

**StudyExam4Less**  
A Division of My Learning Camp, Inc.

**770-456-5430**

**Delivered by**

**<http://www.StudyExam4Less.com>**

**Buy this product today**

**And SAVE BIG**

**Enter Coupon code : **DEMO****

**(This coupon code entitles you 5% discount)**  
**(offer subject to withdrawal without notice)**

CopyRight 2004 <http://www.StudyExam4Less.com>

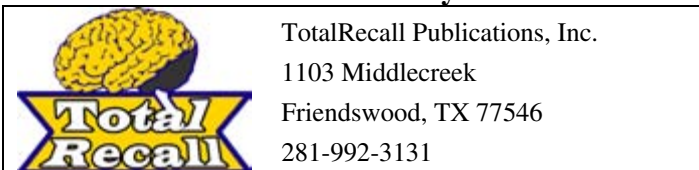
**ExamInsight  
For  
Installing, Configuring, and Administering  
Microsoft® Windows 2000  
Directory Services Infrastructure  
Examination 70-217**



**CD-ROM practice exam provided by  
BeachFrontQuizzer, Inc., Friendswood, Texas**

**Author  
Patrick Simpson  
MCSE, MCT, MCNI, MCNE**

**Published by**



TotalRecall Publications, Inc.  
1103 Middlecreek  
Friendswood, TX 77546  
281-992-3131

**NOTE: THIS IS BOOK IS GUARANTEED:  
See details at [www.TotalRecallPress.com](http://www.TotalRecallPress.com)**

TotalRecall Publications, Inc.

**This Book is Sponsored by BeachFront Quizzer, Inc.**

Copyright © 2003 by TotalRecall Publications, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the United States Copyright Act of 1976, No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means electronic or mechanical or by photocopying, recording, or otherwise without the prior permission of the publisher.

The views expressed in this book are solely those of the author, and do not represent the views of any other party or parties.

Printed in United States of America  
Printed and bound by Data Duplicators of Houston Texas  
Printed and bound by Lightning Source, Inc. in the USA and UK

ISBN: 1-59095-604-4  
USB: 6-43977-02217-2

The sponsoring editor is Bruce Moran and the production supervisor is Corby R. Tate.

Worldwide eBook publication and distribution by:



This publication is not sponsored by, endorsed by, or affiliated with Microsoft, Inc. The “Windows® 2000, MCSE™, MCSA™, MCSE+I™, MCT™” Microsoft logos are trademarks or registered trademarks of Microsoft, Inc. in the United States and certain other countries. All other trademarks are trademarks of their respective owners. Throughout this book, trademarked names are used. Rather than put a trademark symbol after every occurrence of a trademarked name, we used names in an editorial fashion only and to the benefit of the trademark owner. No intention of infringement on trademarks is intended.

**Disclaimer Notice: Judgements as to the suitability of the information herein for purchaser’s purposes are necessarily the purchaser’s responsibility. BeachFront Quizzer, Inc. and BFQ Press extends no warranties, makes no representations, and assumes no responsibility as to the accuracy or suitability of such information for application to the purchaser’s intended purposes or for consequences of its use.**

## **A Quick overview of the book chapters:**

<b>Chapter 1: Windows 2000 Active Directory Services .....</b>	<b>1</b>
<b>Chapter 2: Using DNS With Active Directory Service ....</b>	<b>39</b>
<b>Chapter 3: Configuration Management .....</b>	<b>67</b>
<b>Chapter 4: Active Directory Components .....</b>	<b>107</b>
<b>Chapter 5: Directory Services Infrastructure Security</b>	<b>143</b>
<b>Appendix A: Answers .....</b>	<b>167</b>
<b>Index .....</b>	<b>229</b>
<b>Money Back Book Guarantee .....</b>	<b>233</b>
<b>Microsoft 70-217 Practice Exam Offer .....</b>	<b>234</b>

## Chapter 1: Windows 2000 Active Directory Services

**The objective of this chapter is to provide the reader with an understanding of the following:**

- The basic structure and purpose of Active Directory.
- The various components of Active Directory.
- An understanding of mixed mode versus native mode.
- The various operations master roles in Active Directory.

