Microsoft®
Training &
Certification

Part I: Managing a Microsoft® Windows® Server 2003 Environment

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 1: Introduction to Administering Accounts and Resources

Contents

Microsoft®

Overview

- Multimedia: Introduction to Managing a Microsoft Windows Server 2003 Environment
- The Windows Server 2003 Environment
- Logging on to Windows Server 2003
- Installing and Configuring Administrative Tools
- Creating an Organizational Unit
- Moving Domain Objects

Introduction

In this module, you will learn the skills and knowledge that you need to administer accounts and resources on computers running Microsoft® Windows® Server 2003 software in a networked environment. These lessons provide information and procedures that you will use throughout the course.

Objectives

After completing this module, you will be able to:

- Describe the Windows Server 2003 environment.
- Log on to a computer running Windows Server 2003.
- Install and configure the administrative tools.
- Create an organizational unit.
- Move objects within a domain.

Multimedia: Introduction to Managing a Microsoft Windows Server 2003 Environment

This presentation describes the primary job functions of administering accounts and resources and defines basic concepts of Active Directory
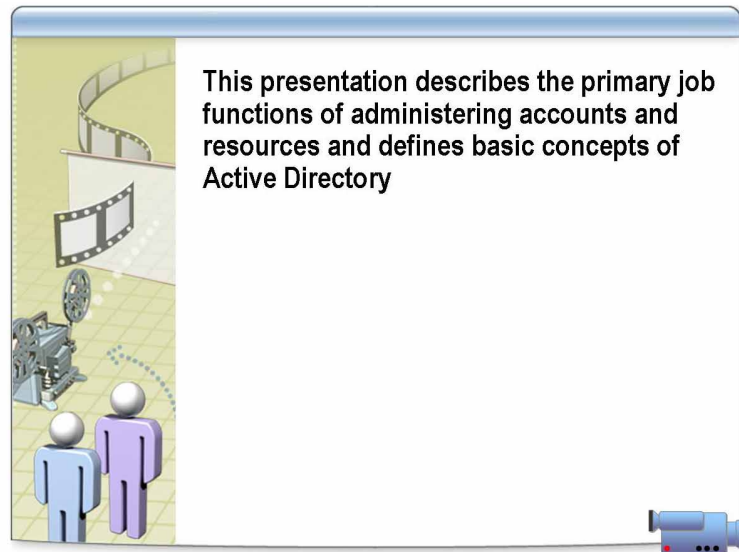
Introduction

In this presentation, you are introduced to the primary job functions of administering accounts and resources in a Windows Server 2003 environment. The tasks and concepts in this presentation are explained in more detail throughout the course.
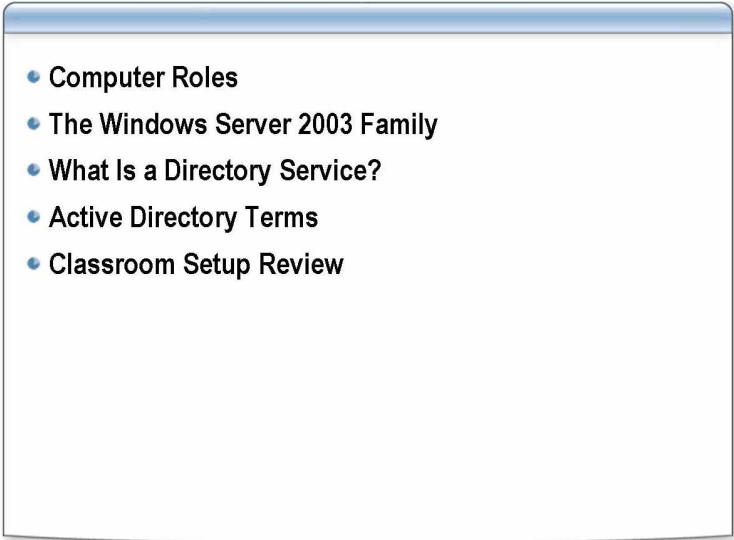
File location

To view the *Introduction to Administering Accounts and Resources* presentation, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

Objective

After completing this lesson, you will be able to describe some common tasks for administering accounts and resources.

Lesson: The Windows Server 2003 Environment

- Computer Roles
- The Windows Server 2003 Family
- What Is a Directory Service?
- Active Directory Terms
- Classroom Setup Review

Introduction

To manage a Windows Server 2003 environment, you must understand which operating system edition is appropriate for different computer roles. You must also understand the purpose of a directory service and how Active Directory® directory service provides a structure for the Windows Server 2003 environment.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the different computer roles in a Windows Server 2003 environment.
- Describe the uses of the different editions of Windows Server 2003.
- Explain the purpose of a directory service.
- Differentiate between the components of an Active Directory structure.

Computer Roles
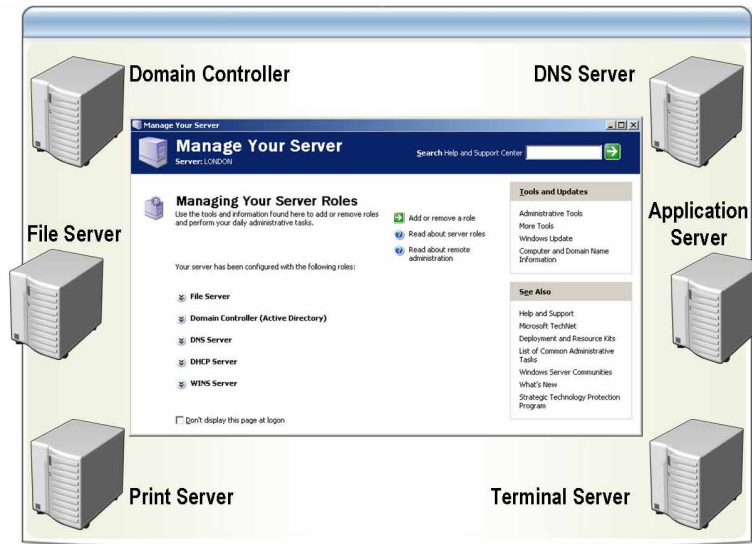
Introduction

Servers play many roles in the client/server networking environment. Some servers are configured to provide authentication, and others are configured to run applications. Some provide network services that enable users to communicate or find other servers and resources in the network. As a systems administrator, you are expected to know the primary types of servers and what functions they perform in your network.

Domain controller (Active Directory)

Domain controllers store directory data and manage communication between users and domains, including user logon processes, authentication, and directory searches. When you install Active Directory on a computer running Windows Server 2003, the computer becomes a domain controller.

Note In a Windows Server 2003 network, all servers in the domain that are not domain controllers are called *member servers*. Servers not associated with a domain are called *workgroup servers*.

File server

A file server provides a central location on your network where you can store and share files with users across your network. When users require an important file such as a project plan, they can access the file on the file server instead of passing the file between their separate computers.

Print server

A print server provides a central location on your network where users can print. The print server provides clients with updated printer drivers and handles all print queuing and security.

DNS server

Domain Name System (DNS) is an Internet and TCP/IP standard name service. The DNS service enables client computers on your network to register and resolve DNS domain names. A computer configured to provide DNS services on a network is a DNS server. You must have a DNS server on your network to implement Active Directory.

Application server

An application server provides key infrastructure and services to applications hosted on a system. Typical application servers include the following services:

- Resource pooling (for example, database connection pooling and object pooling)
- Distributed transaction management
- Asynchronous program communication, typically through message queuing
- A just-in-time object activation model
- Automatic Extensible Markup Language (XML) Web Service interfaces to access business objects
- Failover and application health detection services
- Integrated security

Microsoft Internet Information Services (IIS) provides the tools and features necessary to easily manage a secure Web server. If you plan to host Web and File Transfer Protocol (FTP) sites with IIS, configure the server as an application server.

Terminal server

A terminal server provides remote computers with access to Windows-based programs running on Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition. With a terminal server, you install an application at a single point on a single server. Multiple users then can access the application without installing it on their computers. Users can run programs, save files, and use network resources all from a remote location, as if these resources were installed on their own computer.

The Manage Your Server tool

When Windows Server 2003 is installed and a user logs on for the first time, the Manage Your Server tool starts automatically. You use this tool to add or remove server roles. When you add a server role to the computer, the Manage Your Server tool adds this server role to the list of available, configured server roles. After the server role is added to the list, you can use various wizards that help you manage the specific server role. The Manage Your Server tool also provides Help files specific to the server role that have checklists and troubleshooting recommendations.

The Windows Server 2003 Family

Windows Server 2003 Web Edition	**Use for Web servers**
Windows Server 2003 Standard Edition	**Use for small businesses and departments as domain controllers and member servers**
Windows Server 2003 Enterprise Edition	**Use for medium and large organizations as application servers and domain controllers, and for clustering**
Windows Server 2003 Datacenter Edition	**Use for mission-critical solutions for databases, enterprise resource planning software, high-volume real-time transaction processing, and server consolidation**

Introduction

Windows Server 2003 is available in five editions. Each edition is developed to be used in a specific server role. This enables you to select the operating system edition that provides only the functions and capabilities that your server needs.

