
Module 3: Creating a Windows 2000 Domain

Contents

Overview	1
Introduction to Creating a Windows 2000 Domain	2
Installing Active Directory	3
Lab A: Creating a Windows 2000 Domain	12
The Active Directory Installation Process	16
Examining the Default Structure of Active Directory	27
Performing Post Active Directory Installation Tasks	29
Lab B: Performing Post Active Directory Installation Tasks	38
Troubleshooting the Installation of Active Directory	44
Removing Active Directory	46
Best Practices	48
Review	49



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BackOffice, FrontPage, IntelliMirror, PowerPoint, Visual Basic, Visual Studio, Win32, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Instructor Notes

Presentation:
105 Minutes

This module provides students with the knowledge and skills to install the Active Directory® directory service on a computer running Microsoft® Windows® 2000 Advanced Server, and perform post-installation tasks.

Labs:
60 Minutes

At the end of this module, students will be able to:

- Identify the purpose of creating a Windows 2000 domain.
- Create a Windows 2000 domain by installing Active Directory.
- Describe the process for installing Active Directory.
- Examine the default structure of Active Directory.
- Perform post Active Directory installation tasks.
- Troubleshoot common problems that may occur when creating a Windows 2000 domain.
- Remove Active Directory by using the Active Directory Installation wizard.
- Apply best practices for creating a Windows 2000 domain.

In the hands-on labs in this module, students will have a chance to create a Windows 2000 domain. In the first lab, students will install Active Directory by using the Active Directory Installation wizard. In the second lab, students will verify that Active Directory is correctly installed, convert standard primary DNS zones to Active Directory integrated zones, and convert a domain from mixed mode to native mode. The students will then create organizational units (OUs) according to the OU design provided in the lab.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2154A_03.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read the *unattend.doc* file in the *Deploy.cab* file located in the \Support\Tools folder on the Windows 2000 Advanced Server compact disc.
- Read the white paper, *Active Directory Technical Summary* on the Student Materials compact disc.
- Read chapter 1, “Active Directory Logical Structure” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.
- Read chapter 2, “Active Directory Data Storage” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.
- Read chapter 3, “Name Resolution in Active Directory” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.

Module Strategy

Use the following strategies to present this module:

- Introduction to Creating a Windows 2000 Domain

In this topic, you will introduce creating a Windows 2000 domain. Begin the module with a discussion about the purpose of creating a Windows 2000 domain in Windows 2000.

- Installing Active Directory

In this topic, you will introduce installing Active Directory. Begin the module by presenting the hardware, software, network, and configuration requirements for installing Active Directory. Explain how to use the Active Directory Installation wizard to create the first domain. Use the simulation to demonstrate how to create the first domain, as the first domain cannot be created on the instructor computer. Emphasize that this module focuses only on creating the first domain and adding a replica domain controller to an existing forest. Tell the students that they will learn to create child domains in Module 10 of this course. Next, illustrate how to add an additional domain controller to an existing domain. Finally, illustrate how use an unattended Setup script to install Active Directory. Show the students some sample answer files, and explain the different entries in an answer file.

- Lab A: Creating a Windows 2000 Domain

Prepare students for the lab in which they will install the first domain in a new tree and a new forest. Make sure that you have provided the students with a static Internet Protocol (IP) address, and a domain name. Tell the students to observe the different processes that are occurring while installing Active Directory. After students have completed the lab, ask them if they have any questions concerning the lab.

- The Active Directory Installation Process

In this topic, you will introduce the process that occurs when installing Active Directory. Ask the students what they observed while Active Directory was being installed. Tell them that now you will discuss the installation process, which includes verifying configuration parameters, determining site configuration, configuring the directory service, and identifying additional Active Directory installation operations.

- Examining the Default Structure of Active Directory

In this topic, you will introduce the default structure that is created after installing Active Directory. Open Active Directory Users and Computers, and show the students the default components in Active Directory. Discuss the purpose of these components. Emphasize the difference between a container and an OU.

- Performing Post Active Directory Installation Tasks

In this topic, you will introduce how to perform post Active Directory installation tasks. Demonstrate how to perform post Active Directory Installation tasks, such as verifying Active Directory installation, implementing Active Directory integrated zones, securing updates in Active Directory integrated zones, and changing the domain mode. Finally, present the method to implement an OU structure for defining administrative and Group Policy boundaries in Active Directory.

- Lab B: Performing Post Active Directory Installation Tasks

Prepare students for the lab in which they will verify that Active Directory is correctly installed, implement Active Directory integrated zones, change the domain mode from mixed mode to native mode, and create an OU structure based on a business scenario. After students have completed the lab, ask them if they have any questions concerning the lab.

- Troubleshooting the Installation of Active Directory

In this topic, you will introduce troubleshooting options for resolving problems that may occur when installing Active Directory. Present some of the more common problems that they may encounter when installing Active Directory, along with suggested strategies for resolving them.

- Removing Active Directory

In this topic, you will introduce how to remove Active Directory by using the Active Directory Installation wizard. Discuss the operations performed by the wizard while removing Active Directory. Tell students that some operations are common to all domain controllers, while other operations depend on the type of domain controller being removed.

- Best Practices

Present best practices for creating a Windows 2000 domain. Emphasize the reason for each best practice.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Lab Setup

The labs in this module require that the student computers be configured as DNS servers. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete Module 2, “Implementing DNS to Support Active Directory,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Dnssuf.vbs from the C:\Moc\Win2154A\Labfiles\Custom\Autodns folder.
- Install DNS on the student computers. Configure a forward and reverse lookup zone. Configure both zones to allow updates.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- All student computers become domain controllers. Each student computer is a domain controller in its own domain.
- All domains are in native mode.
- The forward and reverse lookup zones on the student computers are configured as Active Directory integrated zones.
- The following OUs are created:
 - Sales
 - Administration
 - Production
 - Servers

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn how to install Active Directory on a computer running Windows 2000 Advanced Server, and perform post Active Directory installation tasks.

- Introduction to Creating a Windows 2000 Domain
- Installing Active Directory
- The Active Directory Installation Process
- Examining the Default Structure of Active Directory
- Performing Post Active Directory Installation Tasks
- Troubleshooting the Installation of Active Directory
- Removing Active Directory
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

After installing Microsoft® Windows® 2000, you can configure a computer running Windows 2000 Advanced Server to function as a domain controller in a Windows 2000 domain. By implementing a domain structure in the Windows 2000 Active Directory® directory service, you create an administrative structure for your network. To implement a domain structure, you need to create a domain, create organizational units (OUs) within the domain, and then create user, group, and resource objects within the OUs.

When you create a domain, you must identify the DNS name of the new domain, and the location for files that are created during the installation process. Windows 2000 uses the Active Directory Installation wizard to create new domain controllers.

At the end of this module, you will be able to:

- Identify the purpose of creating a Windows 2000 domain.
- Create a Windows 2000 domain by installing Active Directory.
- Describe the process for installing Active Directory.
- Examine the default structure of Active Directory.
- Perform post Active Directory installation tasks.
- Troubleshoot common problems that may occur when installing Active Directory.
- Remove Active Directory by using the Active Directory Installation wizard.
- Apply best practices for creating a Windows 2000 domain.

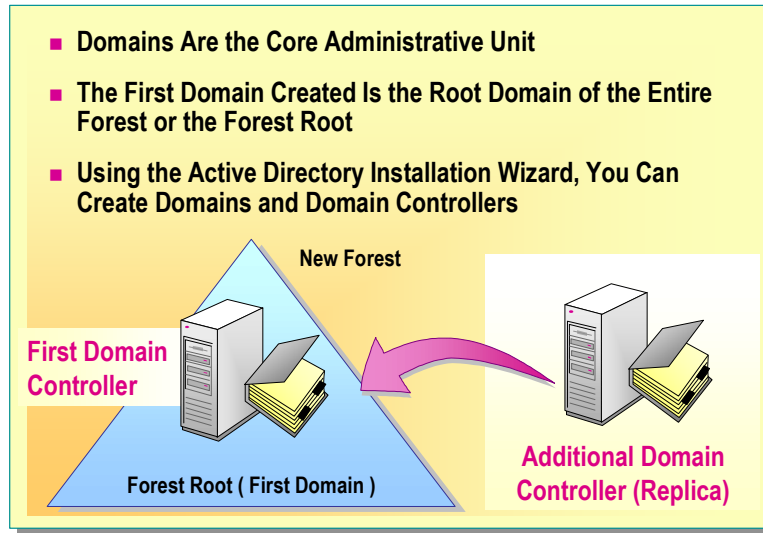
Introduction to Creating a Windows 2000 Domain

Topic Objective

To explain the purpose of creating a Windows 2000 domain.

Lead-in

A domain is the core administrative unit in a Windows 2000 network. The domain created in a new forest is the root domain.



*****ILLEGAL FOR NON-TRAINER USE*****

This module focuses only on creating a new forest, and additional domain controllers in the forest root. Tell the students that the Active Directory Installation wizard is not only used to create a new forest and additional domain controllers, but is also used to create a child domain and a new tree in an existing forest, which will be discussed later in the course.

Key Points

A domain is the core administrative unit that is used to define how information and resources are organized and stored.

The first domain created in Active Directory is the root domain of the entire forest, or the forest root.

A *domain* is the core administrative unit in a Windows 2000 network. In Windows 2000, domains are used to define how information and resources are organized and stored.

The first domain created in Active Directory is the root domain of the entire forest. This domain is also called the *forest root*. When you install Active Directory for the first time in a Windows 2000 network, you create the first domain controller in a new forest, thus establishing the root domain.

The Active Directory Installation wizard guides you through the process of installing Active Directory, to build domain controllers and create Windows 2000 domains. You can promote any stand-alone or member server to a domain controller. When you promote a server to a domain controller, you can create:

- A new forest, including the root domain (first domain in the forest) and the first domain controller.
- An additional domain controller in an existing Windows 2000 domain.

Note Using the Active Directory Installation wizard, you can also create a new child domain in an existing tree, and a new tree in an existing forest. For more information about creating a child domain and creating a new tree in an existing forest, see Module 10, "Creating and Managing Trees and Forests," in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

◆ Installing Active Directory

Topic Objective

To introduce the topics related to installing Active Directory.

Lead-in

You use DCPromo.exe to run the Active Directory Installation wizard. The Active Directory Installation wizard guides you through the process of installing Active Directory.

