
Module 14: Implementing an Active Directory Infrastructure

Contents

Overview	1
Business Scenario	2
Requirements for the Active Directory Infrastructure	4
Class Discussion: How to Implement the Active Directory Infrastructure	5
Lab A: Implementing the Active Directory Infrastructure	17
Course Evaluation	34



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:
45 Minutes

This module provides students with the skills to implement an Active Directory® directory service infrastructure that is based on the business requirements of a fictitious organization.

Lab:
150 Minutes

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

- Describe the infrastructure of a fictitious organization.
- Identify the business requirements for implementing the Active Directory infrastructure.
- Describe how to implement Active Directory based on the infrastructure designed by enterprise architects.
- Perform the tasks necessary to implement the Active Directory infrastructure.

In the hands-on lab in this module, students will have the opportunity to apply the plan discussed for implementing the Active Directory infrastructure in a fictitious organization.

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_14.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete all of the labs for Modules 2 through 12.
- Study the business scenarios and each of the class discussion topics. Prepare alternative answers and alternative ways to implement the business scenario.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- **Business Scenario**

In this topic, you will introduce the business scenario for a fictitious organization. At the beginning of class, instruct the students to run the clean up script so that the computers are ready to go when the lab starts. These business specifications will be used when discussing the implementation plan for the proposed Active Directory infrastructure.

- **Requirements for the Active Directory Infrastructure**

In this topic, you will introduce the requirements for the Active Directory Infrastructure. Emphasize that the implementation plan for the Active Directory infrastructure for Contoso, Ltd. should include all of the requirements given in the topic.

- **Class Discussion: How to Implement the Active Directory Infrastructure**

In this topic, you will discuss how to implement the Active Directory infrastructure. All of the topics in this section are class discussions on how to implement the different components of the Active Directory Infrastructure. The sequence of class discussions matches the sequence of tasks that need to be done in the lab. Emphasize that Contoso, Ltd. wants to have a Domain Name System (DNS) structure installed before installing Active Directory. Use the answer slides provided to show students a possible solution. Students can find different solutions to solve the same problem. Guide them toward the most reasonable solution that can be implemented in the lab.

- **Lab A: Implementing the Active Directory Infrastructure**

Prepare students for the lab in which they will implement the proposed Active Directory infrastructure as discussed in the class. The first exercise in the lab contains worksheets that students will complete to help them prepare for the other exercises. After students have completed the lab, ask them if they have any questions concerning the lab.

Customization Information

This section identifies the lab setup requirements for the 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

There are no setup requirements that affect replication or customization.

Lab Results

Because students have the flexibility to implement this lab in different ways, and because this lab does not provide detailed steps, the results will vary. It is highly recommended that you make this lab the last lab in a customized course or ensure that you properly set up the student computers for any lab that follows this one.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn how to implement an Active Directory infrastructure that is based on the business requirements of a fictitious organization.

- **Business Scenario**
- **Requirements for the Active Directory Infrastructure**
- **Class Discussion: How to Implement the Active Directory Infrastructure**
- **Lab A: Implementing the Active Directory Infrastructure**

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

Before starting this module, instruct the students to log on as Administrator for nwtraders.msft, and then run the cleanup script from C:\Moc\Win2154a\Labfiles\Rmad.vbs. This cleanup process will take 15-20 minutes.

Refer the students to the lab page for the instructions on how to run this script.

This module will provide you the opportunity to apply the knowledge and skills that you learned in this course to implement and administer an Active Directory® directory service infrastructure. You will implement Active Directory based on the business requirements of a fictitious organization.

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

- Describe the infrastructure of a fictitious organization.
- Identify the business requirements for implementing the Active Directory infrastructure.
- Describe how to implement the Active Directory infrastructure.
- Perform the tasks necessary to implement the Active Directory infrastructure.

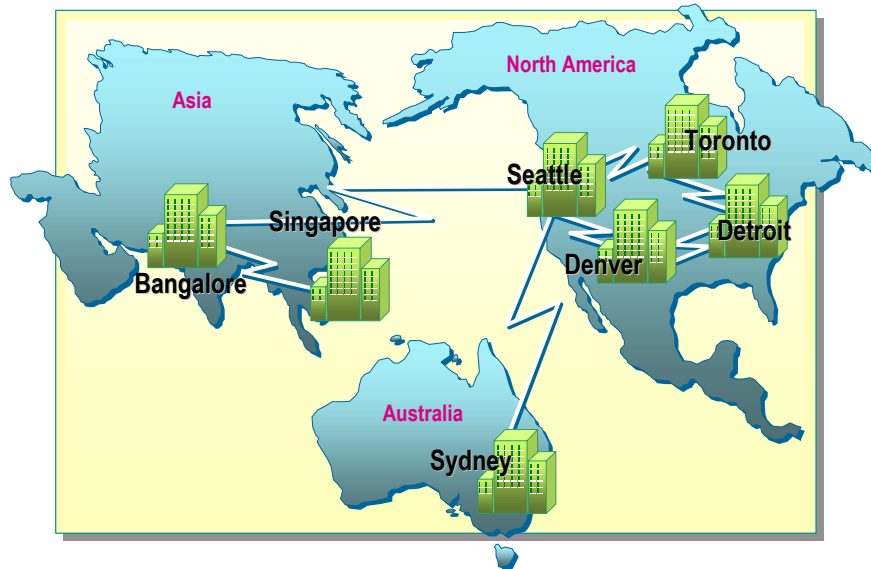
Business Scenario

Topic Objective

To describe the infrastructure of a fictitious organization.

Lead-in

You are required to implement an Active Directory infrastructure in a fictitious organization. First let's discuss the business specifications of this fictitious organization.



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

In this module, a fictitious organization named Contoso, Ltd. will be used to demonstrate how to implement an Active Directory infrastructure based on an organization's business requirements. Contoso, Ltd. is a worldwide organization with 50,000 employees.

The following are the business specifications of the different regions of Contoso, Ltd.

- The North American region has 25,000 employees:
 - 24,500 employees are located in the four primary locations, and the other employees are located in the 10 branch offices in other major North American cities.
 - Three of the four primary locations are separate business units and operate independently. The fourth primary location is corporate headquarters.
 - Each branch office has 50 or fewer employees. The employees need access to resources in all four primary locations. But the employees seldom need access to resources in other locations.
 - T1 lines connect the four primary locations. All branch offices are connected to the nearest primary location by 128 kilobits per second (Kbps) lines.