Web Edition

Windows Server 2003, Web Edition, is designed to be used specifically as a Web server. It is available only through selected partner channels and is not available for retail. Although computers running Windows Server 2003, Web Edition, can be members of an Active Directory domain, you cannot run Active Directory on Windows Server 2003, Web Edition.

Standard Edition

Windows Server 2003, Standard Edition, is a reliable network operating system that delivers business solutions quickly and easily. This flexible server is the ideal choice for small businesses and departmental use. Use Windows Server 2003, Standard Edition, when your server does not require the increased hardware support and clustering features of Windows Server 2003, Enterprise Edition.

Enterprise Edition

Windows Server 2003, Enterprise Edition, has all the features in Windows Server 2003, Standard Edition. However, it also has features not included in Standard Edition that enhance availability, scalability, and dependability.

Windows Server 2003, Enterprise Edition, is designed for medium to large businesses. It is the recommended operating system for applications, XML Web services, and infrastructure, because it offers high reliability, performance, and superior business value.

The major difference between Windows Server 2003, Enterprise Edition, and Windows Server 2003, Standard Edition, is that Enterprise Edition supports high-performance servers. Windows Server 2003, Enterprise Edition, is recommended for servers running applications for networking, messaging, inventory and customer service systems, databases, and e-commerce Web sites. Also, you can cluster servers running Enterprise Edition together to handle larger loads.

Datacenter Edition

Windows Server 2003, Datacenter Edition, is designed for business-critical and mission-critical applications that demand the highest levels of scalability and availability.

The major difference between Windows Server 2003, Datacenter Edition, and Windows Server 2003, Enterprise Edition, is that Datacenter Edition supports more powerful multiprocessing and greater memory. In addition, Windows Server 2003, Datacenter Edition, is available only through the Windows Datacenter Program offered to Original Equipment Manufacturers (OEMs).

Additional reading

For detailed information about each edition's capabilities, see the product overviews on the Windows Server 2003 page at http://www.microsoft.com/windowsserver2003/default.mspx.

What Is a Directory Service?
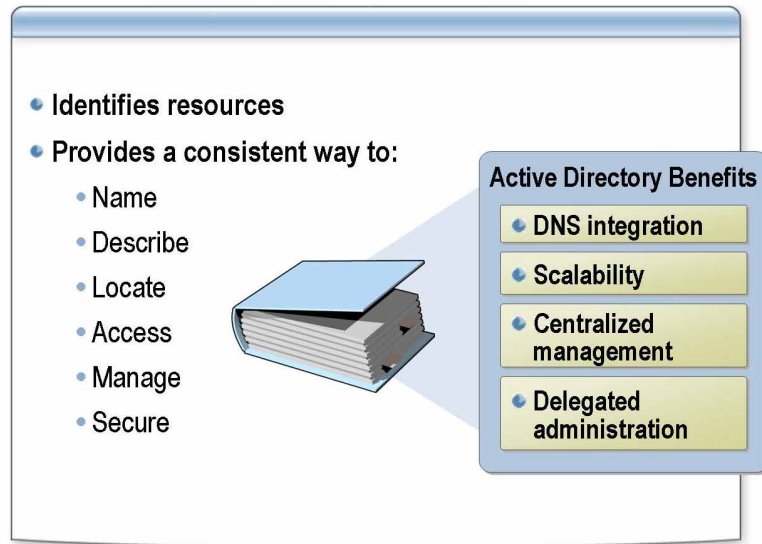
Introduction

As a user logged on to a network, you might need to connect to a shared folder or send a print job to a printer on the network. How do you find that folder and printer and other network resources?

Definition

A directory service is a network service that identifies all resources on a network and makes that information available to users and applications. Directory services are important, because they provide a consistent way to name, describe, locate, access, manage, and secure information about these resources.

When a user searches for a shared folder on the network, it is the directory service that identifies the resource and provides that information to the user.

Active Directory

Active Directory is the directory service in the Windows Server 2003 family. It extends the basic functionality of a directory service to provide the following benefits:

■ DNS integration

Active Directory uses DNS naming conventions to create a hierarchical structure that provides a familiar, orderly, and scalable view of network connections. DNS is also used to map host names, such as microsoft.com, to numeric TCP/IP addresses, such as 192.168.19.2.

■ Scalability

Active Directory is organized into sections that permit storage for a very large number of objects. As a result, Active Directory can expand as an organization grows. An organization that has a single server with a few hundred objects can grow to thousands of servers and millions of objects.

■ Centralized management

Active Directory enables administrators to manage distributed desktops, network services, and applications from a central location, while using a consistent management interface. Active Directory also provides centralized control of access to network resources by enabling users to log on only once to gain full access to resources throughout Active Directory.

■ Delegated administration

The hierarchical structure of Active Directory enables administrative control to be delegated for specific segments of the hierarchy. A user authorized by a higher administrative authority can perform administrative duties in their designated portion of the structure. For example, users may have limited administrative control over their workstation's settings, and a department manager may have the administrative rights to create new users in an organizational unit.

Additional reading

For more information on Active Directory, see *Technical Overview of Windows Server 2003 Active Directory* at http://www.microsoft.com/ windowsserver2003/techinfo/overview/activedirectory.mspx.

Active Directory Terms
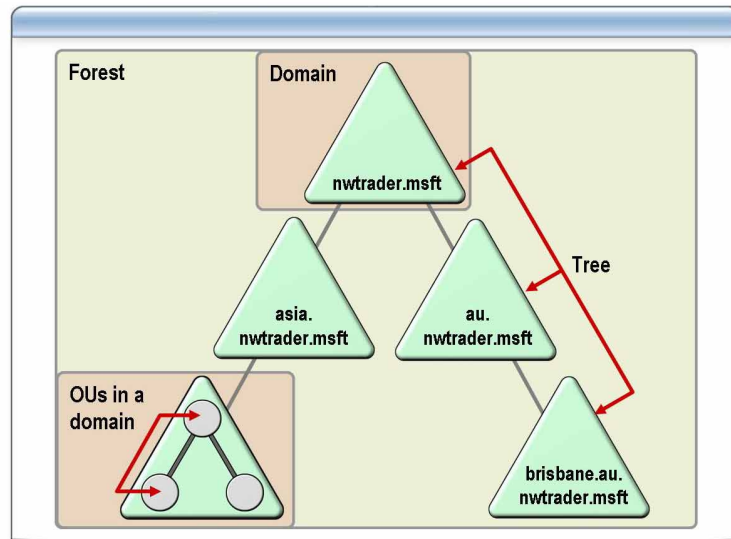
Introduction

The logical structure of Active Directory is flexible and provides a method for designing a hierarchy within Active Directory that is comprehensible to both users and administrators.

Logical components

The logical components of the Active Directory structure include the following:

- *Domain*. The core unit of the logical structure in Active Directory is the domain. A domain is a collection of computers, defined by an administrator, that share a common directory database. A domain has a unique name and provides access to the centralized user accounts and group accounts maintained by the domain administrator.

- *Organizational unit*. An organizational unit is a type of container object that you use to organize objects within a domain. An organizational unit may contain objects, such as user accounts, groups, computers, printers, and other organizational units.

- *Forest*. A forest is one or more domains that share a common configuration, schema, and global catalog.

- *Tree*. A tree consists of domains in a forest that share a contiguous DNS namespace.

Additional reading

For more information about Active Directory domains, see:

- Article 310996, "Active Directory Services and Windows 2000 or Windows Server 2003 Domains (Part 1)" in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=310996.

- Article 310997, "Active Directory Services and Windows 2000 or Windows Server 2003 Domains (Part 2)" in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=310997.

Classroom Setup Review

- The classroom is configured as one Windows Server 2003 domain: nwtraders.msft
- London is a domain controller and the instructor computer
- Glasgow is a member server and is used as a remote computer for student labs
- Student computers are running Windows Server 2003, Enterprise Edition
- Each student computer has an organizational unit
- Students are administrators for their server and organizational unit

Introduction

Now that you have been introduced to the basic components of an Active Directory structure, you can understand the setup of the classroom better.

Classroom setup

The classroom configuration consists of one domain controller and multiple student computers. Each computer is running Windows Server 2003, Enterprise Edition.

The name of the domain is nwtraders.msft. It is named after Northwind Traders, a fictitious company that has offices worldwide. The names of the computers correspond with the names of the cities where the fictitious offices are located.

The domain controller is named London, and the instructor also has a member server called Glasgow. The student computers are named after various cities, such as Acapulco, Bonn, and Casablanca. The name of each computer corresponds with an organizational unit of the same name. For example, the Acapulco computer is part of the Acapulco organizational unit.

The domain has been prepopulated with users, groups, and computer accounts for each administrator to manage.