- **Preparing to Install Active Directory**
- **Creating the First Domain**
- **Adding a Replica Domain Controller**
- **Using an Unattended Setup Script to Install Active Directory**

*****ILLEGAL FOR NON-TRAINER USE*****

When you use the Active Directory Installation wizard to install Active Directory, you must first ensure that all of the requirements necessary for installing Active Directory are met. Then you specify the placement of a domain controller within the Active Directory structure. When installing Active Directory, you also specify detailed information, such as the domain name and the location of files that are created during the installation process.

You can also run an unattended session of the Active Directory Installation wizard by using answer files. An unattended session of the Active Directory installation is helpful during disaster recovery and when installing Active Directory in branch offices where there is no technical support available.

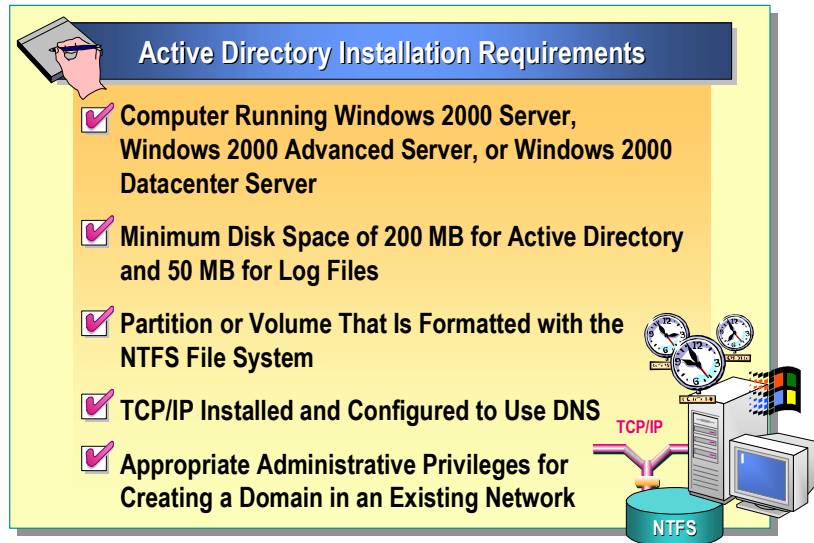
Preparing to Install Active Directory

Topic Objective

To identify the system requirements necessary for installing Active Directory.

Lead-in

Before installing Active Directory, you should ensure that the basic requirements are met on the computer where Active Directory will be installed.



*****ILLEGAL FOR NON-TRAINER USE*****

Please note that the given hard disk space requirements are the minimum requirements for installing Active Directory.

Before you install Active Directory, you must ensure that the computer that will be configured as a domain controller meets certain requirements.

The following list identifies the requirements for Active Directory installation:

- A computer running Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server.
- A minimum of 200 megabytes (MB) of disk space for the Active Directory database and an additional 50 MB for the Active Directory database transaction log files. File size requirements for the Active Directory database and log files depend on the number and type of objects in the domain. Additional disk space is also required if the domain controller is also a global catalog server.
- A partition or volume that is formatted with the NTFS file system. This is required for the SYSVOL folder.
- Transmission Control Protocol/Internet Protocol (TCP/IP) installed and configured to use Domain Name System (DNS).
- The necessary administrative privileges for creating a domain if you are creating a domain in an existing Windows 2000 network.

Note The Active Directory Installation wizard offers the option to install the DNS Server service when you install Active Directory. A DNS server supports SRV (service) resource records and the DNS dynamic update protocol.

Creating the First Domain

Topic Objective
To illustrate how to create the first domain in a new tree in a new forest.

Lead-in
The first domain that you create by using Active Directory is the root domain of the forest.

- **Start the Active Directory Installation Wizard**
- **Select the Domain Controller and Domain Type**
- **Specify the Required Information**
 - Domain, DNS, and NetBIOS names
 - Database, log, and shared system volume locations
 - Select to weaken permissions
 - Specify a password to use in Directory Services Restore Mode
- **The Active Directory Installation Wizard:**
 - Installs Active Directory
 - Converts the computer to a domain controller



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip
Because you cannot use the instructor computer to demonstrate how to create the first domain, use the demonstration called Promoting a Stand-Alone Server to a Domain Controller. To view this demonstration, open the Web page on the Student Materials compact disc, click **Multimedia Presentations**, and then click the title of the demonstration.

Explain the options on each page of the wizard.

When you install Active Directory for the first time in a network, you create the forest root domain. The Active Directory Installation wizard directs you to specify required information for the new domain controller. The information that you must provide when you install Active Directory varies according to the options that you select.

To create the root domain, perform the following steps:

1. In the **Run** box, type **dcpromo.exe** and then press ENTER.
2. In the Active Directory Installation wizard, complete the installation by using the information in the following table.

On this wizard page	Do this
Domain Controller Type	Click Domain controller for a new domain .
Create Tree or Child Domain	Click Create a new domain tree .
Create or Join Forest	Click Create a new forest of domain trees .
New Domain Name	Specify the DNS name for the new domain. If your network requires a presence on the Internet, verify that you have a registered Internet domain name, and then use this domain name as the name of the forest root.
Domain NetBIOS Name	Confirm or specify the NetBIOS name for the new domain. The NetBIOS name is used to identify the domain to client computers running earlier versions of Windows and Microsoft Windows NT®.

(continued)

On this wizard page	Do this
Database and Log Locations	Specify locations for the Active Directory database and log files. The database stores the directory for the new domain, and the log file temporarily stores changes to the database. The default location for the database and log files is <i>systemroot\Ntds</i> . For best performance, place the database and log files on separate hard disks. Installing the database and log files on separate hard disks ensures that reads and writes to the database and log files are not competing for input and output resources.
Shared System Volume	Specify the location for the shared system volume. The shared system volume is a folder structure that is hosted on all Windows 2000 domain controllers. The shared system volume stores files, such as logon, logoff, startup and shutdown scripts, and Group Policy information, which are replicated among domain controllers. You must specify a partition or volume that is formatted with the NTFS file system.
Permissions	Specify whether to assign the default permissions on user and group objects that are compatible with servers running earlier versions of Windows and Windows NT, or only with servers running Windows 2000. Assigning servers running earlier versions of Windows and Windows NT permissions adds the Everyone group to the Pre-Windows 2000 Compatible Access group. This group has read-only access to user and group object attributes that existed in Windows NT 4.0.
Directory Services Restore Mode Administrator Password	Specify a password to use when starting the computer in Directory Services Restore Mode. Windows 2000 domain controllers maintain a small version of the Windows NT 4.0 account database. The only account in this database is the Administrator account and this account is required for authentication when starting the computer in Directory Services Restore mode, as the Active Directory directory service is not started in this mode.

After you finish specifying the installation information, the Active Directory Installation wizard installs Active Directory, and converts the computer to a domain controller.

Adding a Replica Domain Controller

Topic Objective

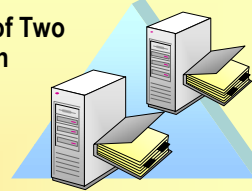
To illustrate how to add a replica domain controller to an existing domain.

Lead-in

To provide minimum fault tolerance, you should have two domain controllers in a domain.

- **Fault Tolerance Requires a Minimum of Two Domain Controllers in a Single Domain**

- **More Than One Domain Controller in a Domain Also Ensures That a Single Domain Controller Is Not Overloaded**



- **Run Dcpromo to Add a Domain Controller to an Existing Domain**

- **The Active Directory Installation Wizard:**

- Converts the computer to a domain controller
- Replicates Active Directory from an existing domain controller

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to create an additional domain controller. Explain the options on each wizard page.

To enable fault tolerance in the event that a domain controller goes offline unexpectedly, you must have a minimum of two domain controllers in a single domain. Because all domain controllers in a domain replicate their domain-specific data to one another, installing multiple domain controllers in the domain automatically enables fault tolerance for the data stored in Active Directory. If a domain controller fails, the remaining domain controllers will provide authentication services and access to objects in Active Directory, allowing the domain to operate as usual.

When a new domain controller is added to a domain, replication occurs to ensure consistency in Active Directory. In addition, having more than one domain controller in a domain helps to ensure that a single domain controller is not overloaded when servicing logon requests, global catalog queries, and other services provided by domain controllers.

To add a domain controller to an existing domain, perform the following steps:

1. In the **Run** box, type **dcpromo.exe** and then press ENTER.
2. In the Active Directory Installation wizard, complete the installation by using the information in the following table.

On this wizard page	Do this
Domain Controller Type	Click Additional domain controller for an existing domain .
Network Credentials	Specify the user name, password, and domain name of a user account that has the privileges to create domain controllers in Active Directory.
Additional Domain Controller	Specify the DNS name of the existing domain for which this computer will become an additional domain controller.

The remaining options in the Active Directory Installation wizard are identical to the options used for creating the first domain. After you finish specifying the installation information, the Active Directory Installation wizard converts the computer to a domain controller, and replicates Active Directory from an existing domain controller.

Using an Unattended Setup Script to Install Active Directory

Topic Objective

To identify how to install Active Directory by using an unattended Setup script.

Lead-in

You have the option of installing Active Directory with an unattended Setup script.

An Answer File:

- Contains all of the parameters needed for an unattended session of installing Active Directory
- Contains only the [DCInstall] section of the unattended setup parameters file
- Can be run after Windows 2000 Server setup has been completed and a user has logged on to the computer
`dcpromo/answer:<answer file>`

Notepad

[Unattended]

[DCInstall]

Answer File

*****ILLEGAL FOR NON-TRAINER USE*****

Show the students an example answer file.

Explain the entries in the [DCInstall] section and the required values for installing the first domain.

Tell the students that the command to run an answer file can be included in the GuiRunOnce section of an answer file used to automate the installation of Windows 2000 Advanced Server. By including the command in the answer file, you can fully automate the installation of a domain controller.

Key Points

Anyone who does not know how to install Active Directory can use the answer file.

The user using the answer file needs to have the required administrative privileges to successfully complete the installation.

You can also install Active Directory by using an *answer file*. Administrators use answer files to specify all of the parameters for the Active Directory installation. These parameters include the domain type and the configuration of the domain being created. The answer file can then be used by anyone who does not know how to install Active Directory. The user using the answer file still needs the required administrative privileges to successfully complete the installation.

An answer file for the Active Directory Installation wizard contains only one section, [DCInstall]. Each operation in the wizard requires values for specific parameters in the [DCInstall] section of the unattend file. Default values are used if a value for a parameter is not specified. The following table describes the entries in the [DCInstall] section that enable you to automatically install Active Directory on the first domain controller in a new forest.