- The Asian region has 15,000 employees:
 - The employees are located in the two locations, Bangalore and Singapore. There are 8,000 employees at the Bangalore location and 7,000 employees at the Singapore location. These locations make up a single business unit.
 - The employees need occasional access to resources in the corporate location in North America, but seldom need access to resources in the Australian location.
 - The Bangalore and Singapore locations are connected to each other and to the North American location by T1 lines.
- The Australian region has 10,000 employees:
 - All employees are located in a single location, Sydney.
 - The employees need occasional access to resources in the corporate location in North America, but seldom need access to resources in the Asian location.
 - The Australian location is connected to the North American location by a 128 Kbps line.
- Contoso, Ltd.'s growth is expected to be minimal over the next three years.
- There are three main departments within Contoso, Ltd.: Accounting, Human Resources, and Information Services. Each of these departments is further divided into smaller departments and each location has employees from each of these departments.

Requirements for the Active Directory Infrastructure

Topic Objective

To identify the business requirements for the fictional organization's Active Directory infrastructure.

Lead-in

Contoso, Ltd. requires you to include the following requirements in the implementation plan for the Active Directory infrastructure.



Implementation Requirements

- ☒ A Single Schema
- ☒ Fault Tolerance in the Forest Root Domain
- ☒ DNS Infrastructure in Place Before Installing Active Directory
- ☒ DNS Solution Must Be Secure
- ☒ Reduction in Network Traffic and Separate Security Group Policy
- ☒ Set Up Printer Locations
- ☒ Standardization of the Administrative Model of OUs
- ☒ Delegation of Administrative Control
- ☒ Creation of User and Group Types
- ☒ Access to Performance Review Data
- ☒ Group Policy to Manage Users' Desktops and Deploy Applications

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

Tell students that these are the requirements of the fictitious organization. All of these requirements may not be necessary for implementing the Active Directory infrastructure in other situations.

The implementation of the Active Directory infrastructure for Contoso, Ltd. should include the following requirements in the infrastructure:

- Use a single schema for the entire organization.
- Provide directory services and Domain Name System (DNS) fault tolerance in the forest root domain.
- Put the DNS infrastructure in place before installing Active Directory.
- Secure the DNS solution so that only authorized clients may register in DNS.
- Reduce network traffic between the North American, Asian, and Australian locations, and apply separate security Group Policy settings to the different locations.
- Set up printer locations so that users can easily locate the printers near them.
- Standardize the administrative model of organizational units (OUs) across all locations.
- Delegate administrative responsibility for OUs to appropriate employees.
- Create appropriate types of users and groups depending on their job requirements.
- Require each location to maintain performance review files of employees. All managers in the organization need access to this information.
- Implement Group Policy to manage users' desktops and deploy applications.

◆ Class Discussion: How to Implement the Active Directory Infrastructure

Topic Objective

To introduce the topics related to the classroom discussion on how to implement the Active Directory infrastructure.

Lead-in

Before implementing the Active Directory infrastructure, let's discuss the plan for implementing DNS, Active Directory, sites and site links, printer locations, OUs, users and groups, and Group Policy.

- Installing and Configuring DNS
- Installing Active Directory
- Creating Sites and Site Links
- Setting Up Printer Locations
- Creating the OU Structure and Delegating Administrative Control
- Creating Users and Groups
- Implementing Group Policy

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

Based on the business scenario of Contoso, Ltd., you will implement a solution that uses Active Directory and Group Policy to satisfy the business requirements of the organization. In this section, you will discuss the plan for implementing DNS, Active Directory, sites and site links, printer locations, OU structure across domains, users and groups, and Group Policy.

Installing and Configuring DNS

Topic Objective

To illustrate how to set up DNS based on the business requirements of a fictitious organization.

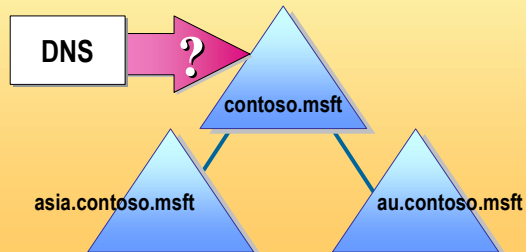
Lead-in

Contoso, Ltd. wants to install DNS structure before installing Active Directory. Let's discuss the DNS implementation plan based on the requirements.



- Root Domain Is contoso.msft
- Minimize DNS Name Resolution Network Traffic Between Regions
- DNS Should Be Secure
- DNS Is Fault Tolerant

How Do You Set Up DNS?



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

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

Delivery Tip

There are two slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second slide to discuss the correct answer with the class.

Contoso, Ltd. wants to install a DNS structure before installing Active Directory. DNS will enable all client computers running Microsoft® Windows® 2000 to resolve domain and computer names, define namespaces, and locate the physical components of Active Directory. The DNS domain name is contoso.msft.

1. How do you minimize DNS name resolution network traffic between the North American, Asian, and Australian regions?

Install DNS servers on all domains and delegate authority so that each domain is a separate zone. Also, create a secondary zone in the child domains of the forest root domain.

2. How do you ensure that DNS is secure so that only authorized clients can register in DNS?

Implement Active Directory integrated zones, and secure dynamic updates on all DNS servers.

3. How do you provide DNS fault tolerance in the forest root domain?

You must have at least two DNS servers in the forest root domain.

Installing Active Directory

Topic Objective

To illustrate how to install Active Directory based on the business requirements of a fictitious organization.

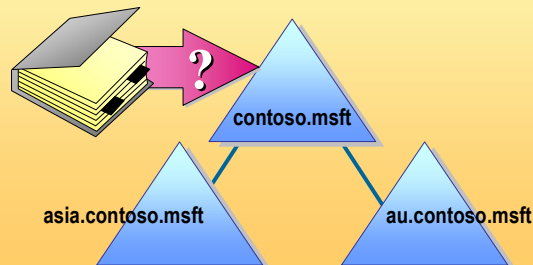
Lead-in

Contoso, Ltd. wants to decentralize administration and centralize management of resources. Let's discuss the Active Directory implementation plan based on the requirements.



- Single Schema
- Directory Services Are Fault Tolerant
- Reduce Network Traffic and Apply Separate Security Group Policy
- Ensure Operations Masters Are Working Correctly

How Do You Install Active Directory?



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

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

Delivery Tip

There are two slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second slide to discuss the correct answer with the class.

Contoso, Ltd. wants to decentralize administration and centralize management of resources by installing Active Directory. The names of the Asian and Australian domains are `asia.contoso.msft` and `au.contoso.msft`, respectively.

1. How do you ensure that there is a single schema across the Contoso, Ltd. network?

Create a single forest.

2. Contoso, Ltd. wants to reduce network traffic between domains. Each region also has separate security Group Policy requirements. How do you ensure that these requirements are fulfilled?

Implement separate domains in each region to reduce replication traffic. Create a domain for North America (`contoso.msft`) with two child domains per root domain. One domain is for Asia, and the other is for Australia.