Lesson: Logging on to Windows Server 2003

- Multimedia: Logon and Authentication
- Logon Dialog Box Options
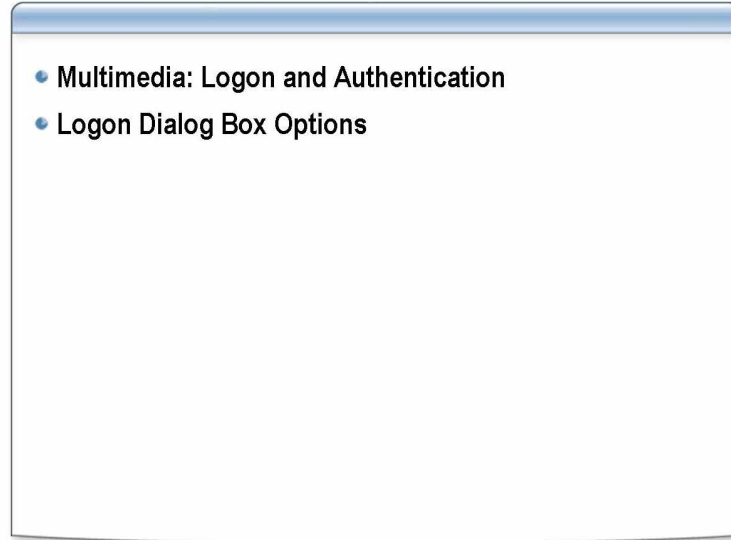
Introduction

Windows Server 2003 authenticates a user during the logon process to verify the identity of the user. This mandatory process ensures that only valid users can access resources and data on a computer or the network.

Lesson objectives

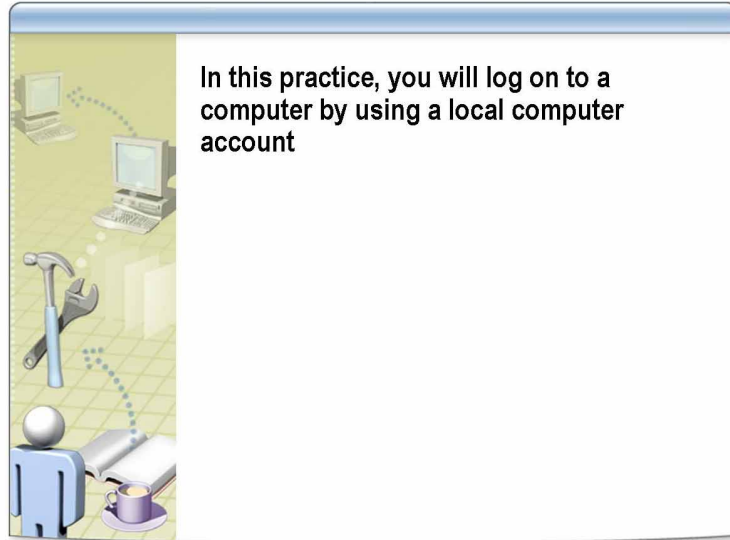After completing this lesson, you will be able to:

- Log on locally.
- Log on to a domain.

Practice: Logging on Using a Local Computer Account

In this practice, you will log on to a computer by using a local computer account

Objective

In this practice, you will log on to a computer by using a local computer account.

Scenario

You have just been hired by Northwind Traders to help with the administration of computers, users, and resources for a city location in the Northwind Traders global network. You will also be responsible for a member server in your city and will occasionally log on with the local Administrator account on the member server.

Practice

► **Log on to your member server by using the local Administrator account**

1. Press CTRL+ALT+DEL.

2. In the **Log On to Windows** dialog box, in the **User name** box, type **Administrator**

3. In the **Password** box, type **P@ssw0rd** (The 0 is a zero).

4. In the **Log on to** box, click the name of your computer.

   The name of your computer has **(this computer)** after your computer name.

5. Click **OK**.

6. Log off the computer by doing the following:

   a. On the **Start** menu, click **Log Off**.

   b. In the message box, click **Log Off**.

Multimedia: Logon and Authentication

This activity presents information about:
- Local logon process
- Domain logon process
- Secondary logon process
- Smart card logon process

Important points to look for:
- Difference between local and domain authentication
- How to perform a secondary logon
- Contents of an access token
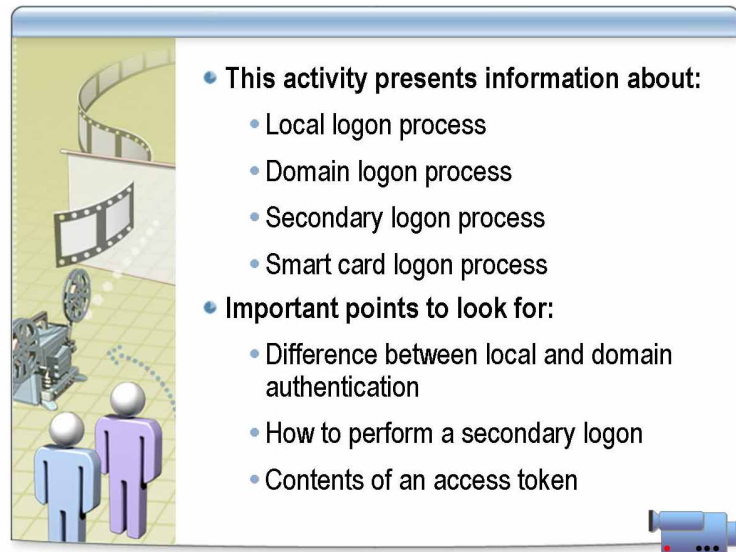
File location

To start the *Logon and Authentication* activity, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the activity.

Questions

Review the information and processes in *Logon and Authentication*, and then answer the following questions.

1. What is the difference between authentication of a local logon and authentication of a domain logon?

   _____

   _____

   _____

2. How do you perform a secondary logon?

   _____

   _____

   _____

3. What type of information is contained in an access token?

     _____

     _____

     _____

Logon Dialog Box Options

By default, Windows Server 2003 assumes the user wants to log on to the domain that the computer is a member of

Select the domain where the user account is located
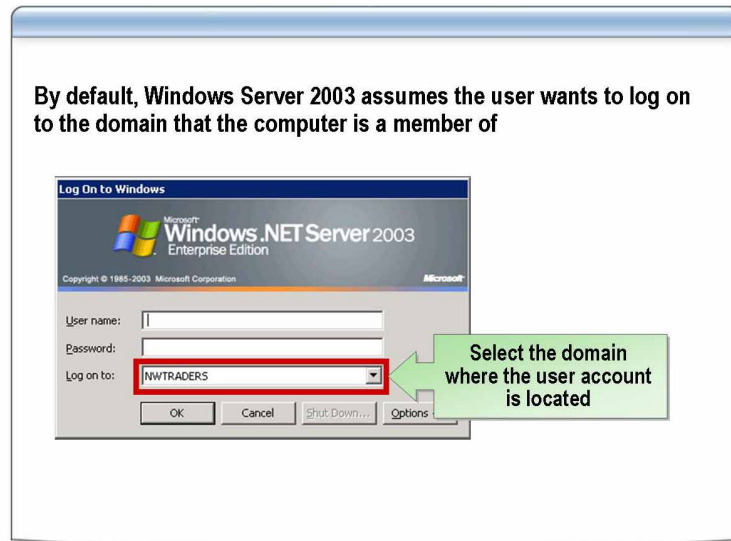
Introduction

Windows Server 2003 provides two options when a user logs on to a domain. Windows Server 2003 enables the user to specify the domain that contains their user account from a computer that is located in a different domain. By default, Windows Server 2003 assumes that the user wants to log on to the domain that the computer is a member of and does not provide a way to specify a domain.

The logon dialog box

The following table describes all the options in the logon dialog box.

Option	Description
User name	A unique user logon name that is assigned by an administrator. To log on to a domain, this user account must reside in the directory database in Active Directory.
Password	The password that is assigned to the user account. Users must enter a password to prove their identity.
	Passwords are case sensitive. The password appears on the screen as asterisks (*) to protect it from onlookers. To prevent unauthorized access to resources and data, users must keep passwords secret.
Log on to	Determines whether a user logs on to a domain or logs on locally. A user can choose one of the following:
	• **Domain name**: The user must select the domain that their user account is in. This list contains all of the domains in a domain tree.
	• **Computer name**: The name of the computer that the user is logging on to. The user must have the Log on Locally user right for the computer. The option to log on locally is not available on a domain controller.
Log on using dial-up connection	Permits a user to connect to a server in the domain by using a dial-up network connection. Dial-up networking enables a user to log on and perform work from a remote location.
Shutdown	Closes all files, saves all operating system data, and prepares the computer so that a user can safely turn it off. On a computer running Windows Server 2003, the **Shutdown** button is not active. This prevents an unauthorized user from using this dialog box to shut down the server. To shut down a server, a user must be able to log on to it.
Options	Switches between the two versions of the **Enter Password** dialog box. One of these two dialog boxes provides the **Log on to** option, which enables the user to select a domain or the local computer.

