Microsoft®
Training &
Certification

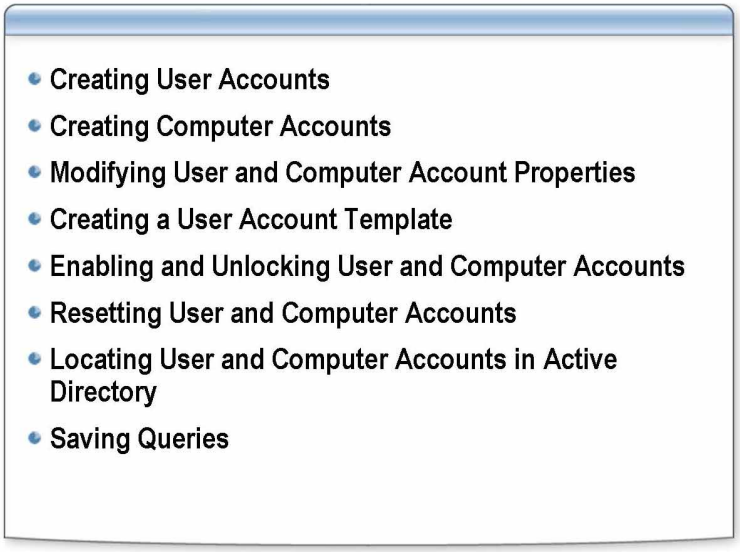
Microsoft® Official
Curriculum

Module 2: Managing User and Computer Accounts

Contents

Microsoft®

Overview



Introduction

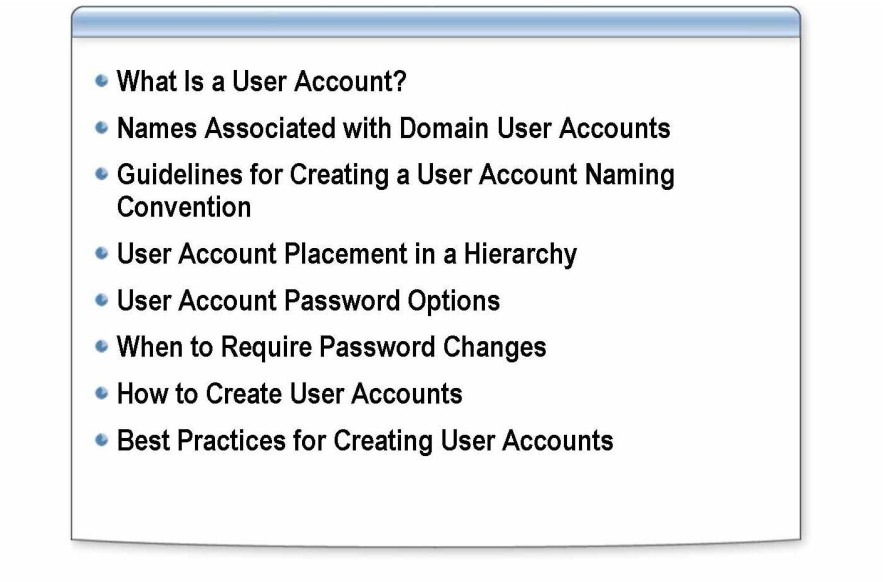
One of your functions as a systems administrator is to manage user and computer accounts. These accounts are Active Directory objects, and you use these accounts to enable individuals to log on to the network and access resources. In this module, you will learn the skills and knowledge that you need to modify user and computer accounts on computers running Microsoft® Windows® Server 2003 in a networked environment.

Objectives

After completing this module, you will be able to:

- Create user accounts.
- Create computer accounts.
- Modify user and computer account properties.
- Create a user account template.
- Enable and unlock user and computer accounts.
- Reset user and computer accounts.
- Locate user and computer accounts in the Active Directory® directory service.
- Save queries.

Lesson: Creating User Accounts



Introduction

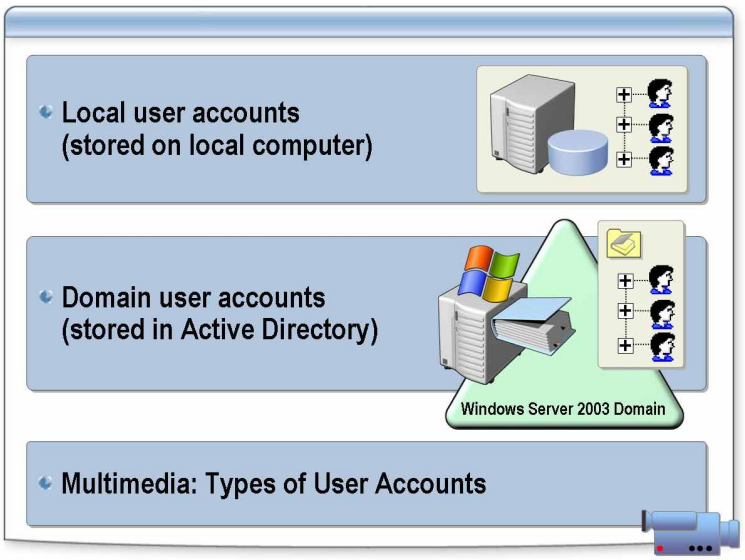
As a systems administrator, you give users access to various network resources. Therefore, you must create user accounts to identify and authenticate the users so that they can gain access to the network.

Lesson objectives

After completing this lesson, you will be able to:

- Explain the purpose of user accounts.
- Describe the types of names associated with domain user accounts.
- Explain guidelines for creating a convention for naming user accounts.
- Describe user account placement in an Active Directory hierarchy.
- Describe user account password options.
- Determine when to require password changes on domain user accounts.
- Create local and domain user accounts.

What Is a User Account?



Definition

A user account is an object that consists of all the information that defines a user in Windows Server 2003. The account can be either a local or domain account. A user account includes the user name and password with which the user logs on, the groups that the user account is a member of, and the user rights and permissions the user has for gaining access to computer and network resources.

You can use a user account to:

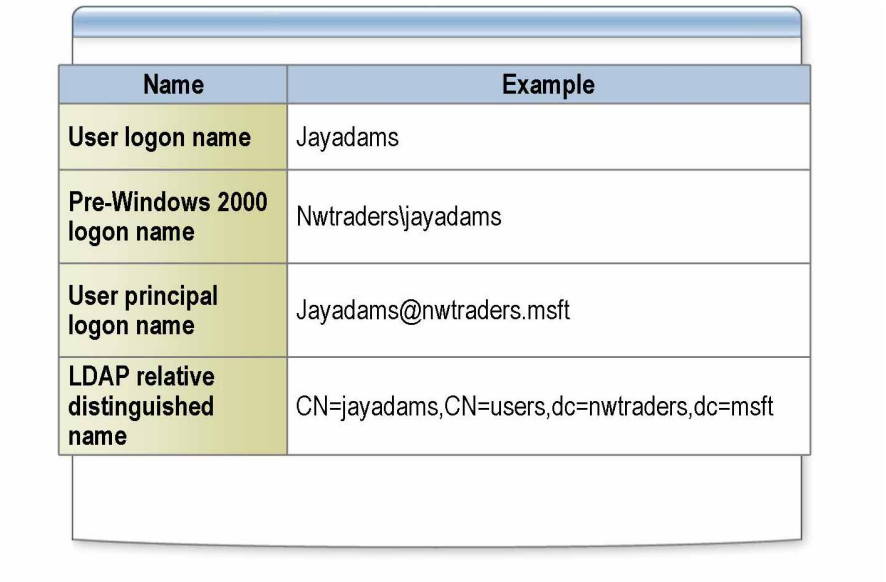
- Enable someone to log on to a computer based on a user account's identity.
- Enable processes and services to run under a specific security context.
- Manage a user's access to resources such as Active Directory objects and their properties, shared folders, files, directories, and printer queues.

