Active Directory is queried, and the server computer’s name or IP address is compared with the list of authorized remote installation servers. If a match is found, the remote installation server is authorized and can start on the network. If a match is not found, the server is not authorized and the services will not work.

Also be aware of the required permissions for creating new computer accounts on the network and know how to set permissions for prestaged computer accounts using the Active Directory Users and Computers console.
Managing, Monitoring, and Optimizing the Components of Active Directory

At the heart of Active Directory administration are the daily tasks of managing, monitoring, and optimizing the objects and performance of the directory.

Active Directory Objects  You should be very familiar with how to create objects, such as user and computer accounts, in the directory—both manually and with scripts. You need to practice moving these objects from one container to another in the directory and understand the effects of such moves. Be able to publish resources such as shared folders and printers in the directory and how to locate those resources for access.
Chapter 1: Introduction to Windows 2000 Directory Services Administration

As an administrator, you must also be well versed in controlling access to directory objects using Active Directory object permissions and know how to use the Delegation of Control wizard to delegate administrative authority over directory objects to a user or group.

**Active Directory Performance**  Exam 70-217 will ask you about the basics of monitoring, maintaining, and troubleshooting domain controllers. You should understand how to use the Performance counters in System Monitor to establish a baseline and measure the performance of the DCs and the Active Directory components.

**Active Directory Replication**  Optimizing Active Directory replication, especially in a multisite network, is an important topic on the exam. To meet exam objectives, you must know the difference between *intersite* and *intrasite* replication and the configuration options available to you for each:

- **Intersite replication**  You must know how to manage replication of directory information between sites, especially how to optimize network bandwidth by modifying the interval and/or scheduling of replication events.
- **Intrasite replication**  This refers to replication between domain controllers that are located within the same site.

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

Security features are tightly integrated into Active Directory. It is important that you be aware of how the new Windows 2000 security components work, how they can be configured, and how to deploy them in a way that will provide a controlled yet accessible environment for your network users. You should also know how to troubleshoot security issues, which are a common source of access problems.

Be particularly aware of the following aspects of Active Directory security:

- Creating, deploying, and modifying Group Policy security policies
- Using the Security Configuration and Analysis feature and security templates
- Establishing audit policies
- Monitoring, analyzing the impact of, and responding to security-related events
CERTIFICATION OBJECTIVE 1.03

What We’ll Cover in This Book

This book covers the topics of each exam objective, along with information on additional resources, tips on common points of confusion, and details often overlooked in the directory services planning/design process and in preparing for the design exam.

Knowledge

In the beginning of each chapter, we provide you with a foundation of knowledge on which conceptual comprehension and practical design skills can be built. This includes definitions of new terms, explanations of processes, and discussion of relationships between components.

We cross-reference subjects that appear elsewhere in the book, that tie in to the topic of the chapter, and/or that will aid you in understanding the material presented in the chapter.

Concepts

In addition to basic knowledge-based information such as definitions and relationships, we provide an overview of the concepts behind the skills-based exercises. For example, managing the replication DNS data via Active Directory involves a particular skill set. An understanding of the concepts of both DNS and directory replication is necessary in order to perform the task correctly.

As much as possible, the authors attempt to make all abstract concepts easy to understand, using analogies and graphical illustrations.

Practical Skills

The heart of Windows 2000 exam preparation is development of practical skills: the ability not just to know about the operating system but also to use the operating system to perform common network administration tasks. The exam questions are expected to be performance based, as is obvious from the wording of the exam
objectives, almost all of which use verbs such as “create, configure, manage, implement, deploy, modify,” and the like. These are action verbs, indicating that you should be able to perform the designated tasks.

The exercises in this and other exam preparation books often involve problem solving—determining which solution is appropriate for a given situation. Other questions are more task oriented, geared toward exercises that simulate using the operating system interface. More so than with the NT exams, it is imperative that you do the practical exercises in each chapter of this book, that you experiment with various options, and that you gather hands-on experience in performing the tasks about which you read. Many of the exam questions are relatively simple for those who have worked with Windows 2000 and actually used the Active Directory for day-to-day tasks in their own networks—and almost impossible to answer for someone who hasn’t gone through the processes themselves. In this book, we attempt to simulate the Windows 2000 working environment as much as possible by liberal use of graphic illustrations and detailed descriptions of every aspect of the environment in which you are working; however, there is no substitute for doing it yourself.