Practice: Logging on Using a Domain Account

In this practice, you will log on by using a domain account
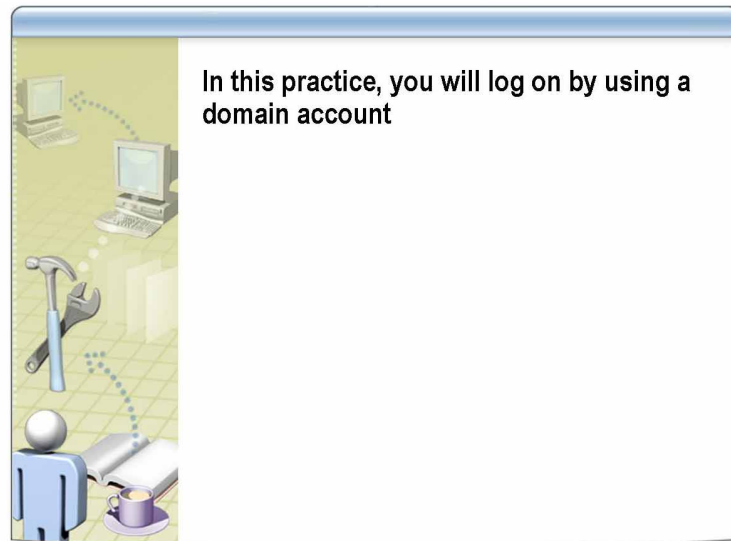
Objective

In this practice, you will log on to a local computer with a domain account.

Scenario
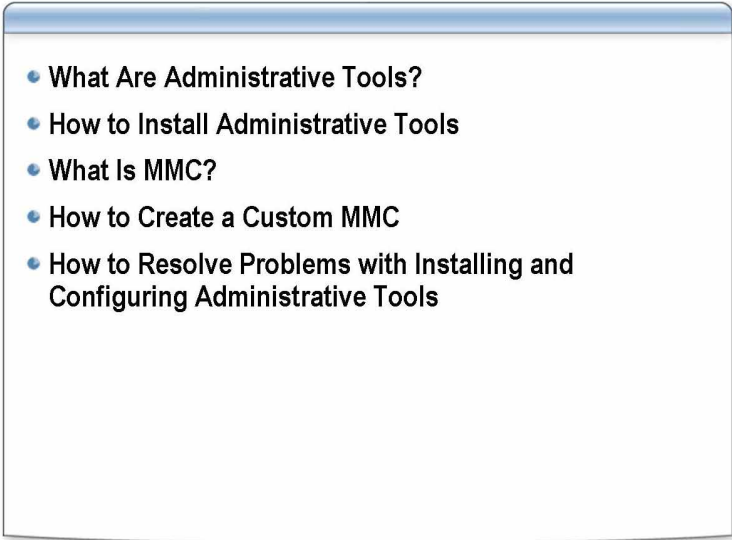
You have just been hired by Northwind Traders to help with the administration of computers, users, and resources for a city location in the Northwind Traders global network. You need to make sure you can successfully log on with your domain Administrator account.

Practice

► **Log on to your member server by using your domain Administrator account**

1. Press CTRL+ALT+DEL.

2. In the **Log On to Windows** box, in the **User name** dialog box, type *ComputerName***Admin** (Example: LondonAdmin).

3. In the **Password** box, type **P@ssw0rd** (The 0 is a zero).

4. In the **Log on to** box, click **NWTraders**, and then click **OK**.

5. Log off the computer by doing the following:

   a. On the **Start** menu, click **Log Off**.

   b. In the message box, click **Log Off**.

Lesson: Installing and Configuring Administrative Tools

- What Are Administrative Tools?
- How to Install Administrative Tools
- What Is MMC?
- How to Create a Custom MMC
- How to Resolve Problems with Installing and Configuring Administrative Tools

Introduction
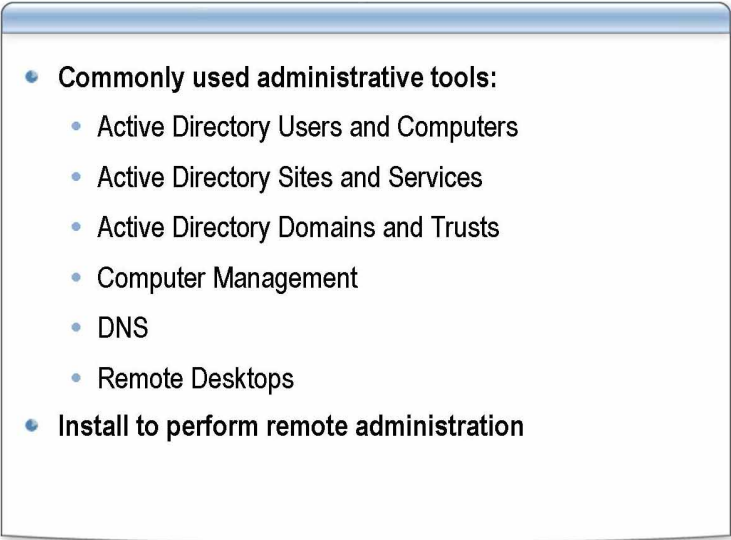
In this lesson, you will learn how to install and configure administrative tools. This lesson also introduces the different types of user accounts and how to create them.

Lesson objectives

After completing this lesson, you will be able to:

- List the most commonly used administrative tools.
- Install administrative tools.
- Describe the Microsoft Management Console (MMC).
- Create a custom MMC.
- Resolve problems with installing and configuring administrative tools.

What Are Administrative Tools?

- **Commonly used administrative tools:**
  - Active Directory Users and Computers
  - Active Directory Sites and Services
  - Active Directory Domains and Trusts
  - Computer Management
  - DNS
  - Remote Desktops
- **Install to perform remote administration**

Introduction

Administrative tools enable network administrators to add, search, and change computer and network settings and Active Directory objects. You can install the administrative tools for managing a Windows Server 2003 environment on computers running Microsoft Windows XP Professional and Windows Server 2003 to remotely administer Active Directory and network settings.

Administrative tools

Some of the more commonly used tools include the following:

- Active Directory Users and Computers
- Active Directory Sites and Services
- Active Directory Domains and Trusts
- Computer Management
- DNS
- Remote Desktops

Installing administrative tools

You will need to install administrative tools on Windows XP Professional when you want to remotely manage network resources such as Active Directory, or network services such as Windows Internet Name Service (WINS) or Dynamic Host Configuration Protocol (DHCP), from a workstation. If you want to install the administrative tools on a computer running Windows XP Professional, Service Pack 1 and a hot fix from Microsoft Knowledge Base article 329357 must be installed.

Windows Server 2003 includes all the administrative tools as snap-ins that can be added to a custom MMC. This includes all the tools for managing Active Directory, but does not include management tools for services that are not installed on the server, such as WINS or DHCP. If you must remotely manage a network service from a computer running Windows Server 2003, and the service is not installed on the computer, you must install the administrative tools.

Note   Uninstall the Windows Server 2003 Administration Tools Pack if someone who is not an administrator is going to use the computer running Windows XP Professional.

How to Install Administrative Tools

Your instructor will demonstrate how to install the
Windows Server 2003 Administration Tools Pack

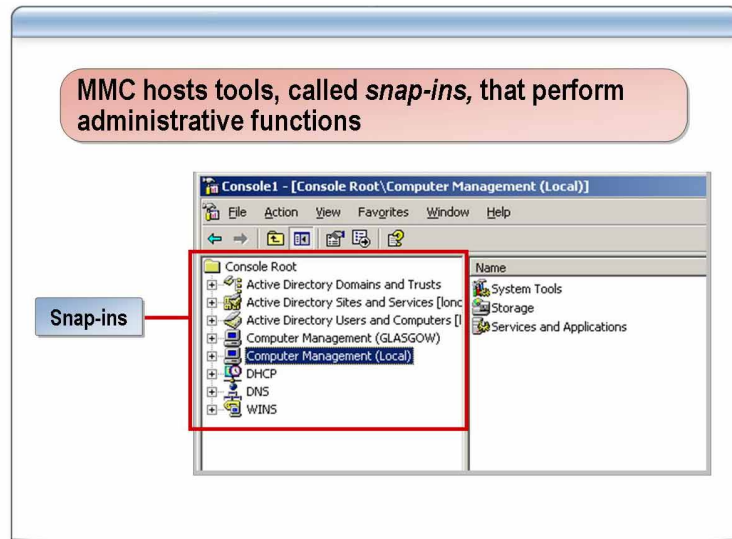...\i386\Adminpak.msi
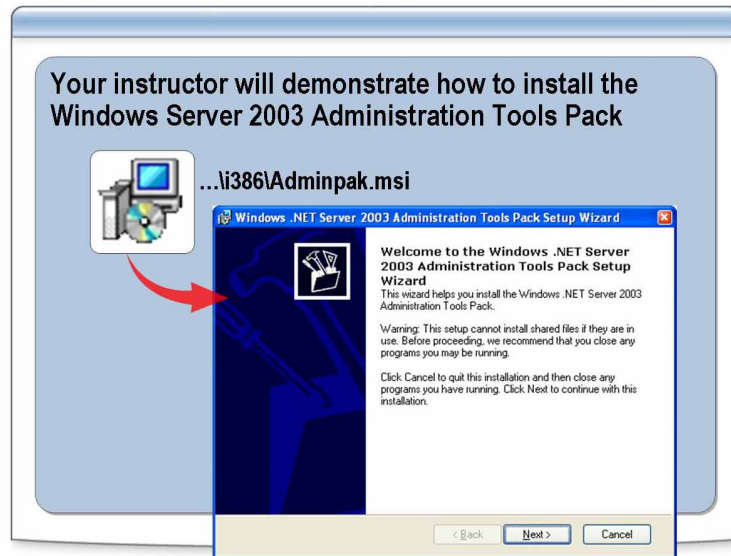
Introduction

To install the Windows Server 2003 Administration Tools Pack on a computer running Windows XP Professional, you must have administrative permissions on the local computer. If the computer is joined to a domain, members of the Domain Administrator group might be able to perform this procedure.