---

### Getting Ready - Questions

- 1) What are the two types of domain environments in Active Directory?
  - 2) A collection of domains in Windows 2000 is called what?
  - 3) What are the three scopes available for groups in Active Directory?
  - 4) What does the acronym OU stand for?
  - 5) What are the five different operations master roles called?
- 



### Getting Ready - Answers

- 1) What are the two types of domain environments in Active Directory? Mixed mode and native mode
  - 2) A collection of domains in Windows 2000 is called what? A tree
  - 3) What are the three scopes available for groups in Active Directory? Domain local, global, and universal (in native mode only)
  - 4) What does the acronym OU stand for? Organizational unit
  - 5) What are the five different operations master roles called? PDC emulator, RID master, infrastructure master, domain naming master, and schema master
- 

## I Introduction

The purpose of this first chapter is to help familiarize you with the basic concepts of Active Directory. How quickly you are able to master these concepts will depend on your background in the computer industry. Those who have an extensive Novell background will find many of the features of Windows 2000 Active Directory familiar. As will those of you who have worked with Microsoft Exchange server. A good fundamental understanding of Windows NT will also be helpful as you strive to learn these topics.

Regardless of your background, please make sure to spend as much time in Chapter One as necessary for you to feel comfortable with these ideas. They form the foundation upon which the understandings of all Active Directory concepts are built. While all of the concepts in Chapter One are covered much more in depth throughout the rest of the book, it's still important to spend the appropriate time in this section.

You might have heard the parable about the man who built his house on sand. Likewise, if you simply skim through the first chapter you could be building a foundation for yourself that isn't solid at all. Now that the ominous warning is out of the way, let's move on. Without further ado, let's begin our journey together into the realm of Active Directory.



## II Components of the Active Directory Service

The first item that we'll look at isn't really a component of Active Directory, but without it Active Directory won't function. I'm referring to the Domain Name System, most often referred to as DNS. This technology has been around for many years and has been primarily used in conjunction with the Internet.

### DNS

The most basic way to describe DNS is this: It's a system for converting human friendly computer names to computer friendly Internet Protocol (IP) addresses. The need for such a system is self-evident. Let's say I want my users to visit my website. Without DNS I would have to give them the IP address of the site. For most people, it's certainly easier to remember [www.bfq.com](http://www.bfq.com) than 216.248.197.15.

In the Microsoft networking world, DNS has been used for a while now, but always as an add-on. Microsoft's preferred method of name resolution in its networks was through the use of Net BIOS names. Early on, this method was OK in small environments that didn't change much. However this method really didn't work well for large-scale networks.

Rather than admit defeat and convert to the DNS naming convention, Microsoft developed the Windows Internet Naming Service (WINS) in Windows NT 3.5. This technology certainly helped to make Net BIOS more viable in an enterprise environment, but it still didn't match up to DNS. With the release of Windows NT 4, Microsoft allowed for integration between WINS and DNS. However, it still wasn't the elegant solution that many administrators were looking for.

With the release of Windows 2000, Microsoft has finally woken up to the fact that DNS is the name resolution method of choice. While Windows 2000 supports Net BIOS naming and the WINS architecture, it is no longer encouraged. In fact, Microsoft has stated that in a properly configured Windows 2000 environment that there should be no need for WINS or Net BIOS at all.

Let's take a brief look at how the most common form of DNS resolution, known as recursion, operates (see Figure 1-1 for a visual representation). Say you enter the address [www.bfq.com](http://www.bfq.com) in the address field of your Internet browser. The first thing your system will do is see if the IP address for that address is in its local cache. The reason it would be there is if you had gone to the website recently.



#### 4 Chapter 1: 70-217 Certification

Assuming that the entry isn't in the cache, it will then contact a predefined DNS server. This server is usually assigned by an administrator manually or through DHCP. That DNS server will see if it has the entry for that address in its cache. The entry would be there if this DNS server had resolved this address for one of its clients recently.