3. How do you ensure that directory services are fault tolerant in the forest root domain?

Configure Active Directory for fault tolerance. There should be at least two domain controllers in the forest root domain.

4. How do you ensure that all operations masters are working correctly?

Transfer the infrastructure master in the forest root domain to the domain controller that is not a global catalog server.

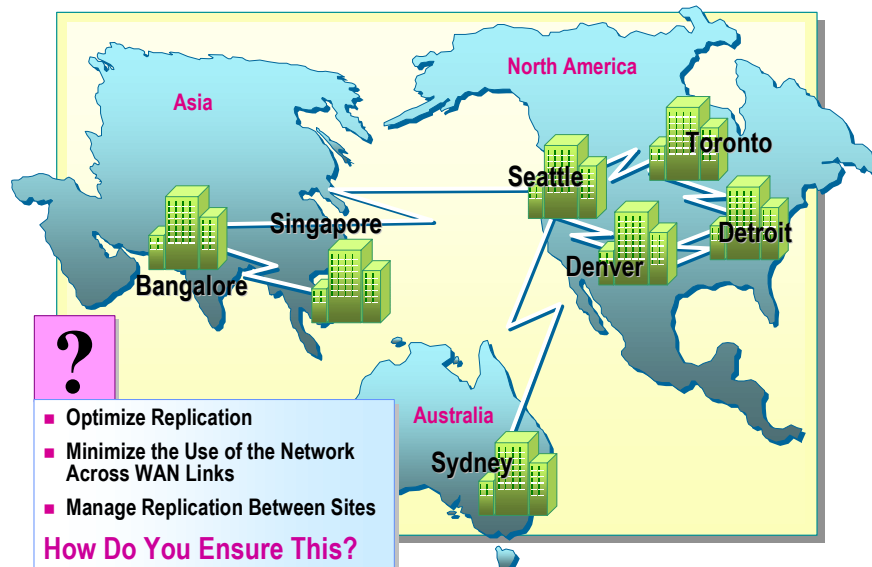
Creating Sites and Site Links

Topic Objective

To illustrate how to create and configure sites based on the business requirements of a fictitious organization.

Lead-in

The offices of Contoso, Ltd. are spread over North America, Asia, and Australia. Let's discuss how you reduce replication traffic between these regions.



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

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

Delivery Tip

There are two slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second slide to discuss the correct answer with the class.

The North American region has four primary locations, Seattle, Toronto, Denver, and Detroit, as well as 10 branch offices. The employees in the Asian region are located in the Bangalore and Singapore locations. The employees of the Australian region are all located in Sydney.

1. What sites do you create to reduce replication traffic among the primary locations in the three main regions of Contoso, Ltd.?

Create four sites in North America, and name them Seattle, Toronto, Denver, and Detroit. You can place the branch offices in the nearest site locations. Create two sites in Asia, and name them Bangalore and Singapore. Create one site in Australia, and name it Sydney.

2. Contoso, Ltd. is geographically distributed with many wide area network (WAN) links connecting the North American, Asian, and Australian regions. Network bandwidth on these WAN links is limited. Active Directory must be aware of which connections are local area networks (LANs) and which are WANs to optimize replication and minimize the use of the network across WAN links. What do you do to ensure this?

Create Internet Protocol (IP) subnet and site objects, and then associate the subnets to the sites.

3. Contoso, Ltd. wants to define the schedule for replication between sites. The schedule is according to the most beneficial time for replication to occur on the basis of network traffic and cost. How do you manage replication between sites?

Create and configure site links according to the specifications given in the lab.

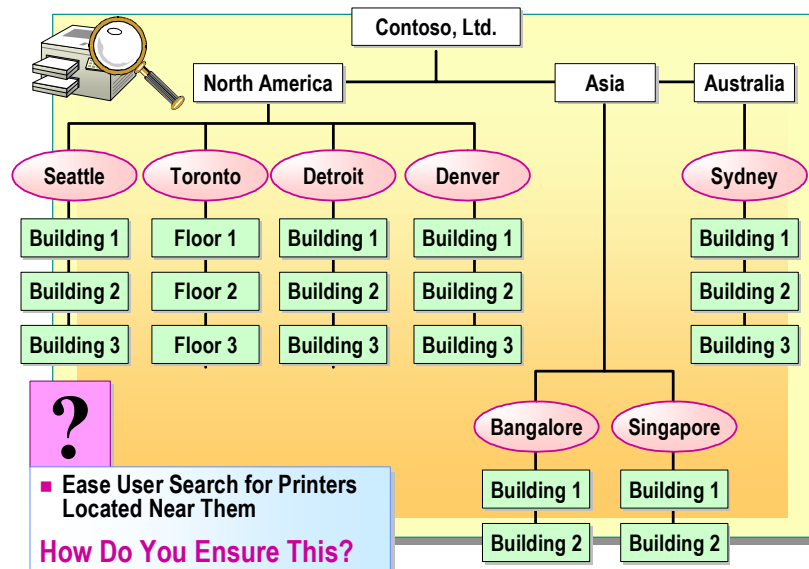
Setting Up Printer Locations

Topic Objective

To illustrate how to set up printer locations.

Lead-in

The IP addressing scheme for Contoso, Ltd. corresponds to the geographical and physical layout of its network. Therefore, to make it easy for users to search for printers near them, the organization wants you to also set up printer locations.



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

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

Delivery Tip

There are two slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second slide to discuss the correct answer with the class. Tell students that the subnet IP addresses are provided in the lab.

Contoso, Ltd. will have an Active Directory network configured with seven sites, and each site will correspond to IP subnet objects. Also, an IP addressing scheme will be present, and will correspond to the geographical and physical layout of the Contoso, Ltd. network. There are multiple office buildings at each location. The organization wants to implement printer locations to allow employees to locate and connect to print devices that are physically located near the employee.

- Contoso, Ltd. has already met the requirements for implementing printer locations, and has devised a naming convention. What are the four main tasks that need to be performed to configure printer locations?
 - **Enable printer location tracking by using Group Policy.**
 - **Create the required subnet objects in Active Directory.**
 - **Set the Location attribute for each subnet object. Use the naming convention that you develop for printer location names as the value of this attribute.**
 - **Set the Location attribute for printers. For each printer located in the physical location that corresponds to the IP subnet, you must add the Location attribute to the printer's properties.**
- How many subnet objects do you need to create to support the printer location feature at the building level?

You need 19 subnet objects, one for each location; building, or floor.

Creating the OU Structure and Delegating Administrative Control

Topic Objective

To illustrate how to implement the OU structure and delegate administrative control based on the business requirements of a fictitious organization.