Procedure

To install or reinstall the Windows Server 2003 Administration Tools Pack from the Windows Server 2003 compact disc (CD):

1. Put your Windows Server 2003 CD into the CD tray of a computer running Windows XP Professional.

2. The CD installation setup runs automatically. If it does not:

   a. Click **Start**, and then click **Run**.

   b. In the **Run** dialog box, click **Browse**.

   c. In the **Browse** dialog box, click **My Computer**.

   d. Double-click the CD drive, and then double-click **setup.exe**.

   e. In the **Run** dialog box, click **OK**.

3. In the **Welcome to Microsoft Windows Server 2003** dialog box, click **Perform additional tasks**.

4. In the **What do you want to do?** dialog box, click **Browse this CD**.

5. Double-click the **i386** folder.

6. Double-click the **Adminpak.msi** icon.

7. Specify the installation location or drive where you want to install the Windows Server 2003 Administration Tools Pack.

What Is MMC?

MMC hosts tools, called *snap-ins,* that perform administrative functions

Console1 - [Console Root\Computer Management (Local)]

File   Action   View   Favorites   Window   Help

Console Root
  Active Directory Domains and Trusts
  Active Directory Sites and Services [lonc
  Active Directory Users and Computers [l
  Computer Management (GLASGOW)
  Computer Management (Local)
  DHCP
  DNS
  WINS

Snap-ins

Name
  System Tools
  Storage
  Services and Applications

Definition

You use Microsoft Management Console (MMC) to create, save, and open administrative tools, called consoles, which manage the hardware, software, and network components of your Windows operating system. MMC runs on all client operating systems that are currently supported.
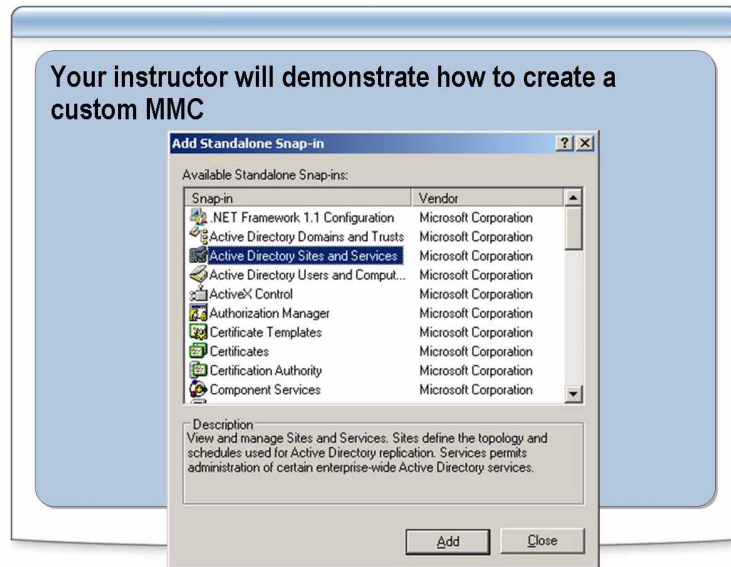
What are snap-ins?

A snap-in is a tool that is hosted in MMC. MMC offers a common framework in which various snap-ins can run so that you can manage several services with a single interface. MMC also enables you to customize the console. By picking and choosing specific snap-ins, you can create management consoles that include only the administrative tools that you need. For example, you can add tools to manage your local computer and remote computers.

Additional reading

For more information about MMC, see *Step-by-Step Guide to the Microsoft Management Console* at http://www.microsoft.com/technet/treeview/ default.asp?url=/technet/prodtechnol/windows2000serv/howto/mmcsteps.asp.

How to Create a Custom MMC

Your instructor will demonstrate how to create a custom MMC

Add Standalone Snap-in

Available Standalone Snap-ins:

Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Comput...	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Authorization Manager	Microsoft Corporation
Certificate Templates	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation

Description
View and manage Sites and Services. Sites define the topology and schedules used for Active Directory replication. Services permits administration of certain enterprise-wide Active Directory services.

[Add]   [Close]

Introduction

You can use MMC to create custom tools and distribute these tools to users. With both Windows XP Professional and Windows Server 2003, you can save these tools so that they are available in the Administrative Tools folder on the Programs menu. To create a custom MMC, you will use the **Run as** command.

Procedure

1. Click **Start**, click **Run**, type **MMC** and then click **OK**.

2. In the console, on the **File** menu, click **Add/Remove Snap-in**.

3. In the **Add/Remove Snap-in** dialog box, click **Add**.

4. In the **Add Standalone Snap-in** dialog box, double-click the item that you want to add.

5. If a wizard appears, follow the instructions in the wizard.

6. To add another item to the console, repeat step 4.

7. In the **Add Standalone Snap-in** dialog box, click **Close**.

8. Click **OK** when you are finished.

9. On the **File** menu, click **Save**.

Practice: Configuring the Administrative Tools
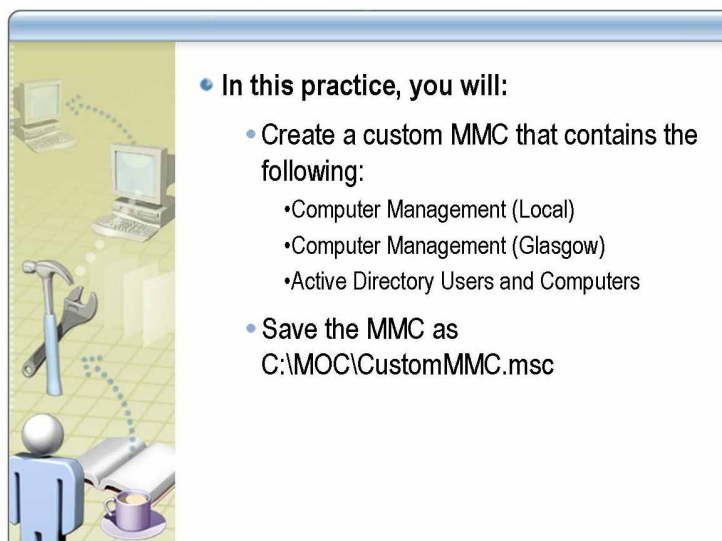
Objective

In this practice, you will:

- Create a custom MMC.
- Add MMC snap-ins.
- Save a custom MMC.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*Admin account.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

Your manager instructs you that you will be adding domain user accounts on the member server that supports your city and an additional server called Glasgow. Configure the support tools so that you have one administrative console that gives you quick access to the tools that you need to do the most common tasks for your job.

Practice

► **Configure a custom MMC**

1. Open a blank MMC.

2. Add a Computer Management snap-in for the local computer.

3. Add a Computer Management snap-in for Glasgow.

4. Add the Active Directory Users and Computers snap-in.

5. Save the MMC as C:\MOC\CustomMMC.msc.

Note   This practice focuses on the concepts in this lesson and as a result may not comply with Microsoft security recommendations. For example, this practice does not comply with the recommendation that users log on with domain user account and use the **Run as** command when performing administrative tasks.

How to Resolve Problems with Installing and Configuring Administrative Tools

Symptom	Cause	Resolution
Cannot install the administrative tools	Insufficient permissions	You must have administrative permissions on the local computer
	Incorrect operating system	You can install the Windows Server 2003 Administration Tools Pack only on currently supported operating systems
Broken links in Help files	Both server and client Help systems are required	Use both Help systems for the Windows Server 2003 Administration Tools Pack by installing the server Help on currently supported client operating systems

Introduction

Two common problems you might encounter when installing and configuring administrative tools are that you cannot install the administrative tools properly and that there are broken links in the Help files.

Cannot install

If you have problems installing or configuring administrative tools in Windows Server 2003, verify that you have administrative permissions on the local computer.

Another reason you may not be able to install the administrative tools is that the incorrect operating system is installed. You can only install the Windows Server 2003 Administration Tools Pack on computers running Windows XP Professional or Windows Server 2003.

Broken Help links

When the Windows Server 2003 Administration Tools Pack is installed on Windows XP Professional, some Help links might appear to be broken. The reason this happens is that you must have both server and client Help files for the Windows Server 2003 Administration Tools Pack on Windows XP Professional.

To resolve the problem, you must integrate the server and client Help files for the Windows Server 2003 Administration Tools Pack by installing the server Help files on Windows XP Professional. This is fairly easy to do and should be done after the Windows Server 2003 Administration Tools Pack is installed on Windows XP Professional.