If the entry does exist in the cache of your DNS server then that server will return the address to your machine. If the entry isn't there, your server will then contact the root domain authority for the .com domain. It will request the IP address of the DNS server that is authoritative for the bfq.com domain. It will then query that server for the proper address.

Once your DNS server has the proper address it will do two things. First, it will send the address back to your machine so that you can get to the appropriate page. It will then place the entry into its cache for a predefined period of time. That way if anyone asks it for that address during that time frame, it can simply return the address it has without having to go through the whole resolution process again.

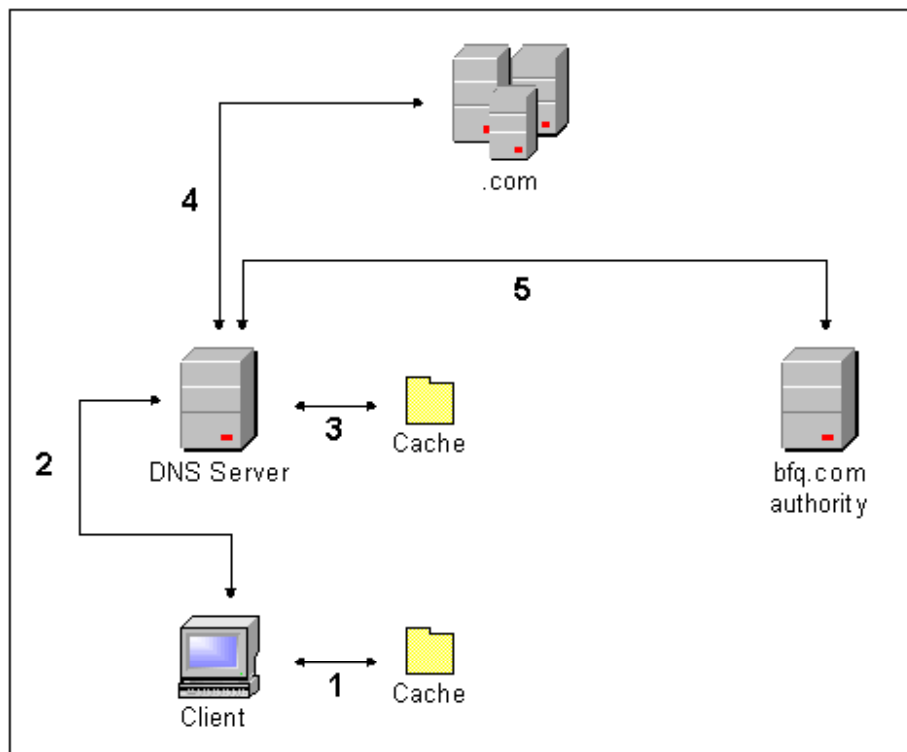


Figure 1-1: DNS Server Addressing



Once your machine has received the address, your web browser should then display the appropriate page on your screen. Your system will also cache the entry itself on your local machine so that if you request the address again within a certain time frame it won't have to go through the whole resolution process again. This not only saves time but also reduces the load on your DNS servers as well as network traffic.

This is but the briefest look at DNS. We will go more in depth into DNS in Chapter 2. The main thing for you to remember is that DNS is not only an Internet name resolution process but is also an integral part of the Active Directory architecture.

## Domains

Those of you coming from the Windows NT world should be intimately familiar with the concept of domains. For those of you who aren't familiar with them or who only have a passing understanding of them, we'll take some time to discuss them in detail. Whether familiar with the concept of Windows NT domains or not, make sure to take the time to read through this section. Domains in Windows 2000 are similar to the ones in NT but they have changed enough that you should take some time to acquaint yourself with the differences.

Domains in Windows NT were designed to provide a centralized method of managing users, computers and resources. They were designed to replace the old workgroup model of networking. In workgroups, every system can act as a client and a server. The main problem with this method is that you have to create user accounts on each machine for each person. Not only can this be a tedious process, it's downright inefficient. Another problem is that there is no centralized method of creating these users.

With the domain architecture, administrators can create one user account for each person accessing the network. This account can be created and managed from a central location. Another benefit of domains is that access to resources such as files and printers can also be controlled from a central location.