[DCInstall] Keys	Value	Description
RebootOnSuccess	Yes	Specifies whether the computer should be rebooted upon successful completion.
DatabasePath	C:\Winnt\Ntds	Specifies the fully qualified, non-universal naming convention (UNC) path to a folder on a fixed disk of the local computer that contains the domain database. The folder must be empty. Creates the folder if it does not exist.

(continued)

[DCInstall] Keys	Value	Description
LogPath	C:\Winnt\Ntds	Specifies the fully qualified, non-UNC path to a folder on a fixed disk of the local computer that contains the domain log files. The folder must be empty. Creates the folder if it does not exist.
SYSVOLPath	C:\Winnt\Sysvol	Specifies the fully qualified, non-UNC path to a folder on a fixed disk of the local computer. The folder must be empty. Creates the folder if it does not exist. The SYSVOL folder must be installed on an NTFS partition.
SiteName	Default-First-Site-Name	Specifies the name of an existing site to place the new domain controller. If not specified, a suitable site is selected. This option applies only when creating a new domain tree in a new forest of domains.
ReplicaOrNewDomain	Domain	Specifies that a new domain controller should be installed as the first domain controller in a new directory service domain. If you set the value to Domain, you must also specify a valid value in the TreeOrChild parameter.
TreeOrChild	Tree	Specifies that the new domain is the root of a new tree. If you set the value to Tree, you must also specify a valid value in the CreateOrJoin parameter.
CreateOrJoin	Create	Specifies the creation of a new forest of domains.
DomainNetbiosName	contoso	Assigns a NetBIOS name to the new domain. This is a required value, and the name specified must be unique in the domain.
NewDomainDNSName	contoso.msft	Specifies the required name when a new forest of domains is being installed.
DNSOnNetwork	No	Specifies that a new forest of domains is being installed and no DNS client is configured on the computer. Setting the value to No skips the DNS client configuration and creates the DNS auto-configuration for the new domain.
AutoConfigDNS	Yes	Specifies that the wizard should configure DNS for the new domain if it has detected that dynamic DNS updates are not available.

The answer file can be run after Windows 2000 Advanced Server Setup has been completed and a user has logged on to the computer. To start the unattended installation of Active Directory, open the command prompt window and type the following:

Dcpromo.exe /answer:*answer file*

Where *answer file* is name of the answer file.

Note For more information about unattended installations, see *unattend.doc* in the Deploy.cab file located in the \Support\Tools on the Windows 2000 Advanced Server compact disc.

Lab A: Creating a Windows 2000 Domain

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will install Active Directory. You will create a new domain in a new forest, and use various tools and utilities to verify the installation.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to install Active Directory by using the Active Directory Installation wizard.

Prerequisites

Before working on this lab, you must have:

- An understanding of the logical components of Active Directory, including domains, trees, and forests.
- An understanding of the purpose and function of domain controllers.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a standalone server.
- Drive C formatted with NTFS.
- A static IP address.
- A DNS server configured for your domain.
- A domain name. Your domain name is *domain.nwtraders.msft*, where *domain* is your computer name with dom appended. For example, if your computer name is Vancouver, then *domain* would be vancouverdom and your full domain name would be vancouverdom.nwtraders.msft.
- A forward lookup zone that matches your domain name. The forward lookup zone should have been created in Lab A of Module 2, “Implementing DNS to Support Active Directory,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Estimated time to complete this lab: 30 minutes

Exercise 1

Installing Active Directory

Scenario

Northwind Traders has decided to install Windows 2000 and use Active Directory to use all of the features and benefits that Active Directory provides. You have been assigned the task of creating the first domain on the network. You have already created a forward lookup zone in DNS. The name of the forward lookup zone is the same name that you will be using for the Active Directory domain name.

Goal

In this exercise, you will create a Windows 2000 domain by installing Active Directory.

Tasks	Detailed Steps
1. Start the Active Directory Installation wizard to create: - A new domain controller for a new domain. - A new domain tree. - A new forest of domain trees.	a. Log on as Administrator with a password of password. b. Click Start, and then click Run. c. In the Run box, type dcpromo and then click OK. d. On the Welcome to the Active Directory Installation Wizard page, click Next. e. On the Domain Controller Type page, ensure that Domain controller for a new domain is selected, and then click Next. f. On the Create Tree or Child Domain page, ensure that Create a new domain tree is selected, and then click Next. g. On the Create or Join Forest page, ensure that Create a new forest of domain trees is selected, and then click Next.
2. Complete the Active Directory installation process, providing the following information: - Full DNS name of domain.nwtraders.msft (where <i>domain</i> is your assigned domain name). - NetBIOS domain name of DOMAIN (where <i>DOMAIN</i> is your assigned domain name). - Default locations for the database, log files, and shared system volume.	a. On the New Domain Name page, in the Full DNS name for new domain text box, type domain.nwtraders.msft (where <i>domain</i> is your assigned domain name), and then click Next. b. On the NetBIOS Domain Name page, ensure that DOMAIN (where <i>DOMAIN</i> is your assigned domain name) appears, and then click Next. c. On the Database and Log Locations page, accept the default locations by clicking Next. d. On the Shared System Volume page, accept the default location by clicking Next. e. On the Permissions page, select Permissions compatible only with Windows 2000 servers, and then click Next. f. On the Directory Services Restore Mode Administrator Password page, in the Password and Confirm password boxes, type password and then click Next.

Tasks	Detailed Steps
2. <i>(continued)</i> • Permissions compatible with only servers running Windows 2000. • A password of password for the Directory Services Restore Mode Administrator password.	g. On the Summary page, review the options you selected, and then click Next.  <i>The Active Directory installation process begins.</i> h. When the Completing the Active Directory Installation Wizard page appears, click Finish, and then restart your computer.

◆ The Active Directory Installation Process

Topic Objective

To introduce the topics related to the Active Directory installation process.

Lead-in

During the Active Directory installation, the Active Directory Installation wizard confirms several configuration and security parameters.

- Configuration Parameters
- Site Configuration
- Directory Service Configuration
- Services and Security Configuration
- Additional Active Directory Installation Operations

*****ILLEGAL FOR NON-TRAINER USE*****

When installing Active Directory, the Active Directory Installation wizard confirms several configuration and security parameters. Active Directory validates the parameters you specify during the installation process. The type of validation performed depends on whether the domain controller being installed is the first in the forest, or the first domain in the replica. The purpose of this verification is to validate the parameters that you specify during the Active Directory installation process.

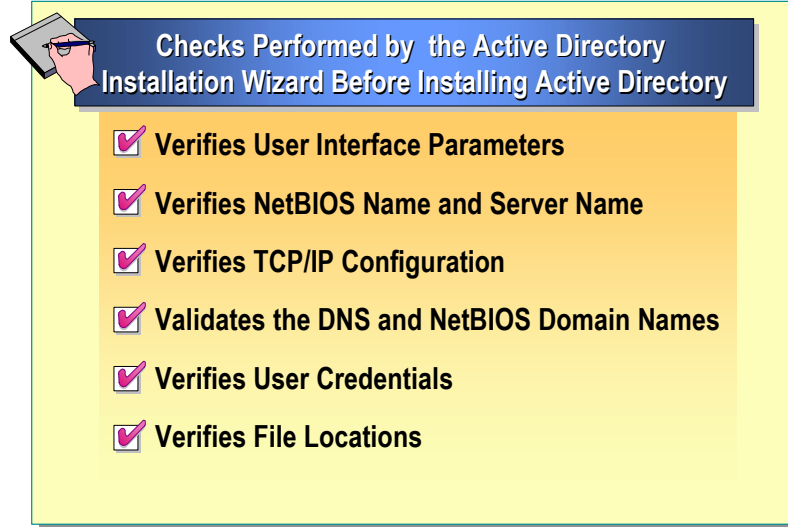
Configuration Parameters

Topic Objective

To identify how the installation process verifies configuration parameters.

Lead-in

The Active Directory Installation wizard performs checks for configuration parameters to ensure the integrity of the installation process.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

User interface verification ensures that the user is logged on as a member of the local Administrators group.

Naming verification ensures that the NetBIOS name of the new domain is unique in the forest.

TCP/IP configuration verification ensures that the DNS server can be located.

DNS name validation ensures that the parent domain exists, and that the domain name is unique in the forest.

User credentials verification ensures that the user installing Active Directory has the appropriate permissions.

File locations verification is essential for replication between domain controllers.

The Active Directory Installation wizard performs several verifications before the actual installation of Active Directory. These verifications are required to ensure the integrity of the installation process.

User Interface Verification

Before the user interface is actually displayed, the Active Directory Installation wizard verifies the following:

- The user currently logged on is a member of the local Administrators group.
- The computer is running Windows 2000 Server or Advanced Server.
- A previous installation or removal of Active Directory has not taken place without restarting the computer.
- An installation or removal of Active Directory is not currently in progress.

If any of these four verifications fail, an error message is displayed and you exit the wizard. After these verifications are completed successfully, the Active Directory Installation wizard performs the remaining verifications.

Naming Verification

Each domain controller has a server object in the Site container. When adding a new domain controller to an existing domain, a verification is made to ensure that the server name does not exist in the Servers container in any site or in the Servers container in the site to which the domain controller is being added. If the server name does exist, the wizard deletes the existing object and assumes that a reinstallation is being performed.

TCP/IP Configuration Verification

If TCP/IP is not installed, or if it is installed and configured to use the Dynamic Host Configuration Protocol (DHCP) service and a DHCP-assigned address is not available, the installation is interrupted and you are prompted to correct the problem.

The wizard also verifies the server's DNS resolver configuration. Active Directory uses DNS to locate servers and services, so a properly configured DNS resolver is critical to the successful installation of Active Directory.

- When installing the first domain controller in a new domain, the Active Directory Installation wizard attempts to locate a DNS server that supports the dynamic update protocol and a DNS server that is authoritative for the DNS domain. If either of these two verifications fail, the user is prompted to either have the wizard install and configure DNS locally during the Active Directory installation process or to do it manually after Active Directory is installed.
- When adding a domain controller to an existing domain, the existence of an appropriate DNS server is assumed and there is no attempt to verify the DNS server.

DNS and NetBIOS Domain Names Validation

When creating a domain, you must provide a DNS name for the domain. The wizard verifies that the new domain name provided is unique in the forest. If the name is not unique, you are prompted to correct the information.