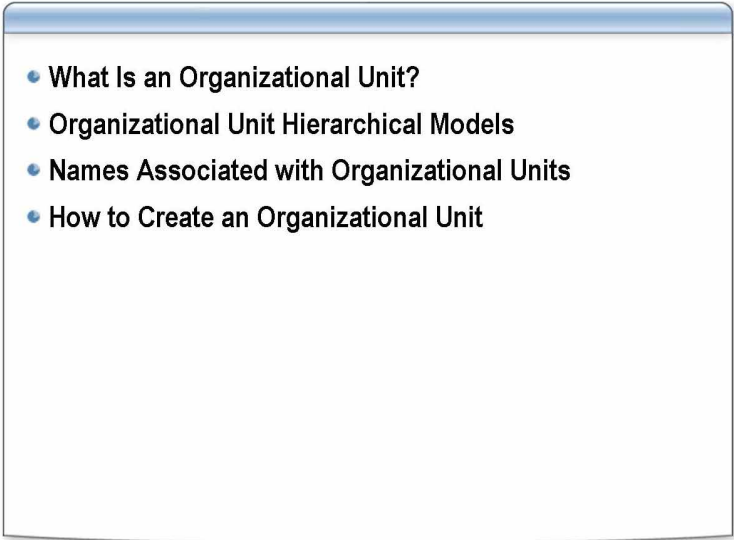To install Help files from another Windows computer, CD, or disk image:

1. On the **Start** menu, click **Help and Support**.

2. In the Help and Support window, in the navigation bar, click **Options**.

3. In the left pane, click **Install and share Windows Help**.

4. In the right pane, depending on where you want to install Help from, click **Install Help content from another Windows computer** or **Install Help content from a CD or disk image**.

5. Type the location of the computer, CD, or disk image, and then click **Find**.

   If you are installing from a CD or disk image, you can click **Browse** to locate the disk containing Help files.

6. When available Help files appear, click the version of Help you want, and then click **Install**.

   When the installation is complete, you can switch to the new Help files.

Lesson: Creating an Organizational Unit

- What Is an Organizational Unit?
- Organizational Unit Hierarchical Models
- Names Associated with Organizational Units
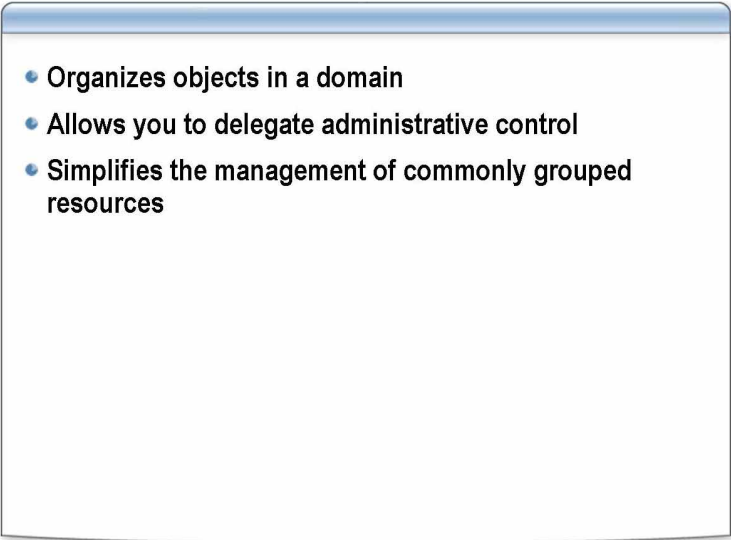- How to Create an Organizational Unit

Introduction

In this lesson, you will learn how to create an organizational unit.

Lesson objectives

After completing this lesson, you will be able to create an organizational unit, including:

- Explain the purpose of an organizational unit.
- Describe organizational unit hierarchical models.
- Identify the names associated with organizational units.
- Create an organizational unit.

What Is an Organizational Unit?

- Organizes objects in a domain
- Allows you to delegate administrative control
- Simplifies the management of commonly grouped resources

Definition

An organizational unit is a particularly useful type of Active Directory object contained in a domain. Organizational units are useful, because you can use them to organize hundreds of thousands of objects in the directory into manageable units. You use an organizational unit to group and organize objects for administrative purposes, such as delegating administrative rights and assigning policies to a collection of objects as a single unit.

Benefits of using organizational units

You can use organizational units to:

- Organize objects in a domain.

    Organizational units contain domain objects, such as user and computer accounts and groups. File and printer shares that are published to Active Directory are also found in organizational units.

- Delegate administrative control.

    You can assign either complete administrative control, such as the Full Control permission, over all objects in the organizational unit, or you can assign limited administrative control, such as the ability to modify e-mail information, over user objects in the organizational unit. To delegate administrative control, you assign specific permissions on the organizational unit and the objects that the organizational unit contains for one or more users and groups.

- Simplify the management of commonly grouped resources.

    You can delegate administrative authority over individual attributes on individual objects in Active Directory, but you will usually use organizational units to delegate administrative authority. A user can have administrative authority for all organizational units in a domain or for a single organizational unit. Using organizational units, you can create containers in a domain that represent the hierarchical or logical structures in your organization. You can then manage the configuration and use of accounts and resources based on your organizational model.

Organizational Unit Hierarchical Models
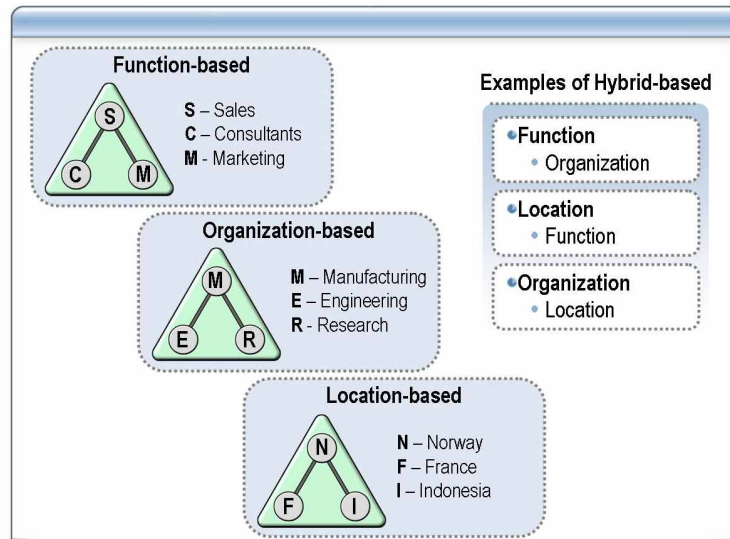
Introduction	As a systems administrator, you do not select the design of the Active Directory structure for your organization. However, it is important to know the characteristics and ramifications of each structure. This knowledge may be critical to you when performing systems administrator tasks within the Active Directory structure. This topic describes the four basic hierarchy designs.
Function-based hierarchy	The function-based hierarchy is based on only the business functions of the organization, without regard to geographical location or departmental or divisional barriers. Choose this approach only if the IT function is not based on location or organization.

When deciding whether to organize the Active Directory structure by function, consider the following characteristics of function-based designs:

- *Not affected by reorganizations*. A function-based hierarchy is not affected by corporate or organizational reorganizations.

- *May require additional layers*. When using this structure, it may be necessary to create additional layers in the organizational unit hierarchy to accommodate the administration of users, printers, servers, and network shares.

- *May impact replication*. Structures that are used to create domains may not result in efficient use of the network, because the domain naming context may replicate across one or more areas of low bandwidth.

This structure is only appropriate in small organizations because functional departments in medium and large organizations are often very diverse and cannot be effectively grouped into broad categories.

Organization-based hierarchy

The organization-based hierarchy is based on the departments or divisions in your organization. If the Active Directory structure is organized to reflect the organizational structure, it may be difficult to delegate administrative authority, because the objects in Active Directory, such as printers and file shares, may not be grouped in a way that facilitates delegation of administrative authority. Because users never see the Active Directory structure, the design should accommodate the administrator instead of the user.

Location-based hierarchy

If the organization is centralized, and network management is geographically distributed, then using a location-based hierarchy is recommended. For example, you may decide to create organizational units for New England, Boston, and Hartford in the same domain, such as contoso.msft.

A location-based organizational units or domain hierarchy has the following characteristics:

- *Not affected by reorganizations*. Although divisions and departments may change frequently, location rarely does change in most organizations.

- *Accommodates mergers and expansions*. If an organization merges with or acquires another company, it is simple to integrate the new locations into the existing organizational units and domain hierarchy structure.

- *Takes advantage of network strengths*. Typically, an organization's physical network topology resembles a location-based hierarchy. If you create domains with a location-based hierarchy, you can take advantage of areas where the network has high bandwidth and limit the amount of data replicated across low bandwidth areas.

- *May cause compromise security*. If a location includes multiple divisions or departments, an individual or group with administrative authority over that domain or over organizational units may also have authority over any child domains or organizational units.

Hybrid-based hierarchy

A hierarchy based on location and then by organization, or any other combination of structure types, is called a hybrid-based hierarchy. The hybrid-based hierarchy combines strengths from several areas to meet the needs of the organization. This type of hierarchy has the following characteristics:

- Accommodates additional growth in geographic, departmental, or divisional areas.

- Creates distinct management boundaries according to department or division.

- Requires cooperation between administrators to ensure the completion of administrative tasks if they are in the same location but in different divisions or departments.

Names Associated with Organizational Units

Name	Example
LDAP relative distinguished name	OU=MyOrganizationalUnit
LDAP distinguished name	OU=MyOrganizationalUnit, DC=microsoft, DC=com
Canonical name	Microsoft.com/MyOrganizationalUnit

Introduction

Each object in Active Directory can be referenced by several different types of names that describe the location of the object. Active Directory creates a relative distinguished name, a canonical name, and a relative distinguished name for each object, based on information that is provided when the object is created or modified.