Multimedia: Types of User Accounts

To view the *Types of User Accounts* presentation, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

The *Types of User Accounts* presentation explains how using accounts that grant different levels of access to the network satisfy the needs of network users.

Names Associated with Domain User Accounts



Name	Example
User logon name	Jayadams
Pre-Windows 2000 logon name	Nwtraders\jayadams
User principal logon name	Jayadams@nwtraders.msft
LDAP relative distinguished name	CN=jayadams,CN=users,dc=nwtraders,dc=msft

Introduction

There are four types of names associated with domain user accounts. In Active Directory, each user account consists of a user logon name, a pre-Windows 2000 user logon name (Security Accounts Manager account name), a user principal logon name, and a Lightweight Directory Access Protocol (LDAP) relative distinguished name.

User logon name

When creating a user account, an administrator types a user logon name. The full name must be unique in the container in which you create the user account. It is used as the relative distinguished name. Users use this name only during the logon process. The user enters the user logon name, a password, and the domain name in separate fields on the logon screen.

User logon names can:

- Contain up to 20 uppercase and lowercase characters (the field accepts more than 20 characters, but Windows Server 2003 recognizes only 20).
- Include a combination of special and alphanumeric characters, except the following: " / \ [ ] : ; | = , + * ? < >.

An example of a user logon name is Jayadams or Jadams.

Pre-Windows 2000 logon name

You can use the pre-Windows 2000 network basic input/output system (NetBIOS) user account to log on to a Windows domain from computers running pre-Windows 2000 operating systems by using a name with the *DomainName\UserName* format. You can also use this name to log on to Windows domains from computers running Microsoft Windows 2000 or Microsoft Windows XP or servers running Windows Server 2003. The Pre-Windows 2000 logon name must be unique in the domain. Users can use this logon name with the **Run as** command or on a secondary logon screen.

An example of a Pre-Windows 2000 logon name is nwtraders\jayadams.

User principal logon name

The user principal name (UPN) consists of the user logon name and the user principal name suffix, joined by the at sign (@). The UPN must be unique in the forest.

The second part of the UPN is the user principal name suffix. The user principal name suffix can be the Domain Name System (DNS) domain name, the DNS name of any domain in the forest, or an alternative name that an administrator creates only for logon purposes. Users can use this name to log on with the **Run as** command or on a secondary logon screen.

An example of a UPN is Jayadams@nwtraders.msft.

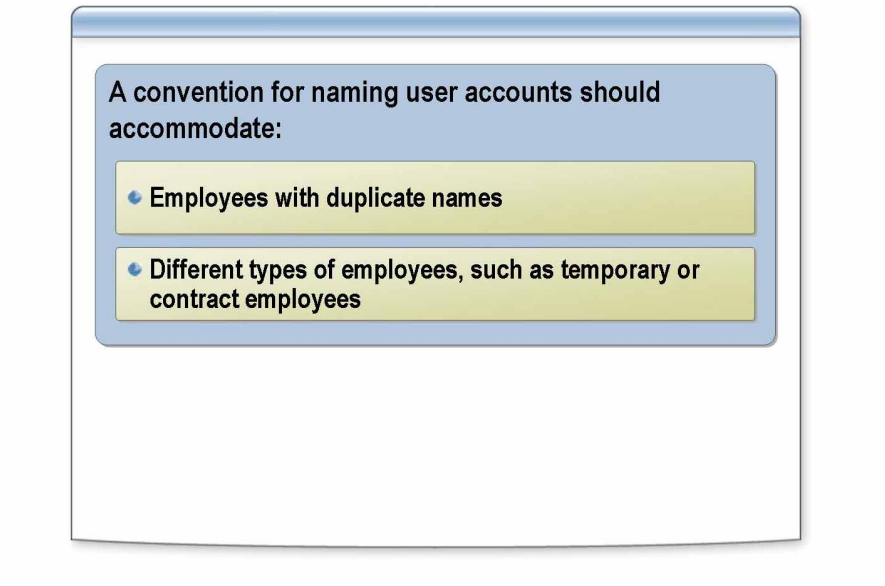
LDAP relative distinguished name

The LDAP relative distinguished name uniquely identifies the object in its parent container. Users never use this name, but administrators use this name to add users to the network from a script or command line. All objects use the same LDAP naming convention, so all LDAP relative distinguished names must be unique in an organizational unit.

The following are examples of an LDAP relative distinguished name:

- CN=jayadams,CN=users,dc=nwtraders,dc=msft
- CN=computer1,CN=users,dc=nwtraders,dc=msft

Guidelines for Creating a User Account Naming Convention



Introduction

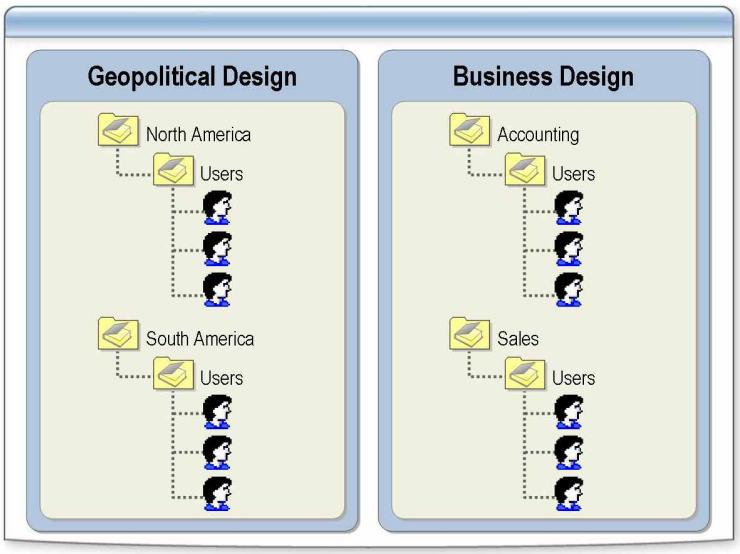
A naming convention establishes how user accounts are identified in the domain. A consistent naming convention makes it easier for you to remember user logon names and locate them in lists. It is a good practice to adhere to the naming convention already in use in an existing network that supports a large number of users.

Guidelines

Consider the following guidelines for creating a naming convention:

- If you have a large number of users, your naming convention for user logon names should accommodate employees with duplicate names. A method to accomplish this is to use the first name and the last initial, and then add additional letters from the last name to accommodate duplicate names. For example, for two users named Judy Lew, one user logon name can be Judyl and the other can be Judyle.
- In some organizations, it is useful to identify temporary employees by their user accounts. To do so, you can add a prefix to the user logon name, such as a T and a hyphen. An example is T-Judyl.
- User logon names for domain user accounts must be unique in Active Directory. Full names for domain user accounts must be unique in the domain in which you create the user account.

User Account Placement in a Hierarchy



Introduction

You can place domain user accounts in any domain in the forest and any organizational unit in the domain. Typically, account hierarchies are based on geopolitical boundaries or business models. By structuring the Active Directory hierarchy and then managing the permissions on the objects and properties in Active Directory, you can precisely specify the accounts that can access information in Active Directory and the level of permissions that they can have.

Place user accounts in an Active Directory hierarchy based on the way the user accounts are managed.