You must also provide a NetBIOS domain name. The NetBIOS domain name is generated from the DNS domain name. The NetBIOS name is formed by taking up to the first 15 characters of the leftmost label in the DNS domain name. The wizard verifies that the NetBIOS domain name is unique, and if it is not, the user is prompted to change the name.

User Credentials Verification

Because creating a new domain controller is a security-sensitive task, the wizard verifies that the user attempting to install Active Directory has the correct security permissions. If the credentials of the currently logged on user do not match these requirements, the user is prompted for an account with sufficient privileges. The following list describes the types of installations that can be performed, and the security permissions required for each installation:

- If a new forest is being created, no verification is performed, and no specific credentials are required.
- If a replica domain controller is being added to an existing domain, the supplied credentials must be sufficient to join the computer to the existing domain. Members of the Domain Admins group in the domain that you are installing the domain controller and members of the Enterprise Admins group are by default assigned the necessary permissions to create new domain controllers.

Note The Active Directory Installation wizard requests credentials in the form of a user name, password, and domain. Therefore, a user principal name entered as *userName@domainName* is not accepted.

File Locations Verification

The locations for the Active Directory database file, log files, and the SYSVOL folder are specified during the Active Directory installation. The contents of SYSVOL are replicated to all domain controllers in the domain. Creation of SYSVOL requires a volume formatted with NTFS. If an NTFS-formatted volume cannot be found, or if there is not sufficient free disk space, the installation cannot proceed.

Note For more information about Servers container in a site, see Module 11, “Managing Active Directory Replication,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Site Configuration

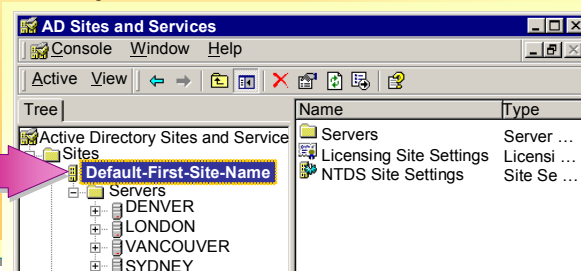
Topic Objective

To describe the installation process that determines the site on which to add the new domain controller.

Lead-in

After verifying the configuration parameters, the Active Directory Installation wizard must determine the site on which to add the new domain controller.

- The Domain Controller Is Added to the Site That Is Associated with Its Subnet
- The Server Is Placed in the Default-First-Site-Name Site if No Subnet Object Is Found
- The Active Directory Installation Wizard Creates a Server Object



*****ILLEGAL FOR NON-TRAINER USE*****

Emphasize that the Default-First-Site-Name site is created when you create the first domain in a new forest.

Key Points

If no subnet objects, the server is placed in the Default-First-Site-Name site.

The Active Directory Installation wizard creates a server object for the domain controller in the appropriate site, and the server object contains a reference to the computer object in the Domain Controllers OU.

The Active Directory Installation wizard queries Active Directory for site data. If the Internet Protocol (IP) address of the server being promoted to a domain controller is within the range for a given subnet defined in the Active Directory, the wizard configures the membership of the domain controller in the site associated with that subnet.

If no subnet objects are defined or if the IP address of the server is not within the range of the subnet objects present in Active Directory, the server is placed in the *Default-First-Site-Name* site. Default-First-Site-Name is the first site that is set up automatically when you create the first domain controller in a forest.

The Active Directory Installation wizard creates a *server object* for the domain controller in the appropriate site. The server object contains information required for replication. The server object contains a reference to the computer object in the Domain Controllers OU that represents the domain controller being created.

Note If a server object for this domain controller already exists, it is deleted and then recreated, because the wizard assumes that you are performing a reinstallation of Active Directory. For more information about subnet objects and server objects, see Module 11, "Managing Active Directory Replication," in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Directory Service Configuration

Topic Objective

To identify how the Active Directory Installation wizard completes the configuration of the directory service.

Lead-in

After a verification of all of the required components is finished, the wizard provides confirmation of the settings specified by the user.



Directory Service Configuration Operations

- ✓ **Operations for All Types of Installations**
 - Creates the required registry entries
 - Sets up the performance counters for Active Directory
 - Configures the server to automatically enroll for an X.509 domain controller certificate
 - Starts the Kerberos V5 authentication service
 - Sets the Local Security Authority (LSA) policy
 - Installs shortcuts to administration tools in Active Directory
- ✓ **Directory Partitions Configuration**
 - Creates the schema directory partition
 - Creates the configuration directory partition
 - Creates the domain directory partition

*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Some operations, such as creating registry entries, and setting up the performance counters and LSA policy, are common to all types of domain controller installations.

Other operations, such as creating the directory partitions and the default domain security principals, depend on the type of domain controller installation.

After the Active Directory Installation wizard completes all of the required verifications, a confirmation page is displayed, which lists the choices that you made in the wizard. When you accept the settings, the wizard begins the actual Active Directory installation process.

Common Active Directory Operations for All Installations

The Active Directory Installation wizard performs the following operations for all types of domain controller installations:

- Creates the required registry entries.
- Sets up the performance counters for Active Directory.
- Configures the server to automatically enroll for an X.509 domain controller certificate from the first Certificate Authority that will process the request. This certificate is required for Simple Mail Transfer Protocol (SMTP)-based replication.
- Starts the Kerberos version 5 authentication protocol.
- Sets the Local Security Authority (LSA) policy to indicate that this server is a domain controller.
- Installs shortcuts to the administration tools for Active Directory.

Directory Partitions Configuration

The directory database template file, Ntds.dit, is copied from its location in the *systemroot\System32* folder to the location that you specify when running the Active Directory Installation wizard. The wizard configures the local server to host the directory service. This process includes creating the directory partitions and the default domain security principals, such as the Domain Admins group.

In Active Directory, a directory partition is a portion of the directory namespace. Each directory partition contains a hierarchy, or subtree of directory objects in the directory tree. Copies, or replicas, of the same directory partition can be stored on many domain controllers, and the copies are updated through directory replication.

The following directory partitions are created on the first domain controller in a forest and are updated through replication on every subsequent domain controller that is created in the forest:

- The schema directory partition. Contains the Schema container, which stores class and attribute definitions for all existing and possible Active Directory objects. The schema directory partition is replicated to all domain controllers in a forest.
- The configuration directory partition. Contains the Configuration container, which stores configuration objects for the entire forest. Configuration objects store information about sites, services, and directory partitions. The configuration directory partition is replicated to all domain controllers in a forest.
- The domain directory partition. Contains a domain container, such as the *contoso.msft* container, which stores users, computers, groups, and other objects for a specific Windows 2000 domain. The domain directory partition is replicated to all domain controllers within a single domain.

Services and Security Configuration

Topic Objective

To identify the services that are configured to start automatically after Active Directory installation, and the type of security set on the file system, Active Directory objects, and default Group Policy objects during Active Directory installation.

Lead-in

The Active Directory Installation wizard configures some services to start automatically. You can use Group Policy to enable other services, such as security.



Configuring Services and Security

- ☒ **Setting Services to Start Automatically**
 - Remote Procedure Call (RPC) Locator
 - Net Logon
 - KDC
 - Intersite Messaging
 - Distributed Link Tracking Server
 - Windows Time
- ☒ **Setting Security**
 - Sets security for the directory service and the file replication folders
 - Configures default DACLs on file and objects in Active Directory
 - Configures default Group Policy by using the security templates

*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

DACLs are configured on Active Directory objects, SYSVOL file system objects, and a few registry keys.

For the first domain controller, default Group Policy settings are configured by using the security templates located in the `systemroot\inf` folder.

During the Active Directory installation, services are configured to start automatically, and security is enabled on the directory service.

Setting Services to Start Automatically

The following services are configured to start automatically:

- *Remote Procedure Call (RPC) Locator*. This service allows distributed applications to use the RPC name service. The RPC Locator service manages the RPC name service database.
- *Net Logon*. This service runs the Domain Controller Locator service. The Net Logon service is also responsible for creating a secure channel between client computers and domain controllers during logon, and for registering SRV resource records in DNS.
- *KDC (Key Distribution Center)*. This service maintains a database with account information for all security principals in its *realm*, which is the Kerberos V5 authentication protocol equivalent of a Windows 2000 domain.
- *Intersite Messaging (ISM)*. This service is used for mail-based replication between sites.
- *Distributed Link Tracking Server*. This service helps resolve shortcuts and OLE links to NTFS-resident files that have had their names changed, paths changed, or both.
- *Windows Time*. This service synchronizes clocks between client computers and servers that run Windows 2000.

Setting Security

During the installation of Active Directory, security is enabled on the directory service and the file replication folders to control the access to Active Directory objects.

Default DACLs on Active Directory Objects

Default *discretionary access control lists (DACLs)* are configured on Active Directory objects. The DACL is a list of entries that identify who is allowed or denied access, and the level of access being allowed or denied for an object. DACLs are also configured for the following file system objects and the following registry keys:

- SYSVOL
- Program Files
- *Windir*
- HKEY_LOCAL_MACHINE\SOFTWARE
- HKEY_LOCAL_MACHINE\SYSTEM
- HKEY_USERS\DEFAULT

Default Group Policy Settings for Domain Controllers

For the first domain controller in a domain, default Group Policy is configured by using the security templates DCFirst.inf, DefltDC.inf, and DCUp.inf located in the *systemroot\inf* folder. When additional domain controllers are added to a domain, Group Policy is replicated from the first domain controller in a domain to all additional domain controllers.

Additional Active Directory Installation Operations

Topic Objective

To identify additional operations that are performed during the Active Directory installation process.

Lead-in

Regardless of the type of domain being created, the Active Directory Installation wizard also performs some additional operations during the Active Directory installation.

Additional Operations

- Sets the Computer DNS Root Domain Name
- Determines Whether the Server Computer Is a Member of the Domain
- Creates a Computer Account in the Domain Controllers OU
- Applies the User-Provided Password for the Administrator Account
- Creates a Cross-Reference Object in the Configuration Container
- Adds Shortcuts
- Creates the SYSVOL Folder
- Creates Schema and Configuration Containers
- Assigns the Specific Roles to the Domain Controller

*****ILLEGAL FOR NON-TRAINER USE*****

Regardless of the type of domain being created, the Active Directory Installation wizard performs the following additional operations during the Active Directory installation.