LDAP relative distinguished name

The Lightweight Directory Access Protocol (LDAP) relative distinguished name uniquely identifies the object in its parent container. For example, the LDAP relative distinguished name of an organizational unit named MyOrganizational Unit is OU=MyOrganizationalUnit. Relative distinguished names must be unique in an organizational unit. It is important to understand the syntax of the LDAP relative distinguished name when using scripts to query and manage Active Directory.

LDAP distinguished name

Unlike the LDAP relative distinguished name, the LDAP distinguished name is globally unique. An example of the LDAP distinguished name of an organizational unit named MyOganizationalUnit in the microsoft.com domain is OU=MyOrganizationalUnit, DC=microsoft, DC=com. Systems administrators use the LDAP relative distinguished name and the LDAP distinguished name only when writing administrative scripts or during command-line administration.

Canonical name

The canonical name syntax is constructed in the same way as the LDAP distinguished name, but it is represented by a different notation. The canonical name of the organizational unit named myOrganizationalUnit in the microsoft.com domain is Microsoft.com/MyOrganizationalUnit. Administrators use canonical names through some administrative tools. It is used to represent a hierarchy in the administrative tools.

How to Create an Organizational Unit

Your instructor will demonstrate how to create an organizational unit
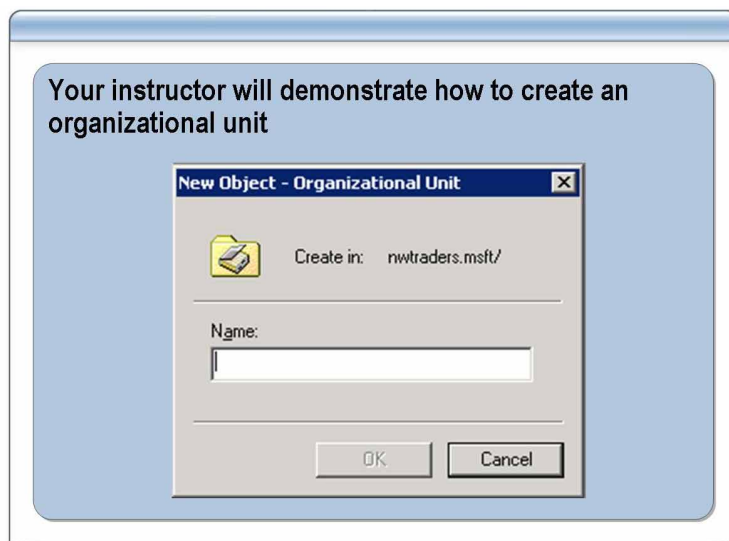
Introduction

You can create organizational units to represent a hierarchy or to manage the objects that go into organizational units.

Procedure

To create a new organizational unit:

1. Open Active Directory Users and Computers.

2. In the console tree, double-click the domain node.

3. Right-click the domain node or the folder in which you want to add the organizational unit, point to **New**, and then click **organizational unit**.

4. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type the name of the organizational unit, and then click **OK**.

Note   To perform this procedure, you must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory, or you must be delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

Using a command line

To create an organizational unit by using **dsadd**:

1. Open a command prompt.

2. Type **dsadd ou** *OrganizationalUnitDomainName* [**-desc** *Description*] [{**-s** *Server* | **-d** *Domain*}] [**-u** *UserName*] [**-p** {*Password* | *****}] [**-q**] [{**-uc** | **-uco** | **-uci**}]

Practice: Creating an Organizational Unit

In this practice, you will create organizational units
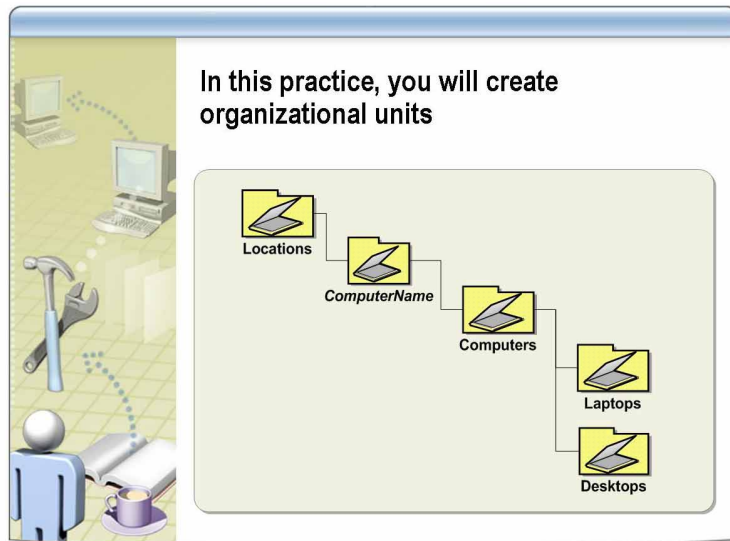
Objective

In this practice, you will create three organizational units.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*Admin account.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

As a systems administrator for Northwind Traders, you are given the task of creating an organizational unit hierarchy designed by the Northwind Traders design team. The organizational unit hierarchy will use a location-based design that separates laptop computers from desktop computers. You will create a hierarchy of organizational units in your city organizational unit to separate computer types.

The following graphic is a representation of what you need to create for the NWTraders domain. The Locations organizational unit and the *ComputerName* organizational unit have already been created.
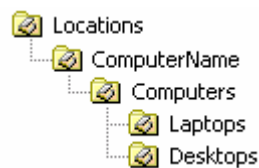
Practice

► **Create the computers, laptops, and desktops organizational units**

1. Open CustomMMC with the **Run as** command.

   Use the following user account: *ComputerName*Admin@nwtraders.msft

2. Expand **Active Directory Users and Computers**.

3. Expand **nwtraders.msft**, and then expand **Locations**.

4. Right-click *CityName*, point to **New**, and then click **organizational unit**.

5. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type **Computers** and then click **OK**.

6. Right-click the **Computers** organizational unit that you just created, point to **New**, then click **organizational unit**.

7. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type **Laptops** and then click **OK**.

8. Right-click the **Computer** organizational unit that you just created, point to **New**, and then click **organizational unit**.

9. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type **Desktops** and then click **OK**.

10. Close and save CustomMMC.

   Your organizational unit hierarchy should look like the preceding diagram.

Scenario

The systems engineers want to test some advanced features of Active Directory. They want your team to create some organizational units in the IT Test organizational unit.

The IT Test organizational unit has already been created. You must add an additional organizational unit that matches your city, as shown in the following graphic.
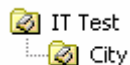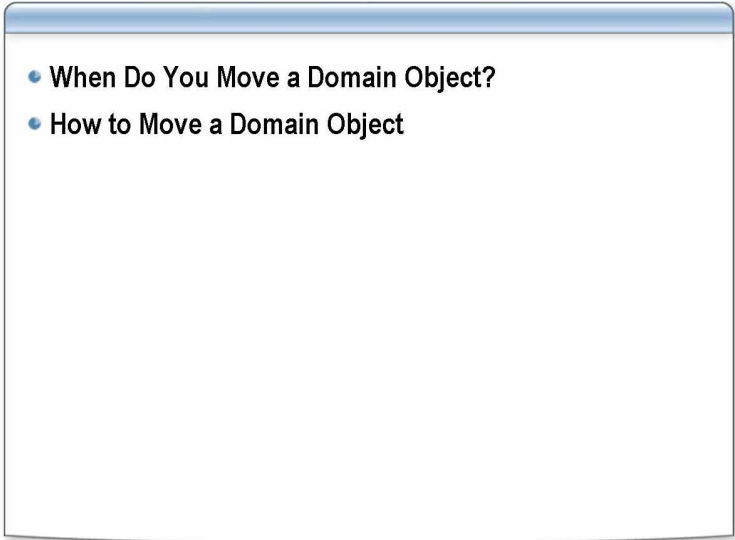

Practice: Using a command line

► **Create an organizational unit by using dsadd**

1. Click **Start**, and then click **Run**.

2. In the **Open** box, type **runas /user:nwtraders***ComputerName***Admin cmd** and then click **OK**

3. When prompted for the password, type **P@ssw0rd** and then press ENTER.

4. At the command prompt, type the following command:

   dsadd ou *OrganizationalUnitDomainName*

   Example: dsadd ou "ou=London,ou=IT Test, dc=nwtraders,dc=msft"

Lesson: Moving Domain Objects

- When Do You Move a Domain Object?
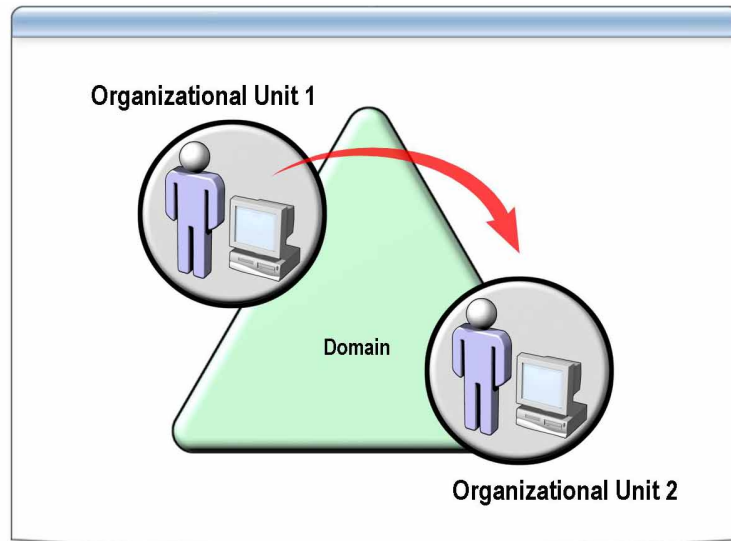- How to Move a Domain Object

Introduction

The information in this lesson presents the skills and knowledge that you need to move domain objects.