While this is all well and good, there are issues with the domain model in Windows NT. The first is scalability. The directory database in NT is what holds the information on all the user, computer and group accounts in a Windows NT domain. Unfortunately it has a maximum recommended size of 40MB. This can be a severe limitation for large organizations.



## 6 Chapter 1: 70-217 Certification

Fortunately NT allows for multiple domains so that you can easily get around this limit. The bad part is that once you get past a few domains things start to become cumbersome. Several tasks can be difficult to manage. Some include establishing and maintaining trust relationships and managing permissions.

Another issue with Windows NT as a server operating system as a whole is the lack of any true directory services. While Microsoft would like people to believe that browsing through the Network Neighborhood icon for resources is a form of directory service, I think most people realize that it isn't. The ability to efficiently locate resources in Windows NT is one feature that operating system is sorely lacking.

Enter Active Directory, which was designed from the ground up as scalable directory services architecture. Active Directory was designed in such a way as to alleviate, if not totally eliminate, the issues listed above. The domains in Active Directory are more flexible and easier to manage than those in Windows NT. Let's take a look at some of the new features and improvements that this domain structure offers.

Let's start with the concept of scalability. Microsoft listened to the complaints about the poor scalability of Windows NT as it was designing Windows 2000. The first thing that they did was to design the directory database in such a way that it could far surpass the 40MB limit that exists in NT. This allows you to create domains that aren't subjected to the same constraints that exist in NT and that can thus be scaled accordingly.

**An important thing to remember about the size of the directory database in Windows 2000 that it can only go above 40MB in Native mode. If you are running your domain in Mixed mode, it is still subject to the 40MB limit.**

When dealing with multiple domains in Windows 2000, Microsoft made several changes to the way in which these domains inter-operate. One of the best things that they did was to allow for the automatic creation of two-way transitive trusts when creating new domains with the same namespace. This eliminates the need to manually create and maintain trusts as you did in Windows 2000 and also makes dealing with permissions across domains easier.

As far as the concept of directory services is concerned, you will find as you read through this book that there is no comparison between finding resources in a Windows 2000 Active Directory domain and finding them in a Windows NT domain.



The ability for users to find and access resources in Active Directory is one of the significant improvements that Windows 2000 offers.

Now that we've looked at the basic concept of what an Active Directory domain is, let's move into what items make up that domain. Let's begin with the servers that contain the Active Directory database. These are called domain controllers.

## Domain Controllers

Just as Windows NT had domain controllers, so to does Windows 2000 and Active directory. In order to understand how domain controllers have changed, let's look at what exactly they are and how they differ between NT and 2000.

In very simple terms, domain controllers are the servers upon which the domain database resides. They are responsible for maintaining the list of all users and computers in a domain as well as all relevant security information. They are what are contacted when a user attempts to logon to the domain to ensure that the user has the appropriate rights to do so. They are also asked to help verify whether a user or group has permissions to access certain resources.

In Windows NT there are two different types of domain controllers: Primary Domain Controllers (PDCs) and Backup Domain Controllers (BDCs). The main difference between the two is that the copy of the directory database, also known as the Security Accounts Manager (SAM) database, on the PDC is the only editable copy. The version on the BDCs is read-only and thus cannot be modified. The other difference is that there can be only one PDC in a domain while there can be as many BDCs as required.

In small network environments this isn't generally a problem. You have a PDC and a few BDCs on your network to assist with user logons and such. However, if your network spans several locations and consists of many thousands of users and computers, having only one editable copy of the SAM database becomes a problem. This server is generally overtaxed in such large environments and if the PDC happens to develop a problem, there can be serious repercussions. Plus, being able to manage users and other domain resources only from the SAM on the PDC can be slow and monotonous since the machine is usually bogged down.

In Windows 2000 and Active Directory this whole concept has changed. Active Directory domain controllers are what is known as multimaster. In essence this means that each of the domain controllers are considered equal.