Geopolitical design

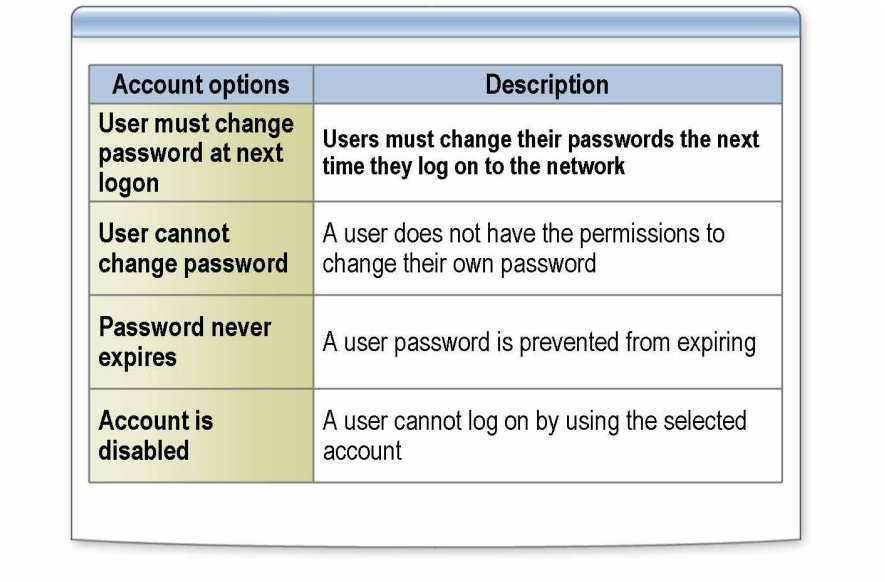
In a geopolitical design, you place users in domains that match their physical location. Geopolitical domain structures place domain controllers that support users of the domain close to the users. This reduces logon times for users and enables users to log on if the wide area network (WAN) is down.

Business design

When the hierarchy of domains is based on business models, you place your sales personnel in a Sales domain and manufacturing personnel in a Manufacturing domain. This model ensures that there are enough domain controllers to support all the users in the WAN.

Note In many cases, one domain will work for a corporate environment. You can still separate administrative control of users by placing them into organizational units.

User Account Password Options



Account options	Description
User must change password at next logon	Users must change their passwords the next time they log on to the network
User cannot change password	A user does not have the permissions to change their own password
Password never expires	A user password is prevented from expiring
Account is disabled	A user cannot log on by using the selected account

Introduction

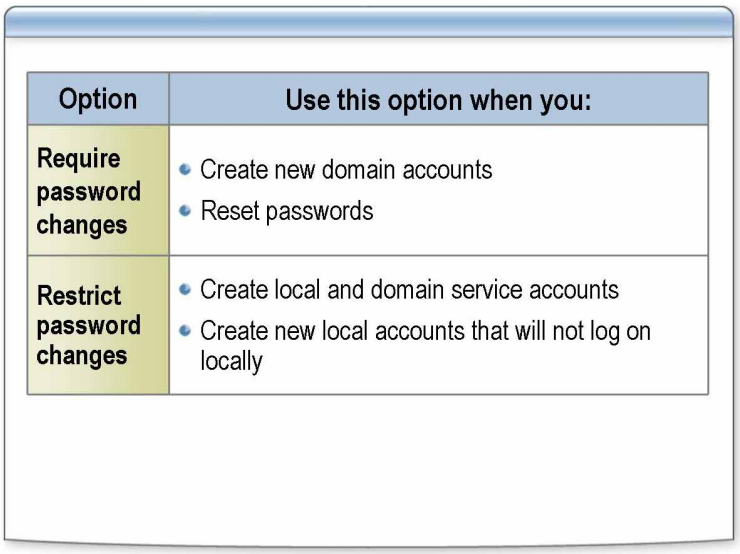
As a systems administrator, you can manage user account password options. These options can be set when the user account is created or in the **Properties** dialog box of a user account.

Password options

The administrator can choose from the following password options to protect access to the domain or a computer:

- **User must change password at the next logon**. This is used when a new user logs on to a system for the first time or when the administrator resets forgotten passwords for users.
- **User cannot change password**. Use this option when you want to control when a user account password can be changed.
- **Password never expires**. This option prevents the password from expiring. As a security best practice, do not use this option.
- **Account is disabled**. This option prevents the user from logging on by using the selected account.

When to Require or Restrict Password Changes



Introduction

To create a more secure environment, require password changes on user accounts and restrict password changes on service accounts. The following table lists when you need to restrict or require password changes.

Password modifications options

Option	Use this option when you:
Require password changes	• Create new domain user accounts. Select the check box that requires the user to change the password the first time the user logs on to the domain. • Reset passwords. This option enables the administrator to reset a password when the password expires or if the user forgets it.
Restrict password changes	• Create local or domain service accounts. Service accounts typically have many dependencies on them. As a result, you may want to restrict the password change policy so that service account passwords are changed by the administrator who is responsible for the applications that depend on the service account. • Create new local accounts that will not log on locally.

Additional Readings

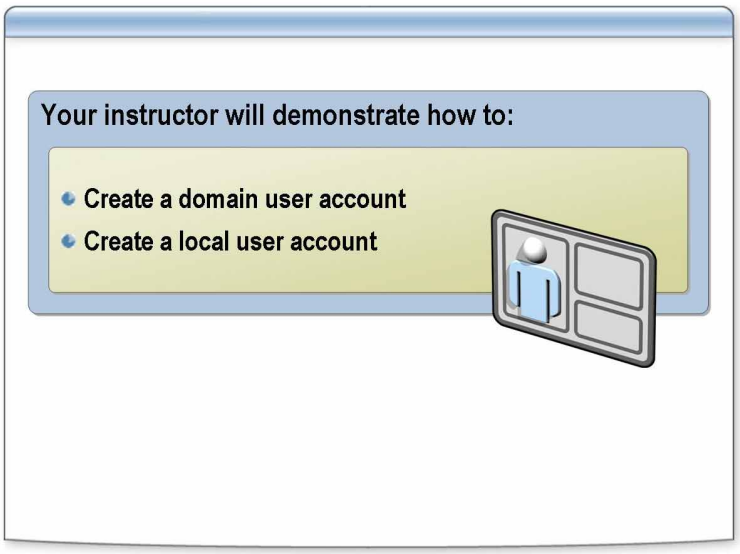
For more information about service accounts, see "Services permissions" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sys_srv_permissions.asp.

Form more information about changing passwords, see:

- Article 324744, "HOW TO: Prevent Users from Changing a Password Except When Required in Windows Server 2003," in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=324744.
- Article 320325, "User May Not Be Able to Change Their Password If You Configure the 'User Must Change Password at Next Logon' Setting," in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=320325.

For more information about preventing passwords of service accounts from being changed, see article 324744, "HOW TO: Prevent Users from Changing a Password Except When Required in Windows Server 2003," in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid= 324744.

How to Create User Accounts



Introduction

Domain user accounts enable users to log on to a domain and access resources anywhere on the network, and local user accounts enable users to log on and access resources only on the computer on which you create the local user account. As a systems administrator, you must create domain and local user accounts to manage your network environment.

Important You cannot create local user accounts on a domain controller.

Procedure for creating a domain user account

To create a domain user account:

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click the domain node.
3. In the details pane, right-click the organizational unit where you want to add the user, point to **New**, and then click **User**.
4. In the **New Object - User** dialog box, in the **First name** box, type the user's first name.
5. In the **Initials** box, type the user's initials.
6. In the **Last name** box, type the user's last name.
7. In the **User logon name** box, type the name that the user will log on with.
8. From the drop-down list, click the UPN suffix that must be appended to the user logon name after the at sign (@).