Lead-in

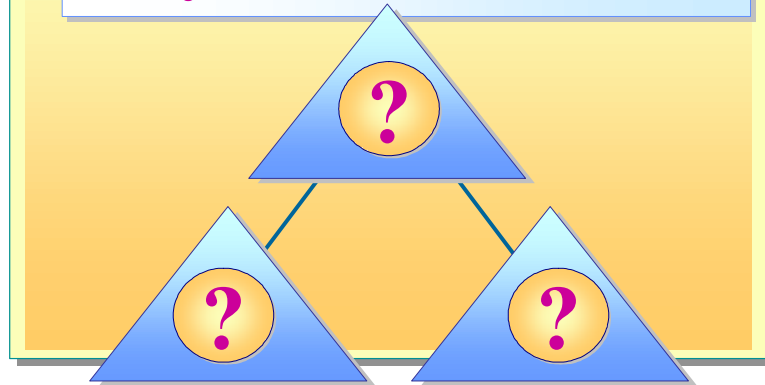
Contoso, Ltd. requires a common OU structure based on its administrative models. Let's discuss the OU structure for all domains.



■ Standardized Administrative Model

■ Delegate Administrative Control

What Is the OU Structure for Each Domain and How Will You Delegate Administrative Control for Each Domain?



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

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

Delivery Tip

There are two slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second slide to discuss the correct answer with the class.

Contoso, Ltd. has three main departments: Information Services, Human Resources, and Accounting. The organization has decided upon a delegated administration model, and one administrator from each department will be responsible for managing the resources and users in that department. The following table lists the names of the subsidiary departments under the three main departments.

Main departments	Subsidiary departments
Information Services	Help Desk Applications Operating Systems Messaging Customer Support
Human Resources	Benefits Payroll Training Recruiting
Accounting	Accounts Payable Accounts Receivable

1. Each of the departments in Contoso, Ltd. is a separate OU. How do you ensure that the administrative model for OUs is standard across all domains in the network of your organization?

Create a common OU structure for each domain in the entire forest.

Information Services

Help Desk

Applications

Operating Systems

Messaging

Customer Support

Human Resources

Benefits

Payroll

Training

Recruiting

Accounting

Accounts Payable

Accounts Receivable

2. How do you ensure that one administrator from each department is responsible for managing the resources and users in that department?

Delegate administrative control of each of the three top level OUs to a different administrator.

Creating Users and Groups

Topic Objective

To illustrate how to set up users and groups based on the business requirements of the fictitious organization.

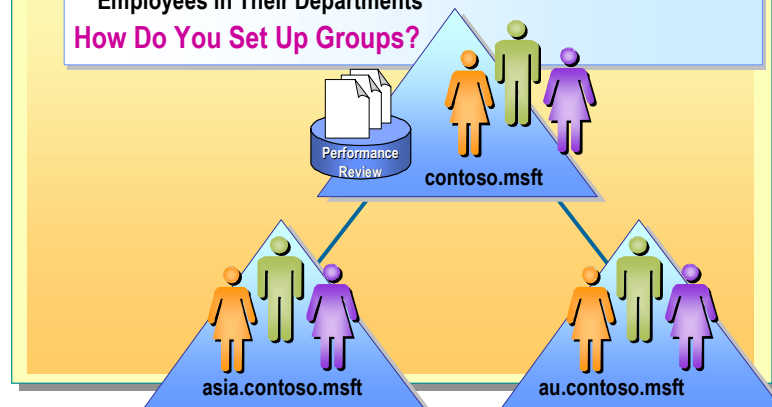
Lead-in

Let's now discuss the creation of users and groups and the strategies for using groups in the Active Directory infrastructure.



- Create Multiple Users
- Managers Need Read Access to the Performance Review Data for the Entire Organization
- Managers Need Full Control to the Performance Review Data of Employees in Their Departments

How Do You Set Up Groups?



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

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

Delivery Tip

There are three slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second and third slides to discuss with the class the correct answers for the questions numbered 2 and 3 respectively on group types.

The managers of each department at Contoso, Ltd. are responsible for completing the performance reviews for their direct reports. Other managers, when considering an internal transfer of an employee from one department to another department, can reference the performance review data. Therefore, all managers require Read access to the performance review data. The managers for each department need Full Control access to the performance review data of the employees in their departments.

1. The Users.txt text file contains the information on all users who are to be added to each domain. How do you ensure that multiple users are created with minimal effort?

Create multiple users to populate the OUs through bulk import.

2. The performance review data is stored in a single file server for each domain. The data is grouped under folders by department name. Each domain has Information Services, Human Resources, and Accounting departments. What proposed group structure enables all managers to have only Read access to the performance review data for the entire organization?

Global group: Information Services Managers

Create this group in the Information Services OU.

Assign group membership to users.

Global group: Human Resources Managers

Create this group in the Human Resources OU.

Assign group membership to users.

Global group: Accounting Managers

Create this group in the Accounting OU.

Assign group membership to users.

Global group: *Domain* Managers (where *Domain* is the name of your domain).

Create this group in the appropriate OU.

Assign group membership to Information Services Managers, Human Resources Managers, and Accounting Managers.

Universal group: All Managers

Create this group in the appropriate OU only in the forest root domain.

Assign group membership to all three *Domain* Managers (where *Domain* is the name of each of the three domains in the forest).

Domain Local group: Performance Data

Create this group in the appropriate OU.

Assign group membership to All Managers.

Assign Read permissions on the Performance folder to the Performance Data group.

Emphasize that it is not recommended that you assign Full control permissions to a resource unless you are sure that the group is required to manage permissions within the folder structure.

3. What proposed group structure enables department managers to have Full Control access to the performance review data of the employees in their departments?

Domain Local group: Information Services Performance Data

Create this group in the Information Services OU.

Assign group membership to Information Services Managers.

Assign Full Control permissions on the Information Services folder under the Performance folder to the Information Services Performance Data group.

Domain Local group: Human Resources Performance Data

Create this group in the Human Resources OU.

Assign group membership to Human Resources Managers.

Assign Full Control permissions on the Human Resources folder under the Performance folder to the Human Resources Performance Data group.

Domain Local group: Accounting Performance Data

Create this group in the Accounting OU.

Assign group membership to Accounting Managers.

Assign Full Control permissions on the Accounting folder under the Performance folder to the Accounting Performance Data group.

Implementing Group Policy

Topic Objective

To illustrate how to implement Group Policy across all domains based on the business requirements of the fictitious organization.