- Sets the computer DNS root domain name to the name of the new domain.
- Determines whether the server computer is already a member of the domain. If the computer is a member of a domain, the wizard removes the computer account for the member server from the domain and recreates the computer account in the Domain Controllers OU. If the computer is being promoted to a domain controller in a different domain, the user is notified that the computer account for the member server must be removed from the original domain.
- Creates a computer account in the Domain Controllers OU in the new domain. The computer account is also added to the Domain Controllers global group in the Users container. This computer account allows the computer to authenticate to other domain controllers when performing operations such as replication.
- Applies the user-provided password for the administrator account that is used to start the domain controller in Directory Services Restore Mode.
- Creates a cross-reference object in the Configuration container. This object is used by LDAP to locate resources in other domains.
- Adds two new shortcuts to Group Policy security settings. These shortcuts are Domain Security Policy and Domain Controller Security Policy.

- Creates the SYSVOL folder, which contains:
 - The SYSVOL shared folder. This shared folder contains Group Policy information.
 - The Net Logon shared folder. This shared folder is used to contain logon scripts for non-Windows 2000–based computers.
- Performs the following operations while creating the forest root domain:
 - The Schema and Configuration containers are created.
 - The Active Directory Installation wizard assigns the primary domain controller (PDC) emulator, relative identifier (RID) operations master, domain naming master, schema master, and infrastructure master roles to the domain controller.

Note For more information about the PDC emulator, RID operations master, domain naming master, schema master, and infrastructure master roles, see Module 12, “Managing Operations Masters,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

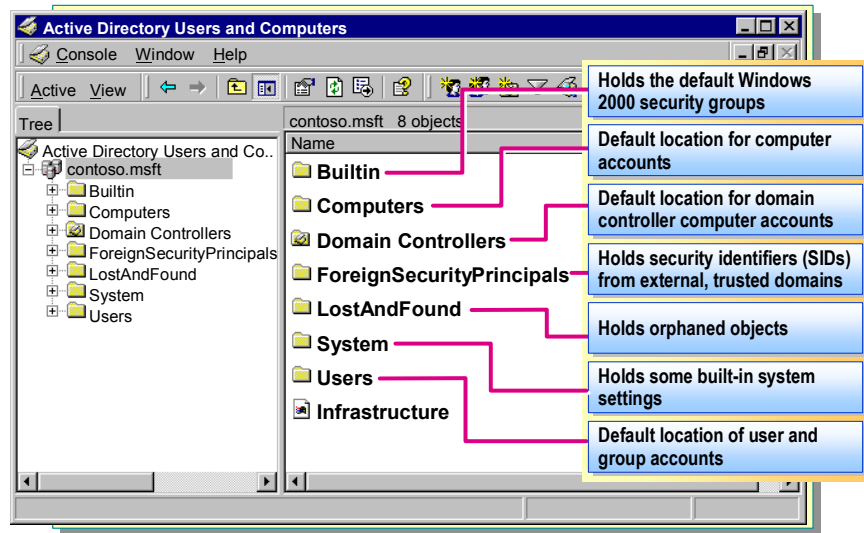
Examining the Default Structure of Active Directory

Topic Objective

To examine the logical structure that is created after installing Active Directory.

Lead-in

You can verify the installation of Active Directory by looking for specific items in the default structure of Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

Tell students that they can apply Group Policy to an OU but not to a container.

Delivery Tip

Show students the Active Directory Users and Computers interface. Open each default object to show the students the contents of each object.

First show students the default objects without displaying Advanced Features. Then, on the **View** menu, click **Advanced Features** and show students the additional default objects.

During the installation of Active Directory on the first domain controller in a new domain, several default objects are created. These objects include containers, users, computers, groups, and organizational units. You can view and manage these default objects by using the Active Directory Users and Computers administrative tool.

The following list describes the purpose of some of these default objects:

- *Builtin (container)*. This object is used to hold the default built-in security groups.
- *Computers (container)*. This object is the default location for computer accounts.
- *Domain Controllers (organizational unit)*. This object is the default location for domain controller computer accounts.
- *ForeignSecurityPrincipals (container)*. This object is used to hold security identifiers (SIDs) from external, trusted domains.
- *Users (container)*. This object is the default location of user and group accounts.

You can view additional objects in Active Directory Users and Computers; to do so, on the **View** menu, click **Advanced Features**.

The following list describes the purpose of the additional objects:

- *LostAndFound*. This object holds orphaned objects. This object holds objects that are left behind, or orphaned, when their parent containers are deleted. For an object to exist in LostandFound, there must be two Domain Controllers in the domain: one where the object is added; and one where the OU or container is deleted.
- *System*. This object holds specific built-in system settings.

Note You can apply Group Policy on an OU, but you cannot apply Group Policy on a container.

◆ Performing Post Active Directory Installation Tasks

Topic Objective

To introduce the topics related to performing post Active Directory installation tasks.

Lead-in

After you install Active Directory, it is important to verify that the necessary files and SRV records are working properly.

- **Verifying the Active Directory Installation**
- **Implementing Active Directory Integrated Zones**
- **Securing Updates for Active Directory Integrated Zones**
- **Changing the Domain Mode**
- **Implementing an Organizational Unit Structure**

*****ILLEGAL FOR NON-TRAINER USE*****

After you install Active Directory, it is important to verify that the necessary directory database files, SYSVOL files, and DNS SRV resource records have been created so that Active Directory works properly.

After you install Active Directory, you should also configure Active Directory integrated DNS zones so that DNS can use the functionality of Active Directory, such as replication, zone transfer, and secure dynamic updates.

If all of the domain controllers in a Windows 2000 network are running Windows 2000, you should change the domain mode from mixed mode to native mode. Only in the native mode can you add new groups within existing groups and add universal security groups.

After creating a domain, you should implement an OU structure to enhance administrative control and apply Group Policy. You can create an OU within a domain or another OU. After you create an OU, you can add objects to it.

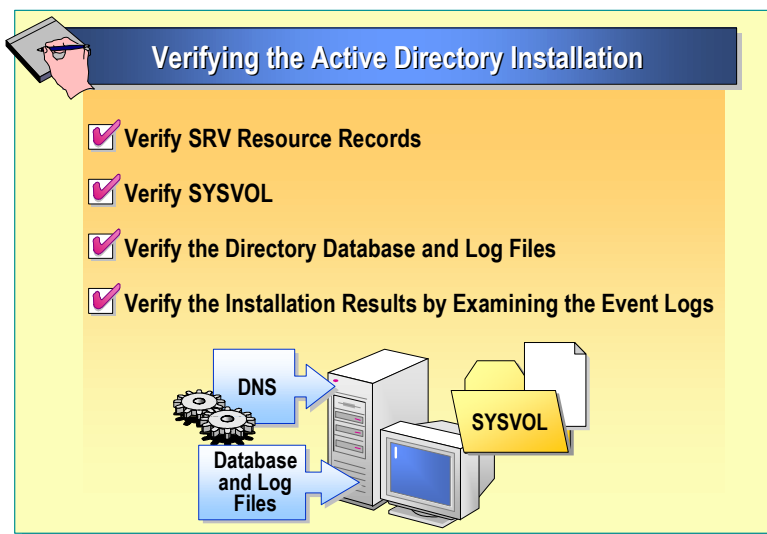
Verifying the Active Directory Installation

Topic Objective

To describe how to verify the Active Directory installation by examining the SRV records in DNS, and how to use Event Viewer to examine log files.

Lead-in

After the wizard completes the installation of Active Directory, you can verify the success of the installation by examining the DNS database, SYSVOL, directory database, and log files.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Open DNS and show students some of the common SRV records registered by domain controllers, and the contents of the SYSVOL folder, and the Ntfs folder.

Key Points

The new domain controller registers its SRV resource records in the DNS database when it restarts.

To verify SYSVOL, first verify that the folder structure was created, and then verify that the necessary shared folders were created.

To verify the database and log files, ensure that Ntfs.dit, Edb.*, and Res*.log files were created.

Always examine the Event logs for any errors that may have been encountered during the installation process.

After the wizard completes the installation of Active Directory, you can verify the success of the installation by:

- Examining the DNS database to ensure that the required SRV resource records were created.
- Ensuring that SYSVOL has been properly created and shared.
- Verifying that the Active Directory database and log files were created.
- Examining the Event logs for any errors generated during the installation.

Verifying SRV Resource Records

After Active Directory is installed, the new domain controller registers its SRV resource records in the DNS database when it restarts.

You can verify the creation of these records either by using the DNS snap-in on the **Administrative Tools** menu or by using the **nslookup** command.

Using the DNS Snap-in

To verify that the SRV resource records were properly registered by using the DNS snap-in, perform the following steps:

1. Open DNS from the **Administrative Tools** menu.
2. Double-click *Server* (where *Server* is the name of your DNS server), double-click **Forward Lookup Zones**, and then double-click *domain* (where *domain* is the domain name).

If the SRV resource records were registered, the following folders will exist in the *domain* folder:

- `_msdcs`
- `_sites`
- `_tcp`
- `_udp`

Using Nslookup

To verify that SRV resource records were properly registered by using the **nslookup** command, perform the following steps:

1. Open a command prompt window.
2. At the command prompt, type **nslookup** and then press ENTER.
3. Type **ls -t SRV domain** (where *domain* is the domain name), and then press ENTER.

If the SRV resource records were properly created, they will be listed. To save the results of this list to a file, type **ls -t SRV domain > filename** (where *filename* is any name you give to the file).

Note If you do not have a reverse lookup zone configured, time-outs will be reported when you first run **nslookup**. This reporting happens because **nslookup** generates a reverse lookup to determine the host name of the DNS server based on its IP address.

Verifying SYSVOL

There are two steps involved in verifying SYSVOL. First, verify that the folder structure was created, and second, verify that the necessary shared folders were created. If the SYSVOL folder is not correctly created, data that is stored in the SYSVOL folder, such as Group Policy, and scripts, will not be replicated between domain controllers.

To verify that the folder structure was created, perform the following step:

- Click **Start**, click **Run**, type `%systemroot%\sysvol` in the **Open** box, and then click **OK**.

Windows Explorer opens and displays the contents of the SYSVOL folder, which should include the following subfolders:

- Domain
- Staging
- Staging areas
- Sysvol

To verify that the necessary shares have been created, perform the following steps:

1. Open a command prompt window.
2. At the command prompt, type **net share** and then press ENTER.

In the list of shared folders on this computer, you should see the shared folders listed in the following table.