9. Click **Next**.
10. In the **Password** and **Confirm password** boxes, type the user's password.
11. Select the appropriate password options.
12. Click **Next**, and then click **Finish**.

Procedure for creating a local user account

To create a local user account:

1. Click **Start**, point to Administrative Tools, and then click **Computer Management**.
2. In the console tree, expand **Local Users and Groups**, and then click **Users**.
3. On the **Action** menu, click **New User**.
4. In the **New User** dialog box, in the **User name** box, type the name that the user will log on with.
5. Modify the full name as desired.
6. In the **Password** and **Confirm password** boxes, type the user's password.
7. Select the appropriate password options.
8. Click **Create**, and then click **Close**.

Note A user name cannot be identical to any other user or group name on the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following:

" / \ [ ] : ; | = , + * ? < >

A user name cannot consist solely of periods or spaces.

Using a command line

Another way to create a domain user account is to use the **dsadd** command. The **dsadd user** command adds a single user to the directory from a command prompt or batch file.

To create a user account by using **dsadd user**:

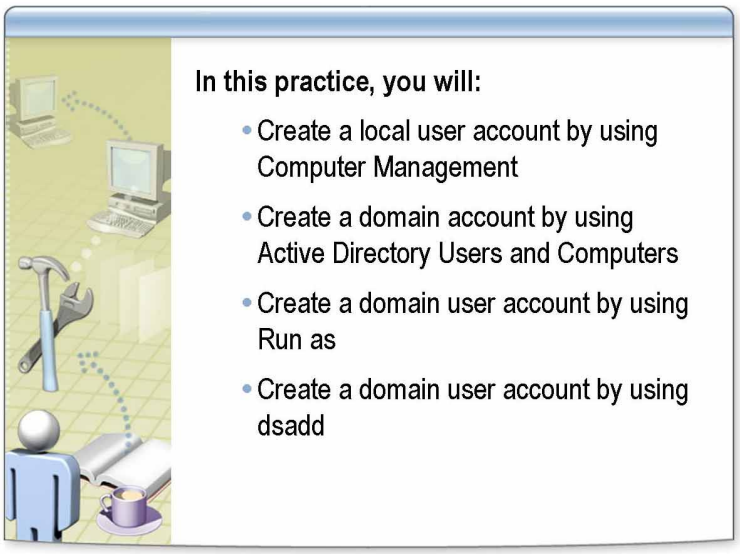
1. Open a command prompt.
2. Type **dsadd user** *UserDomainName* [**-samid** *SAMName*] [**-upn** *UPN*] [**-fn** *FirstName*] [**-ln** *LastName*] [**-display** *DisplayName*] [**-pwd** {*Password*|*****}] Use " " if there is a space in any variable.

Note For the complete syntax of the dsadd user command, at a command prompt, type **dsadd user /?**.

Example of **dsadd user**:

```
dsadd user "cn=testuser,cn=users,dc=nwtraders,dc=msft" –samid
testuser –upn testuser@nwtraders.msft –fn test –ln user –
display "test user" –pwd P@sswOrd
```

Practice: Creating User Accounts



Objective

In this practice, you will:

- Create a local user account by using Computer Management.
- Create a domain account by using Active Directory Users and Computers.
- Create a domain user account by using **Run as**.
- Create a domain user account by using **dsadd**.

Instructions

Before you begin this practice:

- Log on to the student computer 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 (local)
  - Active Directory Users and Computers
- Review the procedures in this lesson that describe how to perform this task.

Scenario

Your manager asks you to create a local user account that will be used to back up your company's software. Another department in your organization will install the software and give the account the user rights needed to back up the server. You must create a local user account to be used as a service account.

Practice: Creating a local user account

► **Create a local user account**

1. Open Computer Management for your local server.
2. Create an account by using the following parameters:
   a. User name: **Service_Backup**
   b. Description: **Service Account for Backup Software**
   c. Password: **P@ssw0rd**
3. Clear the **User must change password at next logon** check box.

Scenario

You will use the Administrator account to perform management tasks. Your company's security practices require that you create a personal user account that you will use to log on to the domain, read and send e-mail, and other nonadministrative tasks.

You must set up a domain user account for yourself. When you need to perform administrative tasks, you will either log on as a different user or use secondary logon credentials. This new account should be created in the nwtraders.msft/IT Admin/IT Users container.

Practice: Creating a domain user account

► **Create a domain user account**

1. Open Active Directory Users and Computers.
2. Add a user account to the IT Users container with the following parameters:
   a. First name: Your first name (Example: Misty)
   b. Last name: Your last name (Example: Shock)
   c. Full name: Your full name (Example: Misty Shock)
   d. User logon name: The first three letters of your first name and the first three letters of your last name (Example: MisSho)
   e. Password: Use a password that:
      - Is at least seven characters long.
      - Does not contain your user name, real name, or company name.
      - Does not contain a complete word that is found in the dictionary.
      - Contains characters from each of the following four groups.

Group	Examples
Uppercase letters	A, B, C ..
Lowercase letters	a, b, c ..
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)	~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] / : " ; ' < > ? , . \

An example of a strong password is J*p2leO4>F.

3. Log off.
4. Test the user account that you just created by logging on by using the user account.
5. Log off.

Scenario

Northwind Traders is in the process of testing advanced features of Active Directory. Your team has the task of creating user accounts in the IT Test organizational unit. The test team will use these accounts. Each member of your team must create five accounts.

Practice: Creating a domain user account using Run as

► **Create a domain user account by using Run as**

1. Log on to the student computer by using the *ComputerName*User account.
2. Open CustomMMC with the **Run as** command.
   - Use the user account Nwtraders*ComputerName*Admin (Example: LondonAdmin).
3. In Active Directory Users and Computers, expand **nwtraders.msft**.
4. Right-click the **IT Test** organizational unit, point to **New**, and then click **User**.
5. Add a user account to the IT Test organizational unit with the following parameters:
   a. First name: **User1**
   b. Last name: Your last name (Example: Shock)
   c. User logon name: **User1** followed by the first three letters of your last name (Example: User1Sho)
   d. Password: **P@ssw0rd**
6. Repeat step 5 and create four more user accounts.

   Example: User2Sho, User3Sho, User4Sho, User5Sho
7. Close all windows.

Scenario

Northwind Traders is in the process of testing advanced features of Active Directory. Your team has the task of creating user accounts in the IT Test organizational unit. The test team will use these accounts. Each member of your team must create five accounts.