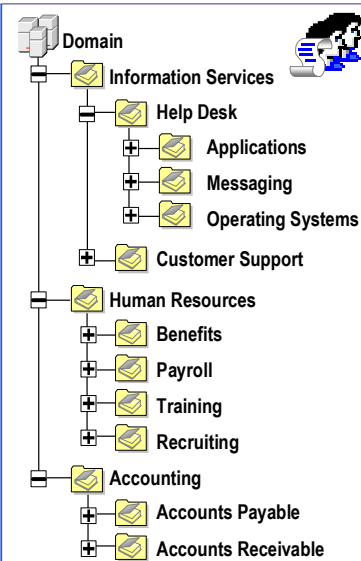
Lead-in

Finally, let's discuss the Group Policy implementation plan for Contoso, Ltd.



- Deploy Cosmo 2 Application to All Users Except Those in Human Resources OU.
- Deploy Windows 2000 Support Tools to All Users in the Information Services OU Except Those in the Contractors Group.
- Implement the Organization-Wide Group Policy Settings by Using Administrative Templates.
- Secure the Network Resources by Implementing Organization-Wide Group Policy Settings.

What Is the Proposed Group Policy Implementation for All Domains?



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

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

Delivery Tip

There are three slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second and third slides to discuss with the class the correct answers for the questions numbered 1 and 2 respectively on blocking inheritance and filtering Group Policy.

Contoso, Ltd. requires you to use administrative template settings to implement the following Group Policy settings across the entire organization:

- Disk quotas must be enabled on all computers.
- The disk quota limit must be enforced on all computers.
- The default quota limit for all users must be 100 megabytes (MB) and the warning level must be 75 MB.
- An event should be logged when the warning level and the quota limits are exceeded.
- Access to Windows Update must be denied.
- All users in all domains must not be able to run Freecell (Freecell.exe), Minesweeper (Winmine.exe), Pinball (Pinball.exe), and Solitaire (Sol.exe) applications.
- The users responsible for administering OUs must have access to only the following Microsoft Management Console (MMC) snap-ins: Active Directory Users and Computers, Group Policy, Group Policy tab for Active Directory Tools, Administrative Templates (Users), and Administrative Templates (Computers).

Contoso, Ltd. also requires you to secure the network resources by implementing the following Group Policy settings across the entire organization:

- Minimum password length of eight characters.
- Account lockout threshold of three logon attempts.
- Account lockout duration of 60 minutes.
- All users must be able to log on locally to all computers, including domain controllers.
- Do not display the last user name in the **Log On to Windows** dialog box.
- Membership in the Group Policy Creator Owners group must be restricted to the Administrator account and the accounts belonging to the users responsible for administering each top level OU.

Based on the given requirements, create Group Policy objects and implement Group Policy in the Active Directory infrastructure.

1. With the exception of the users in the Human Resources OU, all users in all domains must have Cosmo 2 installed. How do you deploy the Cosmo 2 application?

Assign Cosmo 2 in a Group Policy object (GPO) linked to the domains, and then enable Block Inheritance on the Human Resources OU.

2. With the exception of Contractors who work in the Messaging department, all users in the Information Services OU, in all domains, must be able to install the Windows 2000 Support Tools if they choose to. How do you deploy the Windows 2000 Support Tools application?

Create and link a GPO to the Information Services OU that publishes the Windows 2000 Support Tools. Modify the discretionary access control list (DACL) of this GPO so that the user accounts used by the Contractors group in the Messaging OU are denied Apply Group Policy permission.

3. The administrators responsible for each of the top level OUs (Information Services, Human Resources, and Accounting) must be able to link and unlink Group Policy objects (GPOs), create new GPOs, and edit only the GPOs they create. How do you delegate administrative control?

For each administrator in the Information Services OU, Human Resources OU, and the Accounting OU:

Delegate the Manage Group Policy Links task for their OUs.

Assign membership for the Group Policy Creator Owners security group.

Lab A: Implementing the Active Directory Infrastructure

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will implement and test the proposed Active Directory infrastructure.



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

Explain the lab objectives.

In Task 10 of Exercise 2, if students have a problem resolving host names in the forest root domain, suggest that they look in Root Hints to verify that the DNS server that is authoritative for contoso.msft is listed.

Consider suggesting to the students that they may want to change their computer names to match the business scenario. Note that new computer names must be unique in the classroom.

Objectives

After completing this lab, you will be able to:

- Set up the DNS services based on the business requirements of a fictitious organization.
- Install Active Directory based on the business requirements of a fictitious organization.
- Create and configure sites and site links based on the business requirements of a fictitious organization.
- Set up printer locations based on the business requirements of a fictitious organization.
- Implement the OU structure and delegate administrative control based on the business requirements of a fictitious organization.
- Set up users and groups based on the business requirements of the fictitious organization.
- Implement Group Policy across all domains based on the business requirements of the fictitious organization.

Prerequisites

Before working on this lab, you must have:

- An understanding of the components of Active Directory.
- An understanding of how Active Directory uses the DNS service.
- Knowledge of and skills transferring operations master roles.
- Knowledge of and skills working with Active Directory Users and Computers.
- Knowledge of and skills creating and configuring sites and site links.
- Knowledge of and skills defining printer location names and setting up printer locations.
- Knowledge of and skills creating domain user accounts and groups.
- Knowledge of and skills bulk importing data into Active Directory.
- An understanding of Active Directory permissions.
- Knowledge of and skills implementing Group Policy.

Lab Setup

To complete this lab, perform the following steps:

1. Log on as Administrator for nwtraders.msft.
2. Run the script C:\Moc\Win2154a\Labfiles\Rmad.vbs.
3. When the computer restarts, log on as Administrator.

The computer will complete its tasks and then restart again.

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.

Note This script removes all the server objects in the forest with the exception of London, runs Dcpromo.exe by using an answer file to demote the domain controller to a standalone server, removes the preferred DNS server, and removes the primary DNS suffix.

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: 150 minutes

Exercise 1

Planning the Implementation of the Active Directory Infrastructure

Scenario

For Contoso, Ltd., before implementing an Active Directory infrastructure, a best practice is to plan and prepare for the implementation. The diagrams in this exercise will help you to prepare for the implementation by gathering the information for the implementation plan that was reviewed during the class discussion.

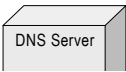
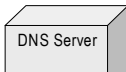
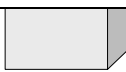
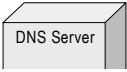
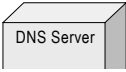
Note: You will be assigned a group number. Use this group number along with the names that you define for the domains. For example, if your group number is 1, then the domain name for the Asian location would be asia1.contoso1.msft.

Goal

In this exercise, you will complete the implementation planning worksheets for the required domains, DNS, sites and OUs for Contoso, Ltd.