Share name	Resource	Remark
NETLOGON	<i>systemroot</i> \SYSVOL\sysvol\domain\SCRIPTS	Logon server share
SYSVOL	<i>systemroot</i> \SYSVOL\sysvol	Logon server share

Verifying the Directory Database and Log Files

To verify that the directory database and log files were properly created, perform the following step:

- Click **Start**, click **Run**, type **%systemroot%\ntds** in the **Open** box, and then click **OK**.

Windows Explorer opens and displays the contents of the Ntds folder, which should include the following files:

- Ntds.dit. This is the directory database file.
- Edb.*. These are the transaction logs and the checkpoint files.
- Res*.log. These are the reserved log files.

Note If you changed the location of the directory database and log files during the installation, replace **%systemroot%** with the correct location.

Verifying the Installation Results by Examining the Event Logs

After installing Active Directory, you should examine the Event logs for any errors that may have been encountered during the installation process. The following logs contain any error messages generated during the installation:

- System Log
- Directory Service
- DNS Server
- File Replication service

Implementing Active Directory Integrated Zones

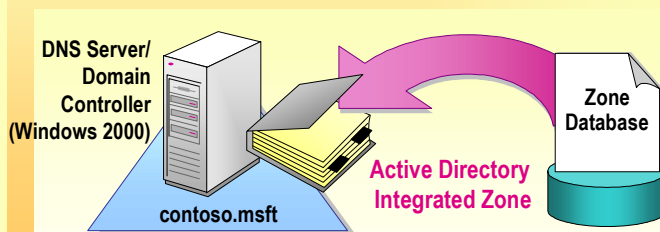
Topic Objective

To illustrate how to implement Active Directory integrated zones.

Lead-in

When you integrate a DNS zone with Active Directory, DNS can use Active Directory to store and replicate DNS zone databases.

- Use DNS to Integrate a DNS Zone with Active Directory
- Implement a Forward Lookup Zone
- Implement a Reverse Lookup Zone



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to use DNS in MMC to implement Active Directory–integrated forward and reverse lookup zones.

Key Point

Implement

Active Directory–integrated forward and reverse lookup zones to enable client computers to perform both forward and reverse lookups.

After installing Active Directory, you can integrate a DNS zone with Active Directory, so that DNS can use Active Directory to store and replicate DNS zone databases. You implement Active Directory–integrated forward and reverse lookup zones to enable client computers to perform both forward and reverse lookups.

To implement the Active Directory–integrated forward or reverse lookup zones, perform the following steps:

1. Open DNS from the **Administrative Tools** menu, and then double-click *Server* (where *Server* is your DNS server).
2. Depending on whether you are implementing a forward or a reverse lookup zone, perform one of the following steps:
 - To implement the Active Directory–integrated forward lookup zone, double-click **Forward Lookup Zones**, click *domain* (where *domain* is your domain name), right-click *domain*, and then click **Properties**.
 - To implement the Active Directory–integrated reverse lookup zone, double-click **Reverse Lookup Zones**, click *AAA.BBB.CCC.x Subnet* (where *AAA.BBB.CCC.x* is your reverse lookup zone), right-click *AAA.BBB.CCC.x Subnet*, and then click **Properties**.
3. On the **General** tab, click **Change**.
4. In the **Change Zone Type** dialog box, click **Active Directory-integrated**, and then click **OK**.
5. In the **DNS** dialog box, click **OK**, and then click **OK** again to close the *domain* **Properties** dialog box or the *AAA.BBB.CCC.x Subnet* **Properties** dialog box.

Note The Active Directory–integrated option is not available in the **Change Zone Type** dialog box until you install Active Directory.

Securing Updates for Active Directory Integrated Zones

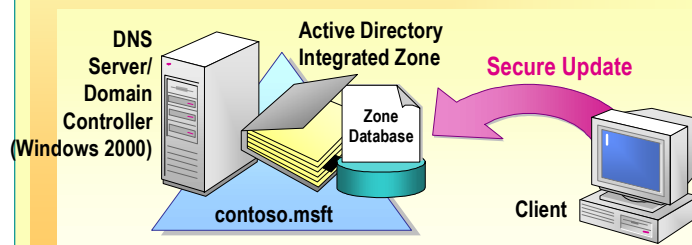
Topic Objective

To illustrate how to secure updates for forward and reverse lookup zones.

Lead-in

You can also configure zones for dynamic updates so that resource records can be updated without administrator intervention.

- Use DNS to Secure Updates for Active Directory Integrated Zones
- Secure the Active Directory Integrated Zones to Enable You to Control Access to Zones and Resource Records



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to use DNS in MMC to allow only secure updates for forward and reverse lookup zones.

Key Points

Only Active Directory integrated zones can be configured for secure dynamic updates.

By setting the properties of an Active Directory integrated DNS zone to allow only secure updates, you can control access to zones and resource records.

After implementing Active Directory integrated zones, you can also configure zones for secure dynamic updates. DNS supports the DNS dynamic update protocol. The DNS dynamic update protocol allows Windows 2000-based computers to update DNS servers automatically, so that resource records can be updated without administrator intervention.

When you set the properties of an Active Directory integrated DNS zone to allow only secure updates, you can control access to zones and resource records by editing the DACL for that zone or resource record.

To allow only secure updates for a forward or a reverse lookup zone, perform the following steps:

1. Open DNS from the **Administrative Tools** menu, and then double-click *Server* (where *Server* is your DNS server).
2. Depending on whether you are securing updates for a forward or a reverse lookup zone, perform one of the following steps:
 - To allow only secure updates for a forward lookup zone, double-click **Forward Lookup Zones**, click *domain* (where *domain* is your domain name), right-click *domain*, and then click **Properties**.
 - To allow only secure updates for a reverse lookup zone, click *AAA.BBB.CCC.x Subnet* (where *AAA.BBB.CCC.x* is your reverse lookup zone), right-click *AAA.BBB.CCC.x Subnet*, and then click **Properties**.
3. On the **General** tab, in the **Allow dynamic updates** list, click **Only secure updates**, and then click **OK** to close the *domain Properties* dialog box or the *AAA.BBB.CCC.x Subnet Properties* dialog box.

Changing the Domain Mode

Topic Objective

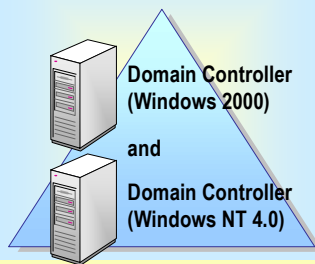
To describe domain modes, and how to changing the domain mode.

Lead-in

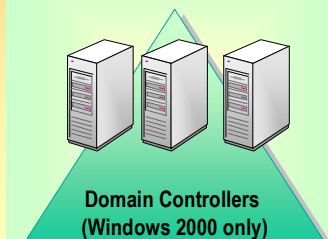
After you install Active Directory and establish a domain, the domain and Active Directory run in mixed mode. However, you need to change the domain mode to the native mode to use some functions in Active Directory, such as group nesting and security-type universal groups.

- Active Directory Installs in Mixed Mode to Provide Support for Existing Domain Controllers
- Group Nesting and Universal Security Groups Requires a Domain to Be in Native Mode

● Mixed Mode



● Native Mode



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to change a domain from mixed mode to native mode.

Key Points

The operating system on the domain controllers determines the mode that your domain can use.

Some functions in Active Directory, such as group nesting and security-type universal groups, require that the domain be in native mode.

You can change only from mixed mode to native mode. You cannot change from native mode to mixed mode.

After you install Active Directory and establish a domain, the domain and Active Directory run in *mixed mode*, which is the default domain mode. A mixed mode domain supports domain controllers that are running either Windows 2000 or Microsoft Windows NT® version 4.0. Active Directory installs in mixed mode to provide support for existing domain controllers that have not been upgraded to Windows 2000. You can operate your domain in mixed mode indefinitely, which allows you to upgrade domain controllers that run Windows NT 4.0 at any time, according to the needs of your organization.

If your network does not have any domain controllers running Windows NT 4.0, or when all of your domain controllers have been upgraded to Windows 2000, you can convert the domain from mixed mode to *native mode*. In a native-mode domain, all domain controllers run Windows 2000. However, member servers and client computers do not need to be upgraded to Windows 2000 before you convert a domain to native mode. Some functions in Active Directory, such as group nesting and universal security groups, require that the domain be in native mode. Although you can no longer add domain controllers running Windows NT 4.0 to a domain in native mode, you can still have clients and member servers that run other operating systems.

To change your domain from mixed mode to native mode, perform the following steps:

1. Open either Active Directory Users and Computers, or Active Directory Domains and Trusts from the **Administrative Tools** menu.
2. Open the **Properties** dialog box for the domain.
3. On the **General** tab, click **Change Mode**.
4. Click **Yes**, and then click **OK**.

Caution The change from mixed mode to native mode is a one-way process; you cannot change from native mode to mixed mode.

Implementing an Organizational Unit Structure

Topic Objective

To illustrate how to implement an organizational unit structure in Active Directory.

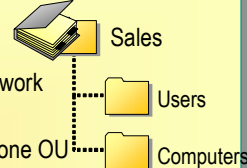
Lead-in

Before you create OUs, you need to do extensive planning to make sure that you organize users and resources by using a hierarchy of OUs that reflects the administrative model of your organization.

■ Implement an OU Structure if You Want to:

● Enhance Administrative Control

- ✓ Delegate administrative control over network resources
- ✓ Group similar network resources under one OU
- ✓ Simplify object administration, and control visibility of network resources
- ✓ Make resource administration more efficient



● Control Group Policy Application

■ Create an OU in a Domain or Within Another OU by Using Active Directory Users and Computers

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to create an OU.

Key Points

You should implement an OU structure within a domain for enhancing administrative control and controlling Group Policy so that it applies to a distinct group of users.

To create an OU, you must be assigned permissions; these permissions can also limit where you are allowed to create an OU.

To create child OUs, users need Read, List Contents, and Create Child (OU) permissions on a parent OU.

You can use OUs for such tasks as addressing an organization's administrative requirements and centrally applying Group Policy. You should create OUs that are meaningful and will not change often. You should implement an OU structure within a domain to either enhance administrative control or control Group Policy.

■ Enhancing administrative control means that you can:

- Delegate administrative control, such as adding, deleting, and updating objects in the OU, and decide who has access to the OU. Delegate administrative control over network resources, while maintaining the ability to manage the resources. You can assign administrative permissions to users or groups of users at the OU level.
- Group network resources with identical security requirements together under one OU to ease the task of administering these resources. For example, you could group all user accounts for temporary employees in one OU.
- Simplify object administration, and control visibility of network resources, such as printers, users, and computers. By controlling visibility of resources, users can view only the resources to which they have access.
- Make resource administration more efficient by assigning permissions once for an OU with many shared resources rather than multiple times for each shared resource.