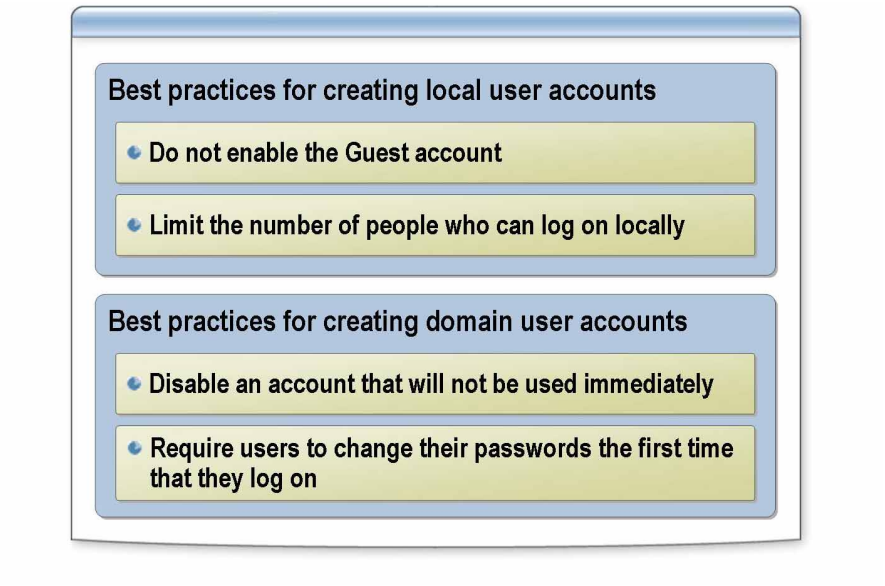
Practice: Using a command line

► **Create a domain user account by using dsadd**

1. Click **Start**, click **Run**, and then type **runas /user:nwtraders***ComputerName***Admin cmd** and then click **OK**.
2. When prompted for the password, type **P@ssw0rd** and then press **ENTER**.
3. At the command prompt, type the following command:

   dsadd user "cn=User6*FirstThreeLettersOfLastName*,**ou=it test,dc=nwtraders,dc=msft" -samid User6***FirstThreeLettersOfLastName* **-pwd** *P@ssw0rd*

Best Practices for Creating User Accounts



Introduction

There are several best practices for creating user accounts that reduce security risks in the network environment. While software products change, review current best practices at www.microsoft.com/security.

Local user accounts

Consider the following best practices when creating local user accounts:

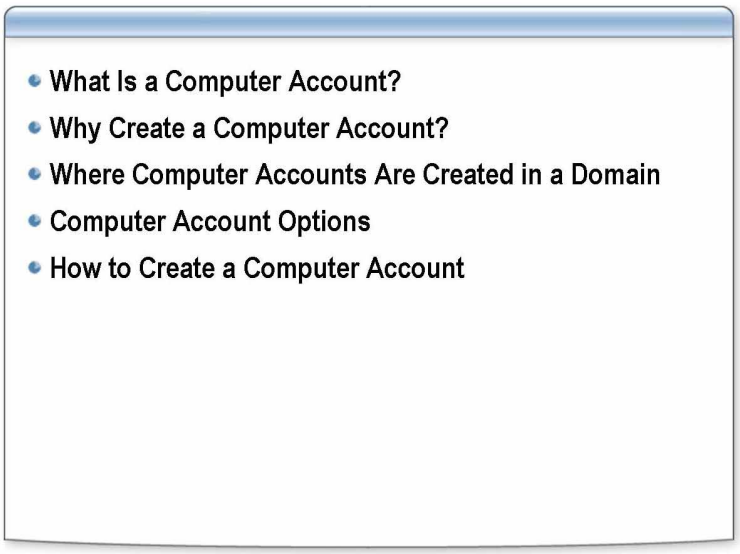
- Do not enable the Guest account.
- Rename the Administrator account.
- Limit the number of people who can log on locally.
- Use strong passwords.

Domain user accounts

Consider the following best practices when creating domain user accounts:

- Disable any account that will not be used immediately.
- Require users to change their passwords the first time that they log on.
- As a security best practice, it is recommended that you do not log on to your computer with administrative credentials.
- When you are logged on to your computer without administrative credentials, it is recommended that you use the **Run as** command to accomplish administrative tasks.
- Rename or disable the Administrator and Guest accounts in each domain to reduce the attacks on your domain.
- By default, all traffic on Active Directory administrative tools is signed and encrypted while in transit on the network. Do not disable this feature.

Lesson: Creating Computer Accounts



Introduction

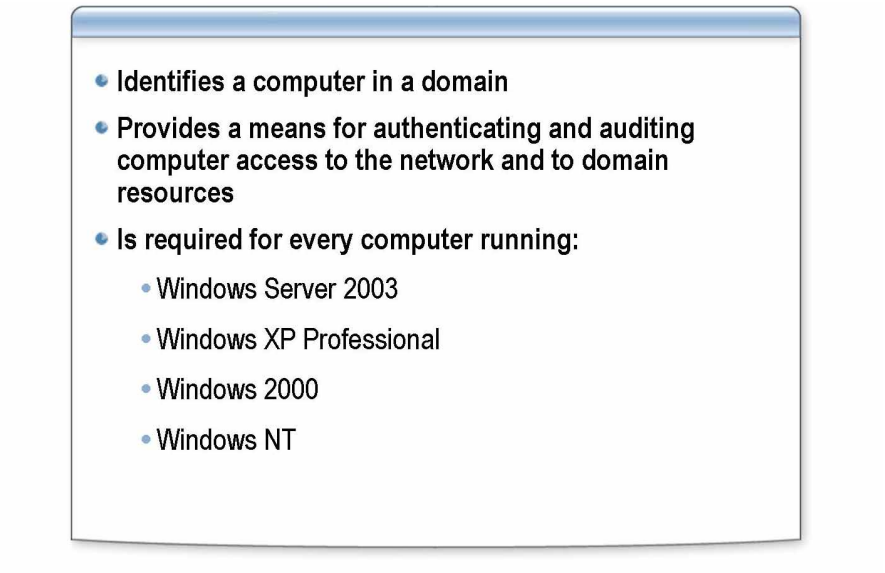
The information in this lesson presents the skills and knowledge that you need to create a computer account.

Lesson objectives

After completing this lesson, you will be able to:

- Define computer account.
- Describe the purpose of computer accounts.
- Describe where computer accounts are created in a domain.
- Describe the various computer account options.
- Create a computer account.

What Is a Computer Account?



Introduction

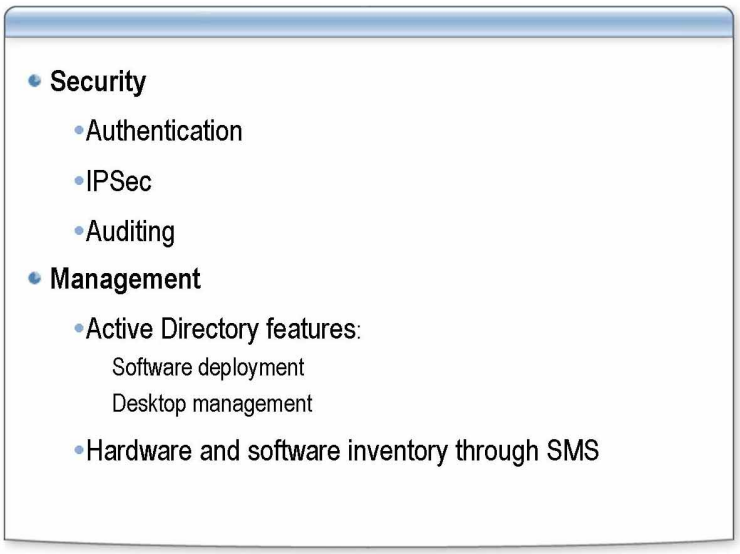
Every computer running Microsoft Windows NT®, Windows 2000, Windows XP, or Windows Server 2003 that joins a domain has a computer account. Similar to user accounts, computer accounts provide a means for authenticating and auditing computer access to the network and to domain resources.

What does a computer account do?

In Active Directory, computers are security principles, just like users. This means that computers must have accounts and passwords. To be fully authenticated by Active Directory, a user must have a valid user account, and the user must also log on to the domain from a computer that has a valid computer account.