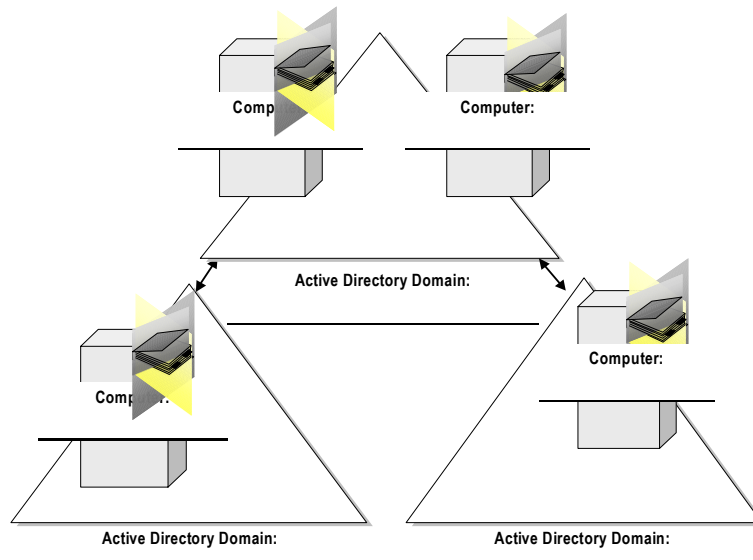
DNS Domain Structure

In the following worksheet, provide the DNS domain names and the reverse lookup zone name for your DNS structure. Also, provide the IP address and the computer name for each of the four computers that you will configure as DNS servers. You will use this information when implementing the DNS infrastructure.

☐ Active Directory integrated ☐ Secure dynamic update	 DNS Server Computer: _____	☐ Active Directory integrated ☐ Secure dynamic update	 DNS Server Computer: _____
 DNS Server Computer: _____  DNS Server Computer: _____			
DNS Domain: _____ Reverse Lookup Zone: _____ IP Address: _____			
☐ Active Directory integrated ☐ Secure dynamic update	 DNS Server Computer: _____	☐ Active Directory integrated ☐ Secure dynamic update	 DNS Server Computer: _____
 DNS Server Computer: _____		 DNS Server Computer: _____	
DNS Domain: _____ IP Address: _____		DNS Domain: _____ IP Address: _____	

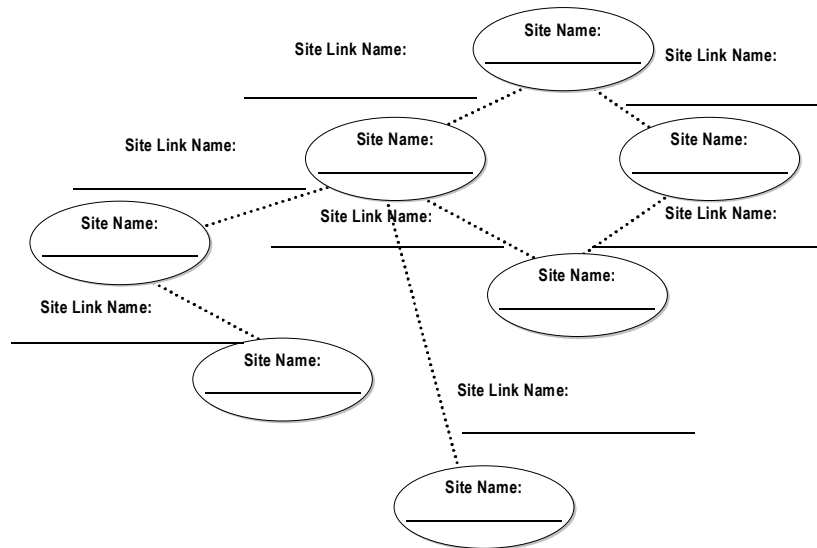
Active Directory Domain Structure

In the following worksheet, provide Active Directory domain names. Also, identify which computer will be configured as the domain controller for the forest root, the additional domain controller for the forest root, and the domain controller for the child domains. You will use this information when implementing Active Directory.



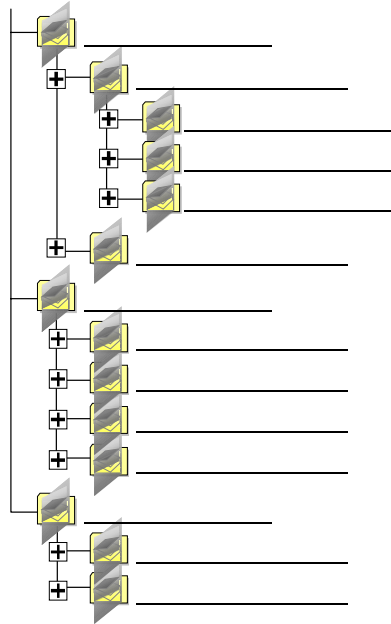
Site Structure

In the following worksheet, provide a name for each site and site link for Contoso, Ltd. You will use this information when configuring sites and site links.



Organizational Unit Structure

In the following worksheet, provide the OU structure names. You will use this information when creating the common OU structure for each domain.



Exercise 2

Installing and Configuring DNS

Scenario

The functional specification requires a working DNS infrastructure to be in place before you install Active Directory. Each Active Directory domain will maintain its own DNS information.

Goal

In this exercise, you will install and configure DNS for each computer you identified as DNS server. You will configure a forward lookup zone for each of the Active Directory domains and a single reverse lookup zone for the forest. You will also configure all forward and reverse lookup zones to support dynamic update. It is a best practice to verify that DNS is installed and configured properly before you create the Active Directory domain structure. Use your planning worksheet to complete this exercise.

Tasks	Detailed Steps
1. Install and configure DNS on each computer.	- Configure the DNS suffix for your computer. When prompted, restart the computer. - Start the Windows Components wizard, and install the Domain Name System (DNS) subcomponent of Networking Services. Copy the required files from the Windows 2000 Advanced Server compact disc.
 Important: Only perform the following tasks on the first DNS server in the contoso.msft domain.	
2. Create forward and reverse lookup zones.	- Add a standard primary forward lookup zone for contoso.msft (where <i>x</i> is your assigned group number). - Add a standard primary reverse lookup zone for your classroom network ID. - Configure the Internet Protocol (TCP/IP) properties of your Local Area Connection to use your computer for DNS.
3. Configure DNS to support dynamic update.	- Configure the forward lookup zone for contoso.msft to support dynamic update. - Configure the reverse lookup zone for your subnet to support dynamic update. - Use the ipconfig command to re-register your computer's DNS records. - Refresh DNS to display the pointer resource record in the reverse lookup zone.
4. Use nslookup to test DNS.	- Confirm that DNS can resolve a host name to an IP address. - Confirm that DNS can resolve an IP address to a host name.
5. Delegate authority for each sub domain.	▪ Perform a new delegation in contoso.msft to a DNS server in each sub domain.