If you are new to computer networking and are not already employed in the field as you study for these exams, see the section “What You Need to Know If You’re New to Networking” later in this chapter for some tips on how to get that all-important hands-on experience.

Some of the practical skills areas with which you should be sure you’re familiar before taking this exam include:

- Installing the Active Directory
- Working with subnets and sites
- Working with Windows 2000 DNS
- Working with Group Policy
- Managing Active Directory objects
- Configuring Active Directory replication options
- Using the Remote Installation Services (RIS)
CERTIFICATION OBJECTIVE 1.04

What You Should Already Know

Because Microsoft’s target audience for the Implementing and Administering a Windows 2000 Directory Services Infrastructure exam (and the other Windows 2000 exams) is those who have experience working with large multisite, multidomain NT networks, there is a presumption that you will have mastered the knowledge, concepts, and terminology presented in the Windows NT 4.0 certification exams.

If you do not have extensive real-world networking experience and you have not already attained the Windows NT MCSE, you should take extra time to ensure that you are familiar with Microsoft networking concepts, Windows 2000 concepts, and the terminology that is peculiar to directory services and Active Directory.

Microsoft Networking Concepts

Certainly anyone attempting to pass the Windows 2000 certification exams should have hands-on experience in deploying and using a Microsoft network. Whether you work with a multinational corporate internetwork or a small home network, the basic concepts of getting computers to communicate with one another are the same.

It is highly recommended that if you are new to the field, you take a basic networking course or work through a text on networking and operating system essentials to familiarize yourself with such basic concepts as:

- Peer-to-peer and client-server networking
- Network architectures and local area network (LAN) and WAN topologies
- Networking hardware and software, including client operating systems such as Windows for Workgroups, Windows 95 and Windows 98, Windows NT Workstation, and Windows 2000 Professional
Chapter 1: Introduction to Windows 2000 Directory Services Administration

- The Open Systems Interconnection (OSI) and U.S. Department of Defense (DoD) networking models, the IEEE specifications, and Internet standards published as requests for comments (RFCs)

Windows 2000 Concepts

We also recommend that you study and take exams 70-210 and 70-215, which focus on the Windows 2000 Professional and Server operating systems, respectively. Be familiar with the many ways in which Windows 2000 differs from its predecessor, Windows NT 4.0, as well as the ways in which the two systems are alike.

Once again, we stress the importance of actually working with Windows 2000 on a day-to-day basis. Get to know the Active Directory “up close and personal,” and it will no longer seem as mysterious, complex, or as much of a challenge to master (although it will remain challenging enough).

Be especially certain that you understand such Windows 2000 concepts as:

- Transitive trust relationships
- Hierarchical domain structure
- The role of Active Directory sites
- How OUs fit into the Active Directory structure

Also be familiar with the administrative tools that come with Windows 2000 Server and the Microsoft Management Console (MMC), including how to create custom MMCs.

Directory Services Terminology

For readers who are beginning their study of Windows 2000 with little exposure to real-life networking, one of the most important (and perhaps most tedious) tasks is to “learn the language” of computer networking. For this exam, that includes the specific terms peculiar to directory services. Otherwise, as you read through the study material, you may feel as though you’re floating in a sea of acronyms and unfamiliar words.

In this book, our policy is to spell out all acronyms in full the first time they appear and to define new terms within the text, whenever possible. However, what is a well-known term to a long-time networking professional may be “new” to you,
and in a book this size, trying to flip back through the pages to find the first occurrence of a word or term could be a time-consuming process. We suggest that you make liberal use of the glossary. If you run across a word or term for which you’re unsure about the meaning and it’s not obvious from the context, don’t just skim over it and hope it will be clarified later. Taking the time to look up the word or term may seem to slow your study, but in actuality it’s one of the best ways to ensure that you remember the meaning later.

As we start, be sure you know the meanings of the following terms:

- **Active Directory Services Interface (ADSI)** – This is a set of COM interfaces that enables Windows 9x, Windows NT, and Windows 2000 applications to access Active Directory and other directory services.

- **Application Programming Interface (API)** – A set of routines used by a program to request and carry out lower-level services performed by the computer’s operating system or other component, which provides the program with a way to communicate with the system.

- **Authentication** – The method used by the system to verify a user’s logon credentials.

- **Child domain** – A domain located directly beneath another (parent) domain in the Active Directory domain tree, which includes the parent domain’s name as part of its namespace.