Note You cannot create computer accounts for computers running Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows Millennium Edition, and Windows XP Home Edition, because their operating systems do not adhere to Active Directory security requirements.

Why Create a Computer Account?



Introduction

Computers are responsible for performing key tasks, such as authenticating user logons, distributing Internet Protocol (IP) addresses, maintaining the integrity of Active Directory, and enforcing security policies. To have full access to these network resources, computers must have valid accounts in Active Directory. The two main functions of a computer account are performing security and management activities.

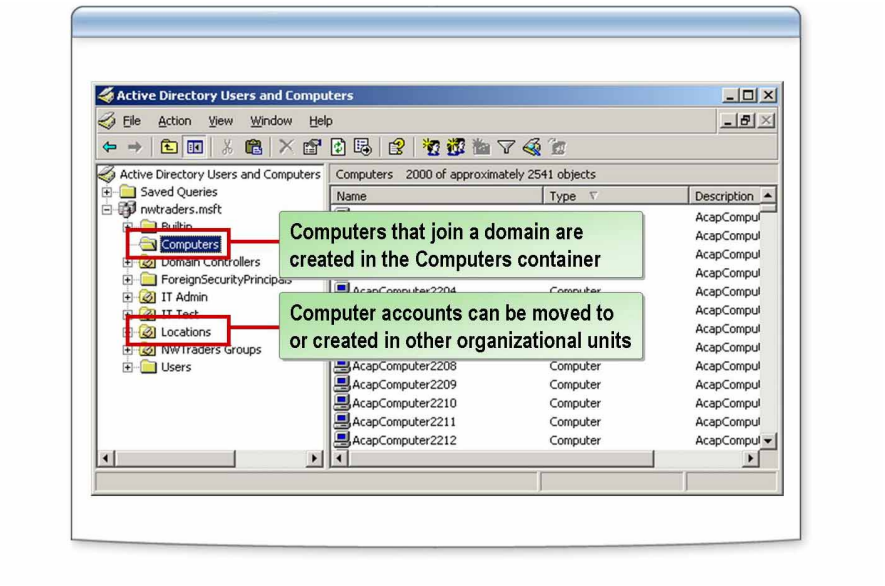
Security

A computer account must be created in Active Directory for users to take full advantage of Active Directory features. When a computer account is created, the computer can use advanced authentication processes such as Kerberos authentication and IP security (IPSec) to encrypt IP traffic. The computer also needs a computer account to dictate how auditing is applied and recorded.

Management

Computer accounts help the systems administrator manage the network structure. The systems administrator uses computer accounts to manage the functionality of the desktop environment, automate the deployment of software by using Active Directory, and maintain a hardware and software inventory by using Microsoft Systems Management Server (SMS). Computer accounts in the domain are also used to control access to resources.

Where Computer Accounts Are Created in a Domain



Introduction

When the systems administrator creates a computer account, they can choose the organizational unit in which to create that account. If a computer joins a domain, the computer account is created in the Computers container, and the administrator can move the account to its proper organizational unit as necessary.

Administrators designate the location of computer accounts

By default, Active Directory users can add up to 10 computers to the domain with their user account credentials. This default configuration can be changed. If the systems administrator adds a computer account directly to Active Directory, a user can join a computer to the domain without using any of the 10 allocated computer accounts.

Pre-staged computer accounts

Adding a computer to the domain with a previously created account is called pre-staging, which means that computers are added to any organizational unit where the systems administrator has permissions to add computer accounts. Usually, users do not have the appropriate permissions to pre-stage a computer account, so as an alternative they join a computer to the domain by using a pre-staged account.

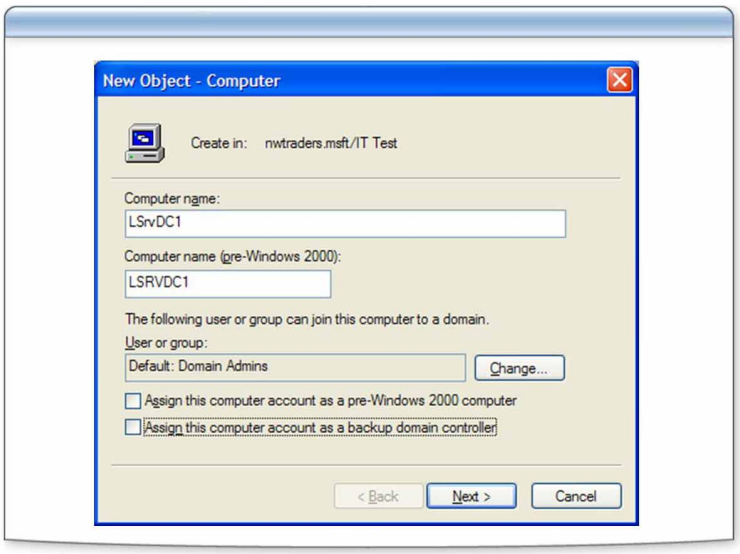
Users designate the location of computer accounts

When a user joins a computer to the domain, the computer account is added to the Computers container in Active Directory. This is accomplished through a service that adds the computer account on behalf of the user. The system account also records how many computers each user has added to the domain. By default, any authenticated user has the user right to add workstations to a domain and can create up to 10 computer accounts in the domain.

Additional reading

For more information about users adding computer accounts to a domain, see article 251335, “Domain Users Cannot Join Workstation or Server to a Domain,” in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=251335.

Computer Account Options



Introduction

There are two optional features that you can enable when creating a computer account. You can assign a computer account as a Pre-Windows 2000 computer or as a backup domain controller (BDC).

Pre-Windows 2000

Select the **Assign this computer account as a pre-Windows 2000 computer** check box to assign a password based on the computer name. If you do not select this check box, a random password is assigned as the initial password for the computer account. The password automatically changes every five days between the computer and the domain where the computer account is located. This option guarantees that a pre-Windows 2000 computer will be able to interpret whether the password meets the password requirements.

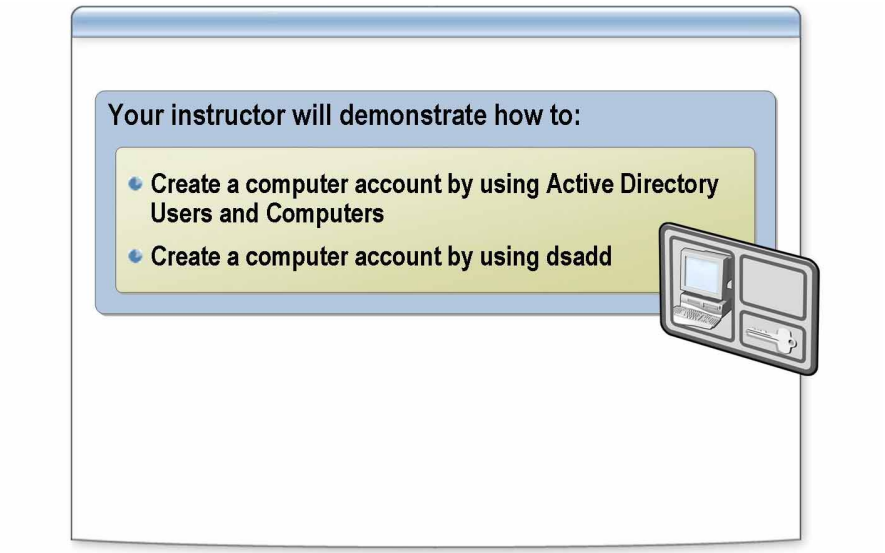
Backup domain controller

Select the **Assign this computer as a backup domain controller** check box if you intend to use the computer as a backup domain controller. You should use this feature if you are still in a mixed environment with a Window Server 2003 domain controller and Windows NT 4.0 BDC. After the account is created in Active Directory, you can then join the BDC to the domain during the installation of Windows NT 4.0.