Tasks	Detailed Steps
 Important: Only perform the following tasks on the second DNS server in the contoso.msft domain.	
6. Create secondary forward and reverse lookup zones of contoso.msft.	- Add a standard secondary forward lookup zone for contoso.msft (where x is your assigned group number). - Add a standard secondary reverse lookup zone for your classroom network ID. - Configure the Internet Protocol (TCP/IP) properties of your Local Area Connection to use your computer for DNS. - Confirm that DNS can resolve a host name to an IP address.
 Important: Only perform the following tasks on the DNS servers in the sub domains.	
7. Create the primary forward lookup zone for your domain.	- Use the Configure the server wizard to add a standard primary forward lookup zone for your domain. - Configure the Internet Protocol (TCP/IP) properties of your Local Area Connection to use your computer for DNS.
8. Create a secondary reverse lookup zone for your domain.	▪ Add a standard secondary reverse lookup zone for your domain from the zone created in contoso.msft.
9. Configure DNS to support dynamic update.	- Configure the forward lookup zone for your domain to support dynamic update. - Use the ipconfig command to re-register your computer's DNS records.
10. Use nslookup to test DNS.	- Confirm that DNS can resolve a host name to an IP address. - Confirm that DNS can resolve a host name in the forest root domain to an IP address.  <i>If you have a problem resolving a host name in the forest root domain, look in Root Hints to verify that the DNS server that is authoritative for contoso.msft is listed.</i>

Exercise 3

Installing Active Directory

Scenario

Now that the DNS infrastructure is in place and properly configured, you can create the Active Directory domain structure for Contoso, Ltd.

Goal

In this exercise, you will install Active Directory to create a single forest with two child domains. You will also configure the forest root domain for fault tolerance, implement Active Directory integrated zones, and transfer infrastructure master to a non-global catalog server. Use your planning worksheet to complete this exercise.

Tasks	Detailed Steps
1. Create the Active Directory domain structure.	■ Use the Active Directory Installation wizard to create: • The forest root domain. • Two child domains.
2. Configure the forest root domain for fault tolerance.	■ Create an additional domain controller for the forest root domain.
3. Implement Active Directory integrated zones in each domain.	a. Convert all of the forward lookup zones to Active Directory-integrated. b. Convert the primary reverse lookup zone to Active Directory-integrated. c. Enable secure updates for Active Directory integrated zones.
4. In the forest root domain, transfer infrastructure master to a non-global catalog server.	a. Determine which domain controller holds the infrastructure master role and which domain controller is a global catalog server. b. If necessary, transfer the infrastructure master to a domain controller that is not a global catalog server.

Exercise 4

Creating Sites and Site Links

Scenario

The North American region has four primary locations: Seattle, Detroit, Toronto, and Denver. The employees in the Asian region are located equally in two locations, Bangalore and Singapore. The employees of the Australian region are all located in Sydney.

Goal

In this exercise, you will create and configure sites and site links based on the information in the following table. Use your planning worksheet to complete this exercise.

IP Site Links	Cost	Frequency (minutes)	Schedule
Seattle – Toronto	100	90	Sun-Sat 7A.M.–1A.M. GMT
Seattle – Denver	100	120	Sun-Sat 12P.M.–1A.M. GMT
Seattle – Bangalore	200	90	Sun-Sat 12A.M.–1A.M. GMT
Seattle – Sydney	900	90	Sun-Sat 12A.M.–2A.M. GMT
Toronto – Detroit	100	180	Sun-Sat 4P.M.–1A.M. GMT
Detroit – Denver	100	200	Sun-Sat 3P.M.–1A.M. GMT
Bangalore – Singapore	100	60	Always available

Tasks	Detailed Steps
1. Create sites for each region.	▪ Use Active Directory Sites and Services to create sites for each region.
2. Create and configure all of the site links.	a. Create all of the site links. Refer to your planning worksheet for the site link names. b. Configure the cost, frequency, and schedule for each site link by using the information the table.

Exercise 5

Publishing Printers and Using Printer Locations

Scenario

To use printers more effectively, printers in each location will be published in Active Directory and the printer location feature will be configured to easily find a printer in the user's location.

Goal

In this exercise, you will create subnet objects, publish printers, and configure the printer location feature based on the scenario. For creating printer locations, use the subnet information in the following table.

Site	Location	Subnet
Denver	US/Denver/Building 1	10.10.1.0/24
Denver	US/Denver/Building 2	10.10.2.0/24
Denver	US/Denver/Building 3	10.10.3.0/24
Seattle	US/Seattle/Building 1	10.15.1.0/24
Seattle	US/Seattle/Building 2	10.15.2.0/24
Seattle	US/Seattle/Building 3	10.15.3.0/24
Toronto	CA/Toronto/Floor 1	10.20.1.0/24
Toronto	CA/Toronto/Floor 2	10.20.2.0/24
Toronto	CA/Toronto/Floor 3	10.20.3.0/24
Detroit	US/Detroit/Building 1	10.30.1.0/24
Detroit	US/Detroit/Building 2	10.30.2.0/24
Detroit	US/Detroit/Building 3	10.30.3.0/24
Bangalore	India/Bangalore/Building 1	10.40.1.0/24
Bangalore	India/Bangalore/Building 2	10.40.2.0/24
Singapore	Singapore/Building 1	10.50.1.0/24
Singapore	Singapore/Building 2	10.50.2.0/24
Sydney	Australia/Building 1	10.60.1.0/24
Sydney	Australia/Building 2	10.60.2.0/24
Sydney	Australia/Building 3	10.60.3.0/24

Tasks	Detailed Steps
1. Create and configure the subnet objects for each site.	- Create the subnet objects and assign them to the appropriate site. - Configure the location field for the subnet objects.
2. Enable the printer location feature.	Use Group Policy to enable the printer location for each domain.
3. Create and publish a printer for each location.	Create and publish a printer for each location and ensure the location information utilizes the location information from the subnet objects.

Exercise 6

Creating the OU Structure and Delegating Administrative Control

Scenario

There is a common OU structure in all of the domains in Contoso, Ltd. There are three main OUs: Information Services, Human Resources, and Accounting. The organization has decided upon a delegated administration model, and one administrator from each OU will be responsible for managing the resources and users in that OU.

Goal

In this exercise, you will create a common OU structure for each domain in the entire forest, and delegate administrative control of each of the three top level OUs to a different administrator. Use your planning worksheet to complete this exercise.

Note: Perform all of the following tasks in each domain.

Tasks	Detailed Steps
1. Create a common OU structure.	■ Create OUs within each domain. Use the same names that you defined during the planning exercise.
 Note: Perform the following task after completing Task 1 in Exercise 7.	
2. Delegate administrative control.	■ Use the Delegation of Control wizard to assign Active Directory permissions for creating, deleting, and managing user accounts, groups, and printers in the Information Services OU, the Human Resources OU, and the Accounting OU to any one user in that OU.