■ Controlling Group Policy means that you can create separate Group Policy settings to a distinct group of users, such as permanent employees or temporary contractors.

You cannot create an OU unless you have been assigned permissions to do so; moreover, these permissions can also limit where you are allowed to create an OU. By default, members of the Domain Admins and Enterprise Admins groups have permission to create OUs. Users who are not members of these groups must be explicitly assigned this permission.

Users assigned Read, List Contents, and Create Child (OU) permissions on a parent OU can create child OUs. List Contents on the parent is not required, but without it, you are not able to see the new child OU after you create it.

To create an OU, perform the following steps:

1. In Active Directory Users and Computers, right-click the domain or OU in which you want to create the new OU.
2. Point to **New**, and then click **Organizational Unit**.
3. Type the name of the OU, and then click **OK**.

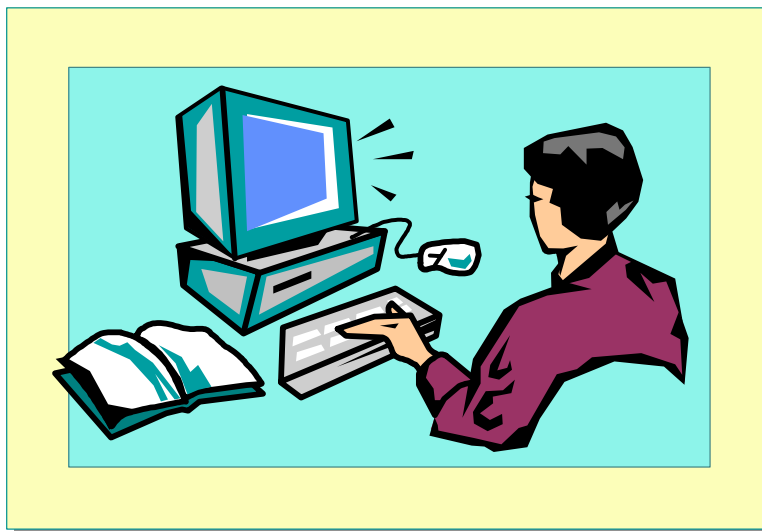
Lab B: Performing Post Active Directory Installation Tasks

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will convert your DNS zones to Active Directory integrated zones. Next, you will convert your domains to native mode. Finally, you will implement an organizational unit structure.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Verify Active Directory is correctly installed.
- Convert standard primary DNS zones to Active Directory integrated zones.
- Convert a domain from mixed mode to native mode.
- Plan an organizational unit (OU) structure.
- Create organizational units.

Prerequisite

Before working on this lab, you must have:

- An understanding of how Active Directory uses the DNS service.
- An understanding of organizational units.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server that is configured as a domain controller.

Estimated time to complete this lab: 30 minutes

Exercise 1

Verifying the Installation of Active Directory

Scenario

Having completed the installation of Active Directory, the second part of your implementation plan requires you to verify that the installation was successful.

Goal

In this exercise, you will verify that the installation of Active Directory was successful. You will do this by using DNS to verify that the required SRV resource records were created, verifying that the shared system volume (SYSVOL) was properly created and shared, and then verifying that the database file and associated log files were created.

Tasks	Detailed Steps
1. Verify that the required SRV resource records have been registered in DNS.	- Log on as Administrator with a password of password. - Open DNS from the Administrative Tools menu. - In the console tree, expand <i>computer</i> (where <i>computer</i> is your assigned computer name), expand Forward Lookup Zones, and then expand <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name).  The following folders appear below your domain name: <i>_msdcs</i>, <i>_sites</i>, <i>_tcp</i>, and, <i>_udp</i>. - Close DNS.
 Note: If the SRV resource records do not appear, open a command prompt, type net stop netlogon and then press ENTER, type net start netlogon and then press ENTER. This forces the registration of the SRV resource records.	
2. Verify that the shared system volume (SYSVOL) was created and shared.	- In the Run box, type %systemroot%\sysvol and then click OK.  A window displays the contents of the SYSVOL folder. You should see the following subfolders: <i>Domain</i>, <i>Staging</i>, <i>Staging Areas</i>, and <i>Sysvol</i>. - Close the SYSVOL window. - Open a command prompt window. - At the command prompt, type net share and then press ENTER.  In the output of the net share command, you should see an entry for SYSVOL, indicating that it has been shared. - Close the command prompt window.
3. Verify that the database and associated log files were created.	- In the Run box, type %systemroot%\ntds and then press ENTER.  A window displays the contents of the Ntds folder. You should see the following files and subfolders: <i>Drop</i>, <i>Edb</i>, <i>Edb</i>, <i>Ntds.dit</i>, <i>Res1</i>, <i>Res2</i>, and <i>Temp.edb</i>. - Close the NTDS window.

Exercise 2

Converting Standard Primary DNS Zones to Active Directory Integrated Zones

Scenario

As part of the plan to deploy Active Directory, you have decided to use Active Directory integrated zones to take advantage of the benefits provided by using Active Directory to store and replicate your DNS resource records.

Goal

In this exercise, you will convert your forward and reverse lookup zones from standard primary zones to Active Directory integrated zones.

Tasks	Detailed Steps
1. Convert the forward lookup zone for your domain from standard primary to Active Directory integrated zone.	- Open DNS from the Administrative Tools menu. - In the console tree, expand <i>Computer</i> (where <i>Computer</i> is your assigned computer name), expand Forward Lookup Zones, and then click <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name). - Right-click <i>domain.nwtraders.msft</i>, and then click Properties. - In the <i>domain.nwtraders.msft Properties</i> dialog box, on the General tab, click Change. - In the Change Zone Type dialog box, click Active Directory-integrated, and then click OK. - In the DNS dialog box, click OK to confirm the change, and then click OK to close the <i>domain.nwtraders.msft Properties</i> box.
2. Convert the reverse lookup zone for your subnet from standard primary to Active Directory integrated zone.	- In the console tree, expand Reverse Lookup Zones, and then click 192.168.y.x Subnet (where <i>y</i> is your assigned classroom number). - Right-click 192.168.y.x Subnet, and then click Properties. - In the 192.168.y.x Properties dialog box, on the General tab, click Change. - In the Change Zone Type dialog box, click Active Directory-integrated, and then click OK. - In the DNS dialog box, click OK to confirm the change, and then click OK to close the 192.168.y.x Properties box. - Close DNS.

Exercise 3

Converting a Domain from Mixed Mode to Native Mode

Scenario

Because you will not be using any Windows NT 4.0 domain controllers in your domain, and you want to take full advantage of all of the benefits offered by Active Directory, you have decided to convert your domain from a mixed-mode domain to a native-mode domain.

Goal

In this exercise, you will convert your domain from mixed mode to native mode.

Task	Detailed Steps
1. Convert the domain from mixed mode to native mode.	- Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, right-click <i>domain.nwtraders.msft</i>, and then click Properties. - In the <i>domain.nwtraders.msft Properties</i> box, click Change Mode. - In the Active Directory dialog box, click Yes to confirm the change. - Click OK to close the <i>domain.nwtraders.msft Properties</i> box, and then click OK to close the Active Directory dialog box. - Close all open windows, and then log off.

Exercise 4

Planning an Organizational Unit Structure

Scenario

The headquarters of Northwind Traders is preparing to deploy Windows 2000. All computers and users in this location will belong to the same domain. Northwind Traders currently has 1,000 users at this location, working in the Sales, Administration, and Production departments. Management expects moderate growth in the next five years, with the total workforce not increasing by more than 100 percent.

Full-time network administrators centrally perform most of the Windows 2000 administration for Northwind Traders centrally. However, an administrator in each of the three departments should handle the daily administration of users and groups. These administrators will be responsible for some administrative tasks, including adding and removing user accounts and occasionally changing passwords.

Most computers at Northwind Traders are similarly configured and have the same business applications installed. However, database servers have different applications installed. Only two senior network administrators should have complete administrative control over these servers. Finally, Northwind Traders has four domain controllers.



Which OUs must you add to the default Active Directory structure? Which objects will you place into these OUs? The key is to keep the structure simple, while still achieving all administrative goals.

At Northwind Traders, different administrators will control user accounts in each of three departments. Each department will have its own OU. Member servers are administered differently from client computers, and should be placed in their own OU. Place all domain controllers into the existing Domain Controllers OU. Leave all client computers in the existing Computers container.

Exercise 5

Organizing a Windows 2000 Domain

Scenario

To achieve the administrative goals stated in exercise 1, you will create an organizational unit structure. You will implement the structure that you discussed in the previous exercise.

Goal

In this exercise, you will create a part of the organizational structure of the Northwind Traders domain.

Task	Detailed Steps
1. Create OUs within the domain <code>domain.nwtraders.msft</code> , with the following names: • Sales • Administration • Production • Servers	- Log on to your domain as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand <code>domain.nwtraders.msft</code> (where <i>domain</i> is your assigned domain name) if necessary, and then click <code>domain.nwtraders.msft</code>.
 What are the default OUs and containers in your domain? Builtin, Computers, Users, ForeignSecurityPrincipals, and Domain Controllers.	
1. (continued)	- Right-click <code>domain.nwtraders.msft</code>, point to New, and then click Organizational Unit.  <i>The New Object – Organizational Unit dialog box appears. Notice that the only required information is the name of the new OU. The dialog box indicates that your domain is the location where the object will be created.</i> - In the Name box, type Sales and then click OK. - Repeat steps d and e to create the Administration, Production, and Servers OUs. - Close all open windows, and then log off.

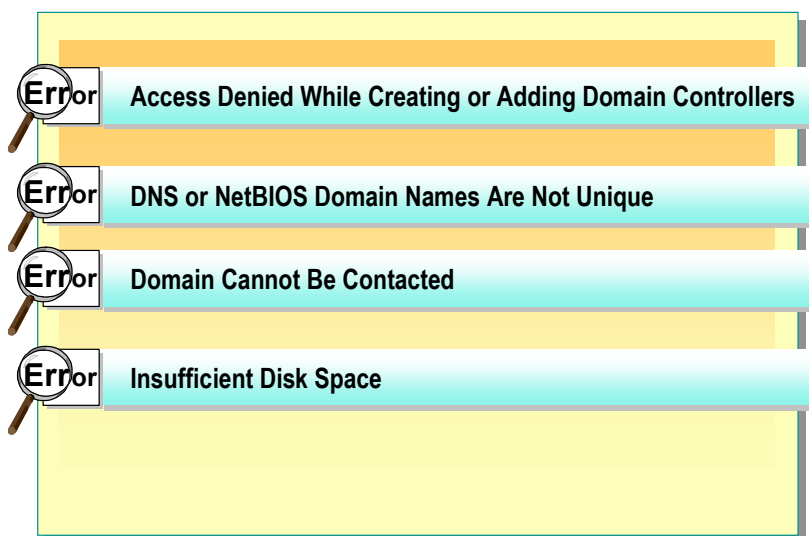
Troubleshooting the Installation of Active Directory

Topic Objective

To troubleshoot common problems with installing Active Directory.