- **Client Installation Wizard (CIW)** – The interface in RIS that makes installation options available to clients.

- **Delegation** – Assignment of administrative authority over a portion of the namespace to a user or group.

- **Directory** – A database containing information about objects.

- **Directory service** – The method by which directory information is stored and accessed by users and applications.

- **Distinguished Name** – A unique name that identifies an object and its location in a tree, which includes the relative distinguished name plus the names of container objects and domains in which the object resides.

- **Domain** – In Windows 2000, a collection of computers that share a common directory database, security policies, and security relationships with other domains and that represent a single security boundary of a Windows 2000
network. Domains can be joined in trees, which can in turn be joined in forests.

- **Domain tree**  A collection of Windows 2000 domains that share two-way transitive trust relationships, a contiguous namespace, and common schema, configuration, and global catalog.

- **Forest**  A group of one or more Windows 2000 domain trees that share schema, configuration, and global catalog but do not share a contiguous namespace.

- **Globally Unique Identifier (GUID)**  A 128-bit number assigned to an object when it is created, guaranteed to be unique on the network.

- **Group Policy**  The Windows 2000 feature used for controlling the behavior of user desktops, setting security, and deploying software.

- **Group Policy Object (GPO)**  A collection of Group Policy settings stored at the domain level and applied to sites, domains, or OUs.

- **Intersite replication**  Replication traffic between sites.

- **Intrasite replication**  Replication traffic within a site.

- **Kerberos version 5**  The latest version of the industry-standard security protocol used to handle authentication in Windows 2000 trust relationships.

- **Lightweight Directory Access Protocol (LDAP)**  A set of proposed standards outlined in RFC 2251, which provides for compatibility among directory services.

- **Multimaster replication**  The replication model used by Windows 2000 in which all domain controllers are capable of accepting and replicating changes in directory information to other domain controllers.

- **Native mode**  The domain condition in which all the domain controllers are running Windows 2000 (there are no “down-level” or NT domain controllers) and native mode has been explicitly enabled by an administrator, allowing the use of features not available in mixed mode.

- **Object**  An entity that is described by a set of attributes. An object could be a file, a user account, or a printer, and its attributes might include a name, location, and others, depending on the nature (class) of the object.
What You Should Already Know

- **Organizational Unit (OU)** A container object in Active Directory, which can be created within a domain for purposes of administrative boundaries. OUs can contain users, groups, computers, printers, and even other OUs.

- **Parent object** An object inside which another object resides (for example, a folder can be a parent object that contains a file, its “child”).

- **Relative Distinguished Name (RDN)** The part of an object’s distinguished name that is an attribute of the object.

- **Remote Installation Services (RIS)** A software service by which an administrator can set up new client computers remotely (via unattended installation).

- **Replication** The act of copying information from one computer to one or more computers to synchronize the data.

- **Schema** A description of the object classes and attributes stored in Active Directory.

- **Site** One or more “well-connected” IP subnets.

- **Subnet** A part of a divided network that shares a network address with other parts of the network and is distinguished by a subnet address.

- **Trust relationship** A relationship between domains in which a trusting domain will honor the logon authentication of a trusted domain.

- **User Principal Name (UPN)** A user account name plus a domain name in which the account resides, with the two separated by an @ sign (for example, deb@shinder.net).

- **Zone** A subtree of the DNS database that is administered as a single entity.

- **Zone transfer** The method by which DNS servers synchronize data.

For Networking Newbies and NT Pros

Readers of this book who are studying for Exam 70-217 will not all be at the same level of experience and expertise. We recognize this fact, and throughout the text, we attempt to offer special tips that are geared toward people who are beginning their networking careers with the study of Windows 2000. We also provide
information that targets readers who have mastered the basics of Windows NT and are already very familiar with Microsoft networking.

**What You Need to Know If You’re New to Networking**

As mentioned, if you are new to computer networking, we recommend that you take a course or study a good book in basic networking concepts before you sit for the mandatory core exams. Even if you are following the Windows 2000 MCSE certification track, it would benefit you to study one of the NT 4.0 Networking Essentials study guides and/or take the Windows 2000 Network and Operating Systems Essentials course.

You will find that familiarizing yourself with basic networking and Active Directory concepts will benefit you in many ways. Not only will the knowledge provide a solid foundation for the material you will study in the process of obtaining Microsoft certification, but most employers will expect you, as an MCP or MCSE, to be familiar with these fundamental concepts.