Additional Reading

For more information about delegating authentication, see “Delegating authentication” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/SE_constrained_delegation.asp.

How to Create a Computer Account



Introduction

By default, members of the Account Operators group can create computer accounts in the Computers container and in new organizational units. However, they cannot create computer accounts in the Builtin, Domain Controllers, ForeignSecurityPrincipals, LostAndFound, Program Data, System, or Users containers.

Procedure

To create a computer account:

1. In Active Directory Users and Computers, in the console tree, right-click **Computers** or the container in which you want to add the computer, point to **New**, and then click **Computer**.
2. In the **New Object – Computer** dialog box, in the **Computer name** box, type the computer name.
3. Select the appropriate options, and then click **Next**.
4. In the **Managed** dialog box, click **Next**.
5. Click **Finish**.

Note To perform this procedure, you must be a member of the Account Operators group, 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.

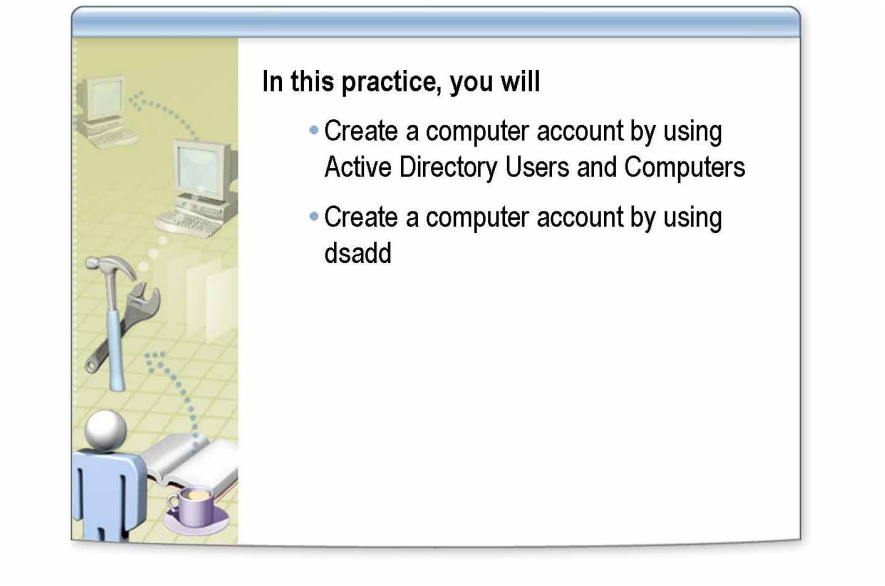
Using a command line

To create a computer account by using **dsadd computer**:

1. Open a command prompt.
2. Type **dsadd computer** *ComputerDomainName* [**-samid** *SAMName*] [**-desc** *Description*] [**-loc** *Location*] [**-memberof** *GroupDomainName* ..] [{**-s** *Server* | **-d** *Domain*}] [**-u** *UserName*] [**-p** {*Password* | *****}] [**-q**] [{**-uc** | **-uco** | **-uci**}]

Note For the complete syntax of the dsadd user command, at a command prompt, type **dsadd computer /?**.

Practice: Creating a Computer Account



Objective

In this practice, you will create computer accounts.

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 for Northwind Traders are testing some advanced features of Active Directory. Each member of your team must create five computer accounts in the IT Test organizational unit.

Practice: Creating a computer account

► **Create a computer account**

1. In Active Directory Users and Computers, expand **nwtraders.msft**, and then click the **IT Test** organizational unit.
2. Create a computer account with the following parameters:
   a. Computer name: *ComputerName***001**
   b. Computer name (pre-Windows 2000): *ComputerName***001**
3. Repeat step 2 for the following computer names: *ComputerName***002**, *ComputerName***003**, *ComputerName***004**
4. Close all windows.

Scenario

The systems engineers for Northwind Traders are testing some advanced features of Active Directory. Each member of your team must create five computer accounts in the IT Test organizational unit.

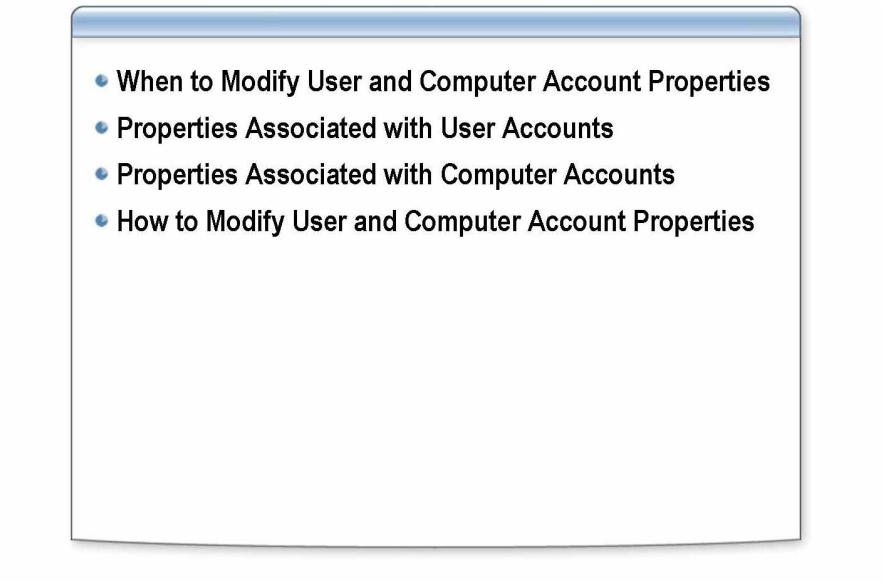
Practice: Using a command line

► **Create a computer account by using dsadd**

1. Click **Start**, click **Run**, and then type **runas /user:nwtraders***ComputerName***Admin cmd**
2. When prompted for the password, type **P@ssw0rd** and then press **ENTER**.
3. At the command prompt, type the following command:

```
dsadd computer "cn=ComputerName005,ou=IT
Test,dc=nwtraders,dc=msft"
```

Lesson: Modifying User and Computer Account Properties



Introduction

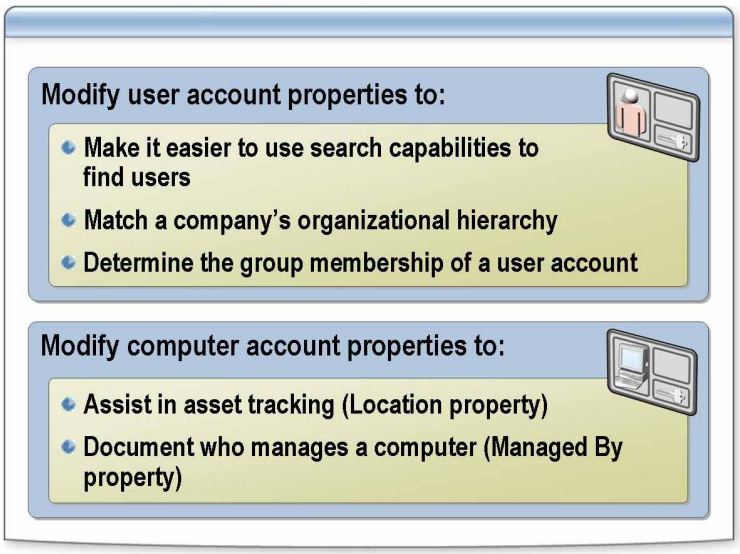
This lesson presents the skills and knowledge that you need to modify user and computer accounts.