Lead-in

You may encounter problems when installing Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

You may encounter problems when installing Active Directory. Here are some of the common problems that you may encounter and some strategies for resolving them:

- Access denied while creating or adding domain controllers. The following are the possible solutions for the access denied error message in different situations:
 - If you receive this message when creating the first domain controller in a new forest, you are not logged on to the server with an account that belongs to the Local Administrators group. Log off and then log on using an account that belongs to the Local Administrators group.
 - If you receive this message when you are adding a domain controller to an existing domain, you must supply credentials of a user account that is a member of the Domain Admins group or the Enterprise Admins group.
- DNS or NetBIOS domain names are not unique. When a domain is being created, both the DNS domain name and the NetBIOS domain names must be unique. If you receive an error message indicating that either one of the domain names is not unique, change the domain name.

-
- Domain cannot be contacted. When adding a replica domain controller to an existing domain, you may receive an error message indicating that the domain cannot be contacted, or that it is not an Active Directory domain. The following are the possible solutions to this problem:
 - Check DNS to ensure that the required SRV resource records exist for the domain that is being contacted.
 - If the SRV resource records are not present, you can force the registration of the SRV resource records by stopping the Net Logon service and then starting the Net Logon service on an existing domain controller.
 - If the SRV resource records are present in DNS, use **nslookup** to ensure that you can resolve DNS names from the computer on which you are trying to install Active Directory.
 - Insufficient disk space. Active Directory requires a minimum disk space of 250 MB, 200 MB for the database and 50 MB for the transaction logs. If you receive an insufficient disk space error message, consider using another volume or partition to store these files.

Removing Active Directory

Topic Objective

To illustrate how to use the Active Directory Installation wizard to remove Active Directory.

Lead-in

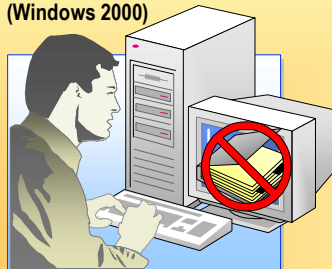
You also use the Active Directory Installation wizard to remove Active Directory. When you start the wizard on a domain controller, the domain controller is identified as a server that contains Active Directory, and the wizard prompts you for the information required to remove Active Directory.

■ Remove Active Directory by:

- Using the Active Directory Installation Wizard
- Providing appropriate administrative credentials

■ The Active Directory Installation Wizard Performs Specific Removal Operations Depending on the Type of Domain Controller

Domain Controller
(Windows 2000)



Provide Credentials:

- ☒ Enterprise Admins group member
- ☒ Domain Admins group member

Remove Active Directory

*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

You must log on to the domain as an administrator or as a member of the Domain Admins group to remove Active Directory from a domain controller that is the last domain controller in the forest.

You must be logged on as a member of either the Domain Admins group or the Enterprise Admins group to remove Active Directory from a domain controller that is not the last domain controller in the domain.

You use the Active Directory Installation wizard to remove Active Directory. When you start the wizard on a domain controller, the domain controller is identified as a server that contains Active Directory, and the wizard prompts you for the information required to remove Active Directory.

To remove Active Directory, you must provide the following administrative credentials:

- To remove Active Directory from a domain controller that is the last domain controller in the forest, you must log on to the domain as a member of the Domain Admins group or the Enterprise group.
- To remove Active Directory from a domain controller that is not the last domain controller in the domain, you do not need to provide credentials. However, you must be logged on as a member of either the Domain Admins group or the Enterprise Admins group.

Depending on whether you are removing Active Directory from the last domain controller in the domain or an additional domain controller, the same operations are common to both procedures. If any operation fails, the removal of Active Directory cannot proceed.

The following operations are common to removing Active Directory:

- Removes the shortcuts to Group Policy security settings, and restores the shortcut on the **Administrative Tools** menu to provide access to the local security settings for the member server or for the stand-alone server.
- Replicates all changes to the configuration and the schema directory partitions. For an additional domain controller, also replicates to the domain directory partition.
- Transfers to another domain controller any single-master roles that the domain controller is holding.

- Removes the system volume objects from the directory database, removes the system volume objects from the File Replication service database, and deletes the SYSVOL folder hierarchy. The File Replication service requests that Net Logon remove the share from the system volume.
- Removes the NTDS Settings object and cross-reference objects.
- Updates DNS to remove the Domain Controller Locator service records.
- Creates the local Security Accounts Manager (SAM) database in the same manner as during a fresh installation, including creating the administrator account and setting the password.
- Modifies the LSA membership policy to distinguish whether the computer is a stand-alone server or a member server.
- Stops the Net Logon service and the other services that were started during the installation of Active Directory. Services that relate only to the directory service are configured to not start automatically.

The following operations are specific to removing an additional domain controller:

- Locates and connects to a source domain controller in the same domain where the additional domain controller account exists and replicates changes to that source domain controller.
- Sets the computer account type to member server and moves the computer account for the additional server from the Domain Controllers OU to the Computers container.

The following operations are specific to removing the last domain controller in the domain:

- Verifies that no child domains exist.
- Locates and connects to a source domain controller in the parent domain and replicates changes to that source domain controller.
- Removes Active Directory objects from the forest that are specific to this domain.
- Removes trust objects on the parent server. The trusted Domain objects in the System folder are deleted.
- Places the server in a workgroup called Workgroup.

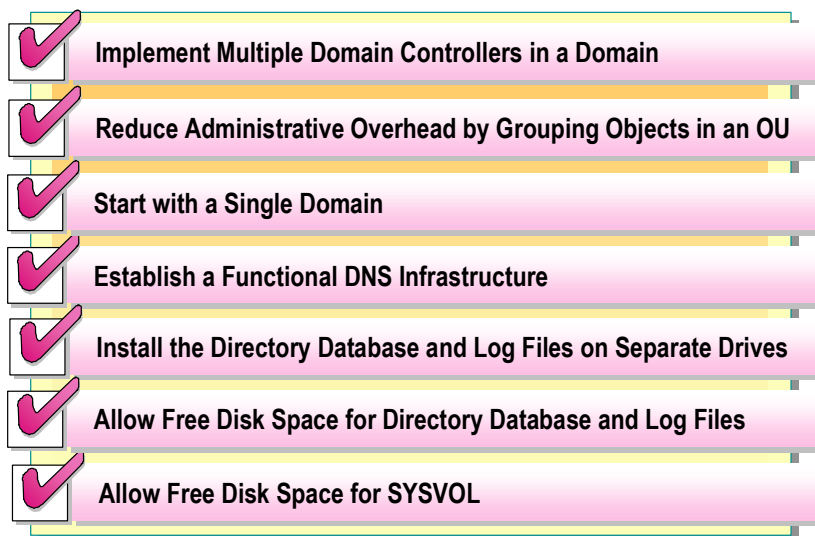
Best Practices

Topic Objective

To identify best practices for creating a Windows 2000 domain.

Lead-in

Review this checklist before you install Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

Emphasize the reason for each best practice.

The following list provides best practices for creating a domain in Windows 2000:

- Consider implementing multiple domain controllers in each domain. Multiple domain controllers provide both fault tolerance and load balancing.
- Reduce administrative overhead by grouping objects with identical security requirements into one OU. You can then easily assign access permissions to the entire OU and all objects within it.
- Consider implementing an Active Directory structure that consists of a single domain, which lowers administrative and hardware costs, and accommodates company reorganizations more efficiently. Add additional domains only when an OU structure does not meet your needs.
- Ensure that your DNS infrastructure is in place and functioning properly before creating the first domain. Active Directory depends on DNS to function properly.
- When installing Active Directory, place the directory database and log files on separate hard drives to help improve performance.
- Verify that the volumes that hold the directory database and log files contain sufficient free disk space to allow for the growth of the Active Directory structure.
- Ensure that the volume that holds the SYSVOL folder structure contains enough free disk space to allow for future growth. Although you can move the directory database and log files by using the **ntdsutil** utility, you cannot move the SYSVOL folder structure without removing and reinstalling Active Directory.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to Creating a Windows 2000 Domain
- Installing Active Directory
- The Active Directory Installation Process
- Examining the Default Structure of Active Directory
- Performing Post Active Directory Installation Tasks
- Troubleshooting the Installation of Active Directory
- Removing Active Directory
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

Give students time to read and answer the review questions on their own, and then discuss the answers as a group.

1. When you install Active Directory for the first time in a Windows 2000 network, what type of domain are you creating?

A forest root domain.

2. You want to run an unattended session of the Active Directory Installation wizard. The name of the answer file is Promote.txt. Which command do you type at the command prompt to run the answer file?

dcpromo /answer:promote.txt

3. When you install a replica domain controller in an existing domain, does the Active Directory Installation wizard check for the existence of a functioning DNS server? Why or why not?

No, when installing a replica domain controller, a functioning DNS server is assumed to exist on the network.

4. Which of the following must be located on a volume formatted with the NTFS file system:

- Directory database
- Log files
- SYSVOL folder structure

The SYSVOL folder structure must be located on a volume formatted with the NTFS file system.

5. When adding a replica domain controller to an existing domain, in which container is the computer object for the new domain controller created?

Domain controller computer objects are created in the Domain Controllers OU container.

6. When attempting to install a replica domain controller, you receive a message that the Active Directory domain you are trying to join cannot be contacted. When examining the DNS database, you notice that the required SRV records have not been created. How can you force the registration of the SRV records?

The registration of the SRV records can be forced by stopping and starting the Net Logon service.

7. You installed Active Directory and a default domain was created. Now you want to use the features of Active Directory, such as group nesting and universal security groups. Which domain mode is necessary to use these features in Active Directory?

Native mode.

8. What are the two main reasons you should plan to implement an OU structure within a domain?

To enhance administrative control.

To control Group Policy application.