## 8 Chapter 1: 70-217 Certification

They each contain a copy of the domain database that is fully editable. As with some of the other features we've already listed, this really helps Active Directory to be much more scalable than Window NT. This also increases the fault tolerance of the operating system since it's now easier to recover from the loss of a domain controller.

While in essence all domain controllers are considered equal, there are certain roles that they can have that differentiate them from one another. These roles are known as Operations Master Roles and are covered in detail later in this chapter.

### Objects

Let's now move into the topic of objects. Objects are the pieces that make up your Active Directory. Each object is a collection of different attributes. These attributes represent the properties of each object. Each type of object is known as a class. Below is a list of the more common object classes in Active Directory.

#### Users

Users are the objects that represent the individuals that will be accessing the resources on your network. In Windows 2000, as was the case in Windows NT, Microsoft recommends that you don't assign permission directly to users. Instead they recommend the use of groups.

#### Groups

Groups are simply a collection of users. Groups are the primary method used to assign permissions to resources. Rather than going through the task of trying to assign permissions to individual users, you should place users who should have the same level of access into the same group and assign access to that group.

For example, let's say you want to give the accounting department access to a particular share called Payroll on your server. Further, let's say you want to give them all the ability to print to a printer called CheckPrinter. Rather than going through the process of giving permissions to every individual user, you would add them to a group (let's use Accounting). You would then give the Accounting group access to each of these resources. In that way, if you have a new employee join the accounting department, you can simply add them to the group.

In Active Directory there are two classifications of groups: Security and Distribution. Security groups are used for applying permissions to Active Directory objects.



Distribution groups are used by Windows 2000 savvy programs for non-security related functions. An example of this would be the use of a distribution group for email purposes for Microsoft Exchange users.

These classifications are then broken down into one of three categories: domain local, global and universal. Domain local groups are just that, groups that are local to a single domain.

In a mixed mode environment they can contain users and groups from any domain. In a native mode domain they can also contain universal groups from any domain and other domain local groups from the same domain.

Global groups are groups that are created in a single domain but can be utilized in other domains. In mixed mode the only thing that global groups can contain are users from the same domain. In native mode global groups can also contain other global groups from the same domain.

Universal groups are a new group type in Windows 2000 that only exist in native mode. They can contain users, global groups and other universal groups from any domain in your forest. Obviously, the features of universal groups are better than those of other groups so you might be wondering why you would ever want to use the other types in a native environment. The primary reason has to do with the Global Catalog (which we'll discuss in detail later). Domain local groups and global groups are listed in the global catalog, but their members aren't. Universal group members are listed however, making the Global catalog larger and thus increasing replication traffic.

### OUs

Organizational units (OUs) are a new type of container object in Windows 2000. They are used to organize the different resources in your network into easily managed pieces. How you set these up is entirely up to you. You can organize them geographically, by department, by administrative function, or however you see fit. They were designed to reduce the number of domains that you might need to setup in Windows 2000.

OUs can contain users, groups, printers, computers, and other OUs. One of the primary purposes for OUs is to assign group policies. They can also be used as a method of delegating administrative authority. Another thing that they can be used for is to assign software to users and computers. There are many more uses that we'll cover throughout the book.



**Remember that even though OUs are preferred over domains to organize your resources, domains form the security boundaries of Windows 2000. That means that if you want to have different password security policies, you will have to do them through the use of domains.**

## Trees

One of the new concepts that differentiates Windows 2000 from Windows NT is that of trees. A tree is a collection of domains that share a contiguous namespace. Simply put, that means if your root domain is bfq.com, then all of your other domains within that tree will contain bfq.com in their name. This is demonstrated in Figure 1-2.