Exercise 7

Creating Users and Groups

Scenario

The managers of each department at Contoso, Ltd are responsible for conducting the performance reviews for their direct reports. Other managers can use the performance review data when considering an internal transfer of employee from one department to another department. Therefore, all managers require the Read access to the performance review data. The managers for each department need Full Control access to the performance review data of the employees in their department.

Goal

In this exercise, you will create multiple users to populate the OUs through bulk import by using the common OU structure. You will create appropriate groups to enable all managers to have only Read access to the performance review data for the whole organization. You will also create appropriate groups to enable department managers to have Full Control access to the performance review data of the employees in their department.

Note: Perform all of the following tasks in each domain.

Tasks	Detailed Steps
1. Create multiple users accounts.	- Prepare the Users.txt file for use with the csvde bulk import utility. - Perform a bulk import of Users.txt. - Verify that the bulk import was successful.
2. Create a global group called Contractors in the Messaging OU.	▪ Create a global group called Contractors in the Messaging OU.
3. Create folders and files for the performance review data.	- Create and share the folder C:\Performance Data on one server in each domain. - Create subfolders Information Services, Human Resources, and Accounting under the Performance Data folder. - Create a blank text file in each of the subfolders.
4. Create groups for managers in the Accounting division who require Read access to the performance review data for the whole organization.	- Create appropriate global groups in each department OU. - Add the department global groups into a Domain Managers global group. - Add the Domain Managers global group into a universal group. - Add the Universal group into domain local groups for each domain. - Assign Read permission to the domain local groups.
5. Create groups for managers who require Full Control access to the performance review data of the employees in their department.	- Create appropriate global groups and add them into a department global group. - Add department global groups into each domain local group. - Assign Full Control permission to the domain local group for a department.

Exercise 8

Implementing Group Policy

Scenario

Contoso, Ltd. wants to deploy the Cosmo 2 application to all users except those in the Human Resources OU, and Windows 2000 Support Tools to all users in the Information Services OU except those in the Contractors group. They also want you to implement the organization-wide Group Policy settings by using Administrative Templates, and secure the network resources by implementing organization-wide Group Policy settings.

Goal

In this exercise, you will apply Block Inheritance, apply filtering by using DACLs, implement the Group Policy settings by using Administrative Templates, secure the network resources by implementing Group Policy settings, and delegate administrative control for implementing Group Policy.

Tasks	Detailed Steps
1. Deploy the Cosmo 2 application so that it is available to all users, except the users in the Human Resources OU.	▪ Apply Block Inheritance on the Human Resources OU.
2. Deploy the Windows 2000 Support Tools application so that it is available to all users in the Information Services OU, except the users who are members of the Contractors group in the Messaging OU.	a. Create and link a GPO to the Information Services OU that publishes the Windows 2000 Support Tools. b. Modify the DACL of this GPO so that the members of the Contractors group in the Messaging OU are denied Apply Group Policy permission.
3. Implement organization-wide Group Policy settings.	a. Create new GPOs linked to the appropriate OUs. b. Edit the administrative template settings for the new GPO to: • Enable disk quotas on all computers. • Enforce the disk quota limit on all computers. • Set the default quota limit for all users to 100 MB and the warning level to 75 MB. • Log an event when the warning level and the quota limits are exceeded. • Deny access to Windows Update. • Prevent users in all domains from running Freecell (Freecell.exe), Minesweeper (Winmine.exe), Pinball (Pinball.exe), and Solitaire (Sol.exe) applications. • Enable access to the MMC snap-ins: Active Directory Users and Computers, Group Policy, Group Policy tab for Active Directory Tools, Administrative Templates (Users), and Administrative Templates (Computers) to the users responsible for administering OUs.

Tasks	Detailed Steps
3. <i>(continued)</i>	c. Verify that the Group Policy settings contained in the Admin Template GPO are being properly applied.
4. Secure the network resources.	a. Create new GPOs as required to implement the following settings: • Minimum password length of eight characters. • Account lockout threshold of three logon attempts. • Account lockout duration of 60 minutes. • All users must be able to log on locally to all computers, including domain controllers. • Do not display the last user name in the Log On to Windows dialog box. • Membership in the Group Policy Creator Owners group must be restricted to the Administrator account and the accounts belonging to the users responsible for administering each top-level OU. b. Verify that the modifications to the Additional Security Settings Policy GPO are being applied correctly.

Exercise 9

Verifying the Implementation

Scenario

Now that you have implemented the Active Directory infrastructure for Contoso, Ltd., you need to verify the implementation.

Goal

In this exercise, you will verify that:

- You can correctly configure domains and ensure that the global catalog is working.
- The minimum password length is set correctly.
- The group structure has been correctly defined and proper access to resources is in place.
- The printer location feature is enabled and that all of the buildings are properly defined.
- The OU delegation and Group Policy has been implemented.
- Replication is working correctly on all domain controllers.

Tasks	Detailed Steps
1. Verify that the domains and global catalog are working correctly.	■ Log on using Sandra Martinez's user principal name from another domain.
2. Verify that managers have Full Control access over the performance review data in their department and Read permissions on the performance data in the other departments.	a. Test the Full Control access over the data in the Accounting department. b. Test the Read access over the data in the other departments.
3. Verify that the minimum password length of eight characters is in effect.	■ Attempt to change Sandra Martinez's password to a string of less than eight characters.
4. Verify that the printer location feature is functioning.	■ In the Find Printers dialog box, click Browse and verify that all building printer locations are displayed.
5. Verify that the OU delegation is correct.	a. Verify that the user delegated permission for the Information Services OU can create user accounts for all of the OUs under Information Services. b. Verify that the user delegated permission for the Information Services OU cannot create user accounts under the Human Resources OU.

Tasks	Detailed Steps
6. Verify that the Group Policy objects are configured correctly.	a. Log on as a user under the Human Resources OU and verify that the Cosmo 2 application is not available and the Windows 2000 Support Tools application is available. b. Create a user account in the Messaging OU that is a member of the Contractors group. Then log on as that user and ensure that the Windows 2000 Support Tools application is not available and the Cosmo 2 application is available.
7. Verify that replication is working correctly on all domain controllers.	a. Check the directory service event log. b. Use Replication monitor to verify that connection objects exist between domain controllers.

Course Evaluation

Topic Objective

To direct students to a Web site to complete a course evaluation.

Lead-in

Go to the Web site listed on this page to complete a course evaluation.



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

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

To complete a course evaluation, go to
<http://www.metricsthatmatter.com/survey>.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.