Lesson objectives

After completing this lesson, you will be able to:

- List reasons for moving a domain object.
- Move a domain object.

When Do You Move a Domain Object?

Introduction

You can move objects between organizational units in Active Directory when organizational or administrative functions change, for example, when an employee moves from one department to another. As a systems administrator, it is your task to maintain the Active Directory structure as business needs change.

The following items can be moved within the Active Directory structure:

- User account
- Contact account
- Group
- Shared folder
- Printer
- Computer
- Domain controller
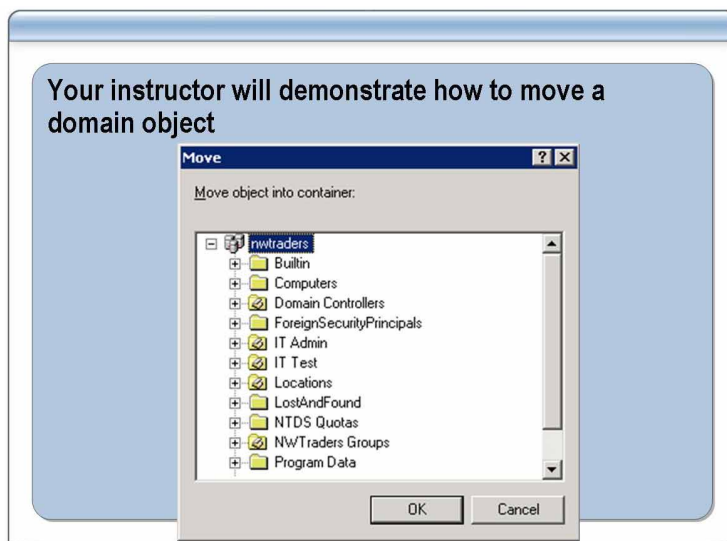- Organizational unit

Change locations

One reason to move a domain object is when your business physically moves from one location to another. If the Active Directory structure is based on geopolitical boundaries, such as city or country, you may need to move objects from one location to another location as objects are physically moved.

Organizational unit restructuring

Another reason to move a domain object is if your Active Directory structure is based on an organizational chart. You may need to move objects if the organizational structure changes.

For example, suppose the Sales team is represented by an organizational unit, the Marketing team is represented by another organizational unit, and both teams are merged into one Sales and Marketing team. In Active Directory, the objects are merged into one organizational unit. To make this process easier, you can select and move multiple domain objects at the same time.

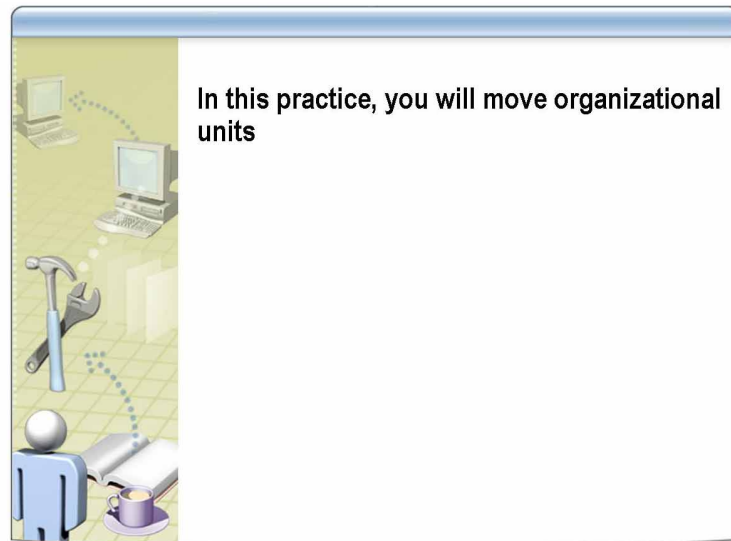# How to Move a Domain Object

Introduction

You can move domain objects either by using the menu option or by dragging the object from one organizational unit to another.

Procedure

To move a domain object:

1. In Active Directory Users and Computers, right-click the object you want to move, and then click **Move**.

   You can also drag the object to the new location.

2. In the **Move** dialog box, browse to the container that you want to move the object to, and then click **OK**.

Practice: Moving Active Directory Domain Objects

In this practice, you will move organizational units

Objective

In this practice, you will move domain objects from one organizational unit to another.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders*ComputerName*Admin (Example: LondonAdmin).
- Ensure that CustomMMC contains Active Directory Users and Computers.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

The systems engineers are testing some advanced reporting functionalities in Active Directory. They want you to create some domain objects and move them from the IT Test organizational unit to an organizational unit named IT Test Move.

Practice

► **Create and move organizational units**

1. Create the following organizational units in the IT Test organizational unit:

   - OU*ComputerName*1
   - OU*ComputerName*2

2. Move them to the IT Test Move organizational unit.

Lab A: Creating Organizational Units

After completing this lab, you will be able to create organizational units
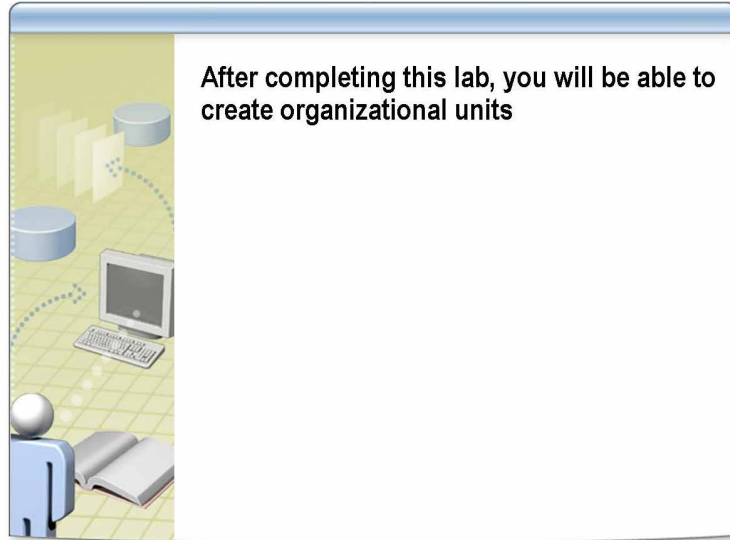
Introduction

After completing this lab, you will be able to create organizational units.

Prerequisites

Before working on this lab, you must have:

- Experience navigating an organizational unit structure in Active Directory Users and Computers.

- Experience creating organizational units.

Lab setup

The Lab Setup section lists the tasks that you must perform before you begin the lab. To complete this lab, you must have reviewed the procedures in the module and successfully completed each practice.

Before you begin this lab:

- Log on to the domain by using the *ComputerName*User account.

- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders*ComputerName*Admin (Example: LondonAdmin).

- Ensure that CustomMMC contains the following snap-ins:

  • Computer Management (Glasgow)

  • Computer Management (Local)

  • Active Directory Users and Computers

Review the procedures in this lesson that describe how to perform this task.

Estimated time to complete this lab: 30 minutes

Exercise 1
Creating an Organizational Unit Hierarchy

In this exercise, you will create an organizational unit hierarchy.

Scenario

As a systems administrator for Northwind Traders, you have been given the task of creating an organizational unit hierarchy designed by the Northwind Traders design team. The organizational unit hierarchy will use a location-based design that separates user and group accounts. You will create the organizational unit hierarchy in your city organizational unit.

At the end of this lab your organizational unit hierarchy should look like the following diagram:
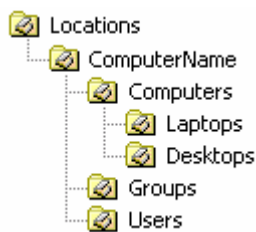
Note You created the Computers, Laptops, and Desktops organizational units that are shown in the graphic in practices.

Tasks	Specific Instructions
1. Open CustomMMC by using the **Run as** command.	▪ User name: **NWTraders***ComputerName***Admin** ▪ Password: **P@ssw0rd**
2. Find the organizational unit that matches your computer name.	▪ Find the Nwtraders/Locations/*ComputerName* organizational unit.
3. Create an organizational unit in your *ComputerName* organizational unit named Users.	▪ Create the Nwtraders/Locations/*ComputerName/*Users organizational unit.
4. Create an organizational unit in your *ComputerName* organizational unit named Groups.	▪ Create the Nwtraders/Locations/*ComputerName*/Groups organizational unit.