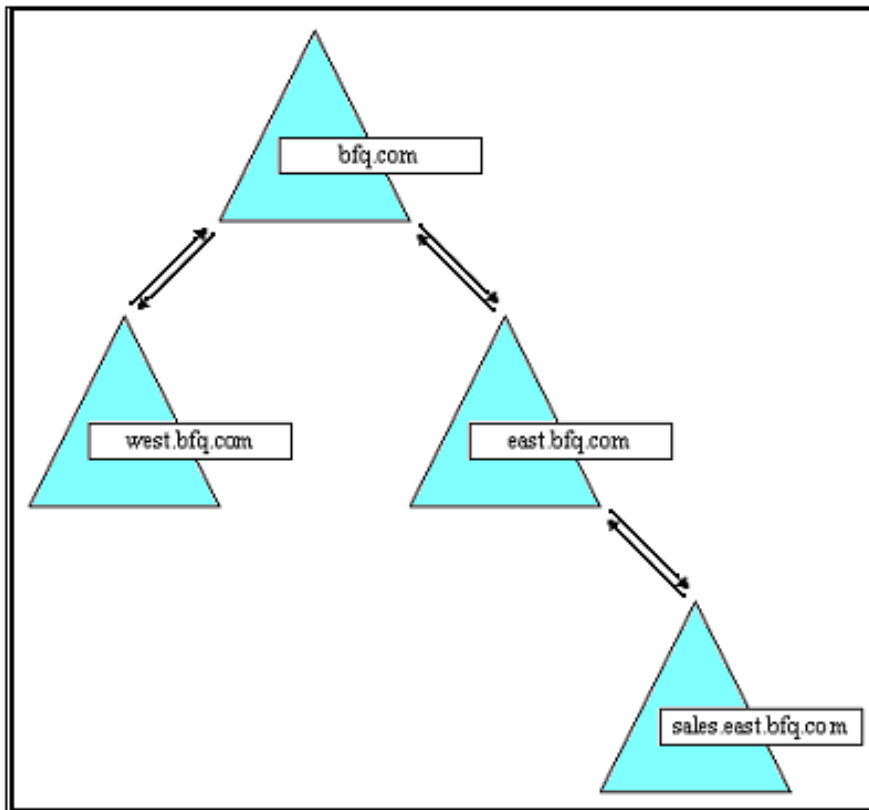


Figure 1-2: Tree Domains



**Other Microsoft Certification books by  
TotalRecall Publications**

**InsideScoop to MCP / MCSE Certification: Exam 70-217  
Managing a Microsoft Directory Services Infrastructure**

**ExamWise For MCP / MCSE Certification: Exam 70-217  
Managing a Microsoft Directory Services Infrastructure**

**ExamInsight For MCP / MCSE Certification: Exam 70-210  
Managing Microsoft Windows 2000 Professional**

**ExamInsight For MCP / MCSE Certification: Exam 70-216  
Implementing and Administering a Microsoft Windows 2000  
Network Infrastructure**

**ExamInsight For MCP / MCSE Certification: Exam 70-219  
Designing a Windows 2000 Directory Services Infrastructure**

**ExamInsight For MCP / MCSE Certification: Exam 70-220  
Designing Security for a Microsoft Windows 2000 Network**

**ExamInsight For MCP / MCSE Certification: Exam 70-221  
Designing a Microsoft Windows 2000 Network Infrastructure**

**ExamInsight For MCP / MCSE Certification: Exam 70-227  
Installing, Configuring, and Administering Microsoft Internet  
Security and Acceleration (ISA) Server 2000, Enterprise Edition**

**ExamInsight For MCP / MCSE Certification: Exam 70-270  
Microsoft Windows XP Professional**



# **BeachFront Direct**

**If you can PASS our Simulated Exam,  
We Guaranty you will PASS the Real Exam.**

## **Call**

**877-654-2265**

**727-450-0476**

**[www.bfqd.com](http://www.bfqd.com)**

**[www.BeachFrontDirect.com](http://www.BeachFrontDirect.com)**

**StudyExam4Less**

A Division of My Learning Camp, Inc.

**770-456-5430**

**StudyExam4Less.com offers great quality study guides at very affordable prices.**

**Check them out at**

**<http://www.StudyExam4Less.com>**

- **CompTIA**
- **Microsoft**
- **Cisco**
- **Novell**

**Take our word! You will like it.**

**That is not all. Enjoy our 5% additional discount. Enter**

**Coupon code: DEMO at <http://www.StudyExam4Less.com>**

**(offer subject to withdrawal without notice)**

CopyRight 2004 <http://www.StudyExam4Less.com>