The very best investment a networking neophyte can make, though, is building your own network from the ground up. Even a simple two-computer thinnet will give you a taste of the challenges faced by enterprise pros in the field. Many of the setup, maintenance, and troubleshooting scenarios associated with large production networks can be simulated on a smaller scale with a small home network. Deploy Active Directory on your test network and learn how it really works. Even on such a small scale, the experience will teach you many valuable lessons about the difference between a plan that “looks good on paper” and one that really works in the field.

**New Ways of Working for Experienced NT Administrators**

If you are already certified and/or experienced in NT 4.0, you may be tempted to skip some parts of this book, such as those that discuss familiar protocols or services such as DNS. But don’t skip too much! Windows 2000 is built on the NT kernel, and you will find much in the new operating system that feels like “home”—but the Active Directory of Windows 2000 differs drastically from the rather feeble directory services of NT. You will also discover, as you delve deeper, that there are many fundamental changes, even to “old friends” such as DNS.

NT professionals need to guard against the possibility that their experience and mastery of the earlier operating system will be their biggest enemy on the Windows
2000 certification exams. Expect questions that try to “trick” exam takers by providing solutions that would have been correct if you were using NT or that measure whether you’re aware of the differences between the two operating systems (just as there were traditionally questions on the NT certification exams that used experience with Windows 9x against a test taker in the same way).

We certainly don’t advise NT pros to forget everything you ever knew about network operating systems, but we do encourage you not only to study Windows 2000, but to actually use it on a day-to-day basis. If possible, upgrade your primary workstation to Windows 2000 Professional so that the slightly different ways of performing routine tasks, the subtle differences in the interface, become second nature to you. Work with Windows 2000 Server or Advanced Server on the job if you can, at home or in the classroom if not. The real differences between NT and Windows 2000 show themselves in the server products. As you work with the Windows 2000 network, consider how design decisions that were made during the pre-implementation stage affect their ease of administration (or lack thereof) on a day-to-day basis.

Your NT experience can put you a step ahead of the networking newcomers—if you remember not to make too many assumptions (generally a good policy to follow in all areas of life).

CERTIFICATION SUMMARY

This chapter provided a brief introduction to the many Active Directory concepts and design issues that are discussed in this book. We have given you an overview of the topics you might expect to see in exam 70-217, as well as some tips on the background information you will need before you begin to study for the Implementing and Administering a Windows 2000 Active Directory Infrastructure exam.

We offered some advice for brushing up on Active Directory terminology and wrapped up with information aimed at particular types of exam candidates, such as networking newbies and NT “old pros.” We also included a brief description of each exam objective provided by Microsoft.

The subsequent chapters of this book address each exam objective in detail and provide practical exercises geared toward teaching you the exam material in a hands-on, step-by-step process.
TWO-MINUTE DRILL

What Is Windows 2000 Directory Services Administration?

- A directory is a database that contains information about objects and their attributes; a directory service is the component that organizes the objects in a logical and accessible structure and provides a means of locating them within the directory.

- Active Directory offers far greater scalability than NT’s directory service, NTDS, allowing for millions of security objects in a domain, compared with about 40,000 allowed in NT.

- Directory data includes domain data, configuration data, and schema data, and this data is replicated to all domain controllers in the domain so that each has an identical read/write copy of the directory database on its hard disk.

- Some advantages of Active Directory that make it a global directory service include support for Internet and industry standards such as LDAP, DNS, DHCP, and TCP/IP and its centralized management through a consistent management interface, the MMC.

Overview of Exam 70-217

- The Active Directory has both a physical structure, defined by sites, and a logical structure, defined by domains. Domain structure is hierarchical, with domains joined in a tree; trees themselves are joined into forests, in which all domains share a common schema, configuration, and global catalog.

- Installing the Active Directory is done by running the command DCPROMO.EXE on a Windows 2000 Server, which starts the Active Directory Installation wizard. The same command and wizard are used to demote a domain controller to member or stand-alone server status and remove the directory.

- Active Directory uses multimaster replication; however, some operations must be performed as single-master operations. For this purpose, five special roles, called operations masters, are assigned to one domain controller per forest or per domain (depending on the role) which include
schema master, domain naming master, infrastructure master, RID master, and PDC emulator.

- **Organizational units (OUs)** are container objects that represent the smallest administrative boundary in Active Directory and can contain users, groups, computers, printers, and other OUs.

- DNS is thoroughly integrated in Active Directory, and DNS zone information can be replicated via either standard zone storage or directory-integrated zone storage, which optimizes replication because the information is stored in the directory.

- **Group Policy** is used to control user environments, deploy software, and otherwise exercise flexible, granular administrative control. **Group policy objects (GPOs)** are collections of Group Policy settings that can be applied to sites, domains, or OUs and filtered by security groups.

**What We’ll Cover in This Book**

- **Remote Installation Services (RIS)** are used to install Windows 2000 Professional in unattended mode on multiple computers.

- Active Directory resources, such as shared folders and printers, can be **published** to the directory and easily located by network users, who don’t have to be aware of the objects’ physical locations to find and access them.

- The Windows 2000 certification core exams will focus on performance-based questions that measure skills rather than just knowledge.

**What You Should Already Know**

- Windows 2000 Active Directory uses two-way transitive trust relationships between all domains in a tree or forest.

- Setting up a network from scratch and using it on a day-to-day basis—even if it is only a two-computer simple home network—will help you tremendously in understanding the concepts and application of those concepts as you study Windows 2000 and the Active Directory.

- Prior to beginning your study of how to implement and administer a Windows 2000 directory services infrastructure, you should familiarize yourself with common Active Directory terminology, as outlined in this chapter.
SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully because there may be more than one correct answer. Choose all correct answers for each question.

What Is Windows 2000 Directory Services Administration?

1. “An underlying base or foundation for an organization or system” is the definition of which of the following?
   A. Active Directory
   B. An infrastructure
   C. Directory services
   D. Attributes

2. Which of the following distributes directory data across the enterprise network and is participated in by all domain controllers in a Windows 2000 domain?
   A. Global catalog
   B. Security subsystem
   C. Data store
   D. Replication

3. Which of the following definitions describes the schema?
   A. A set of rules defining the classes of objects and attributes contained in the directory
   B. A means of querying and indexing information
   C. A map of the physical structure of the directory and how replication occurs between sites
   D. A collection of domains that share a contiguous namespace

4. Which of the following is true of Active Directory? Select all that apply.
   A. The Active Directory namespace is flat.
   B. The Active Directory is LDAP compatible.
   C. The Active Directory uses Kerberos authentication.
   D. The Active Directory uses explicit two-way, nontransitive trust relationships between domains, by default.
5. Which of the following is an example of directory data that is replicated? Select all that apply.
   A. Configuration data
   B. Site data
   C. Global data
   D. Domain data

6. Which of the following is the set of high-level, language-independent directory service programming interfaces that support the ability to work with resources provided by other operating systems and directory services?
   A. SSPI
   B. TCP/IP
   C. ADSI
   D. ADSL

7. In Windows 2000’s Active Directory environment, which of the following is used to customize and control the user environment?
   A. System Policy
   B. Group Policy
   C. Audit Policy
   D. Windows Explorer

8. How can Active Directory sites benefit a large network with multiple geographic locations? Select all that apply.
   A. To optimize logon authentication traffic
   B. To optimize directory replication traffic
   C. To optimize broadcast traffic
   D. To optimize routing

9. Which of the following describes a hierarchical structure or arrangement?
   A. All objects are peers, on the same “level.”
   B. There are numerous “roots” that spawn branches.
   C. Objects residing beneath other objects are known as child objects, and those above them are known as parent objects.
   D. The namespace is noncontiguous.
10. Which of the following commands would you use if you wanted to demote a Windows 2000 Server domain controller to member server status and remove the Active Directory?
   A. DCDEMOTE.EXE
   B. DCPROMO.EXE
   C. DCPROMOTE.EXE
   D. DCDEMO.EXE

11. Which of the following describes a domain controller that contains a partial replica of every domain in Active Directory but includes only some of the objects’ attributes—those most often used in search operations?
   A. Primary domain controller
   B. Replica server
   C. Global catalog server
   D. All domain controllers

12. Which of the following operations master roles is forestwide? Select all that apply.
   A. Schema master
   B. Infrastructure master
   C. RID master
   D. Domain-naming master

13. Which of the following can be placed into OUs? Select all that apply.
   A. Other OUs
   B. Printers
   C. Schemas
   D. Sites

14. Which of the following is true of an authoritative restore? Select all that apply.
   A. It can be performed on all Windows 2000 Servers but not on Windows 2000 Professional machines.
   B. It restores only replicated system state data.
   C. It is performed using the NTDSUTIL.EXE utility.
   D. It can be done by administrators, server operators, and power users.
SELF TEST ANSWERS

What Is Windows 2000 Directory Services Administration?

1. B. An infrastructure is defined as “an underlying base or foundation for an organization or system.”
   A is incorrect because the Active Directory is an example of a directory service. C is incorrect because a directory service is defined as a means of organizing directory information and providing a way to search and locate objects within the directory. D is incorrect because attributes are the properties of an object.

2. D. Replication is the process of distributing directory data across the network.
   A is incorrect because a global catalog is a subset of information about all the objects in the directory, used to find directory information. B is incorrect because the security subsystem is the means of providing secure logon and access control. C is incorrect because the data store is another term for directory.

3. A. The schema is the set of rules that defines the classes of objects and attributes contained in the directory.
   B is incorrect because the schema does not pertain to queries and indexing. C is incorrect because a map of the physical structure of the directory showing how replication occurs is the replication topology. D is incorrect because a collection of domains that share a contiguous namespace is a domain tree.

   A is incorrect because the NT namespace is flat, whereas the Active Directory namespace is hierarchical. D is incorrect because the Active Directory trusts are implicit two-way transitive trust relationships.

5. A and D. Configuration data and domain data, along with schema data, are the three types of directory data that are replicated.
   B and C are incorrect because there is no such specific data type as site data or global data.

6. C. The Active Directory Services Interface (ADSI) is the programming interface that supports interoperability with other operating systems and directories and is used for developing applications for Windows 2000 Server.
   A is incorrect because SSPI is the Security Services Provider Interface. B is incorrect because TCP/IP, Transmission Control Protocol/Internet Protocol, is the standard protocol
stack used for communication on large networks and the Internet. D is incorrect because ADSL is Asymmetric Digital Subscriber Line, a high-performance telephone service.

7. ☑ B. Group Policy is the component used to control the user environment in Windows 2000 Active Directory networks.
   ☒ A is incorrect because System Policy was used in NT networks to control the user environment. C is incorrect because audit policy is used to track logons/logoffs, access to objects, and other activities. D is incorrect because the Windows Explorer is used for file management.

8. ☑ A and B. Establishing separate sites for areas connected by slow WAN links, you can optimize both logon authentication traffic and directory replication traffic because you can configure interval and scheduling of intersite replication, and the Active Directory client will seek a domain controller within its site to log onto.
   ☒ C is incorrect because sites do not affect broadcast traffic. D is incorrect because sites do not affect routing of packets.

9. ☑ C. In a hierarchical structure such as a domain tree, objects residing beneath other objects are known as child objects, and those above them are known as parent objects.
   ☒ A is incorrect because the objects are not all on the same level, as they would be in a flat structure. B is incorrect because each hierarchy has only one root. D is incorrect because the namespace is contiguous, with the full name of each child object containing the full name of its parent.

10. ☑ B. The DCPROMO.EXE command invokes the Active Directory Installation wizard, which is used to both promote a Windows 2000 server to domain controller and demote a domain controller to member or standalone server.
    ☒ A, C, and D are incorrect because there are no such commands as DCDEMOTE.EXE, DCPROMOTE.EXE, and DCDEMO.EXE.

11. ☑ C. The global catalog server is a domain controller that contains a partial replica of every domain in Active Directory. The global catalog holds a replica of every object in Active Directory, but it includes only some of the objects’ attributes—those most often used in search operations.
    ☒ A is incorrect because the primary domain controller is the master domain controller on a Windows NT network. B is incorrect because there is no such thing as a replica server. D is incorrect because not all domain controllers are global catalog servers.

12. ☑ A and D. The schema master and domain-naming master are the two operations masters whose roles are forestwide, and there can be only one of each in a forest.
B and C are incorrect because both the infrastructure and RID master roles are domainwide, so there is one for each domain.

13. A and B. Organizational units can contain other OUs (called nesting), printers, users, groups, shared folders, and other network resources.

C is incorrect because a schema is a set of rules that applies to an entire forest. D is incorrect because sites are components of the physical directory structure.

14. B and C. An authoritative restore is performed using the NTDSUTIL.EXE utility, and only replicated and system state data such as Active Directory data and File Replication Service data are restored.

A is incorrect because it can be performed only on Windows 2000 domain controllers, not all servers. D is incorrect because it can be performed only by administrators.