Lesson objectives

After completing this lesson, you will be able to:

- Determine when to modify user and computer account properties.
- Describe properties associated with user accounts.
- Describe properties associated with computer accounts.
- Modify user and computer account properties.

When to Modify User and Computer Account Properties



Introduction

As a systems administrator, you may be responsible for creating user and computer accounts in Active Directory. You also may be responsible for maintaining those user and computer accounts. To complete these tasks, you must be very familiar with the various properties for each user and computer account.

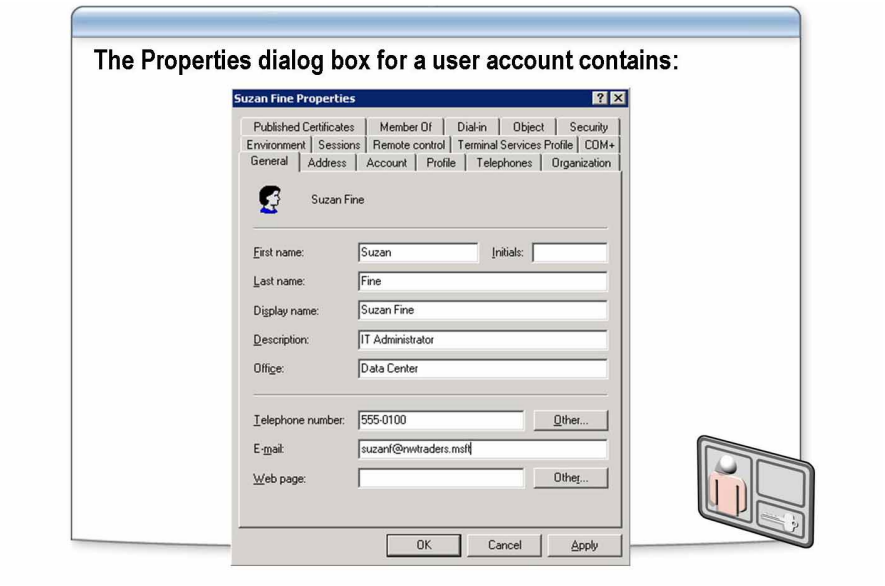
User account properties

It is critical that systems administrators are familiar with user account properties so that they can manage the network structure. Users may use the user account properties as a single source of information about users, like a telephone book, or to search for users based on items such as office location, supervisor, or department name. The systems administrator can use the properties of a user account to determine how the user account behaves in a terminal server session or how the user can gain access to the network through a dial-up connection.

Computer account properties

To maintain computer accounts, you must find the physical location of the computer. The most commonly used properties for computer accounts in Active Directory are the **Location** and **Managed by** properties. The **Location** property is useful, because you can document the computer's physical location in your network. The **Managed By** tab lists the individual responsible for the server. This can be useful when you have a data center with servers for different departments and you need to perform maintenance on the server. You can call or send e-mail to the person who is responsible for the server before you perform maintenance on the server.

Properties Associated with User Accounts



Introduction

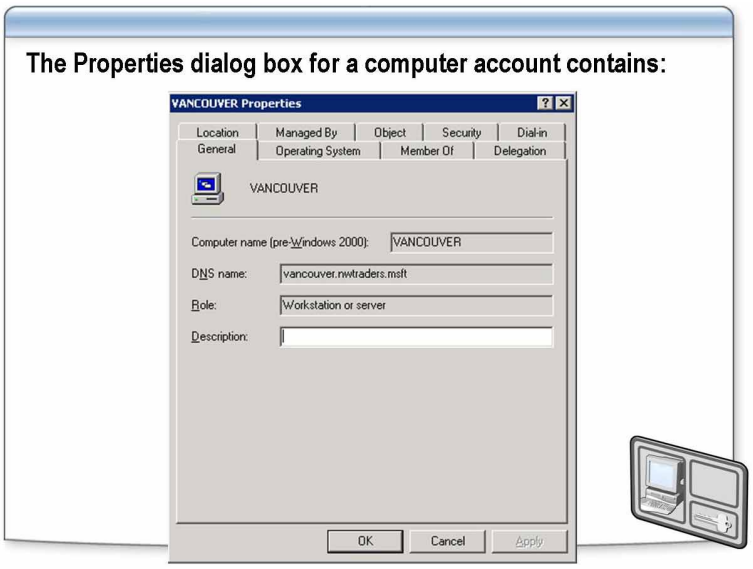
The **Properties** dialog box for a user account contains information about each user account that is stored in Active Directory. The more complete the information in the **Properties** dialog box, the easier it is to search for users in Active Directory.

User account properties

The following table lists the most commonly used property options for user accounts.

Tab	Properties
General	Name, description, office location, telephone number, e-mail address, and home page information
Address	Street address, post office box, city, state or province, postal zip code, and country
Account	Logon name, account options, unlock account, and account expiration
Profile	Profile path and home folder
Telephone	Home, pager, mobile phone, fax, and IP telephone numbers
Organization	Title, department, manager, and direct reports
Member Of	Groups to which the user belongs
Dial-in	Remote access permissions, callback options, and static IP address and routes
Environment	One or more applications to start and the devices to connect to when a Terminal Services user logs on
Sessions	Terminal Services settings
Remote control	Terminal Services remote control settings
Terminal Services Profile	The user's Terminal Services profile

Properties Associated with Computer Accounts



Introduction

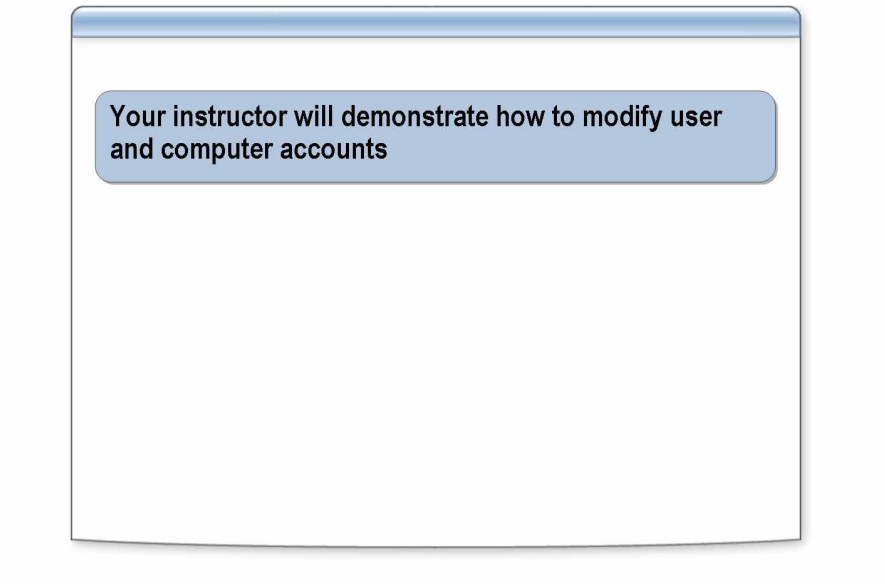
The **Properties** dialog box for a computer account contains unique information about each computer account that is stored in Active Directory. The more complete the information in the **Properties** dialog box, the easier it is to search for computers in Active Directory.

Computer account properties

The following table lists the most commonly used property options for computer accounts.

Tab	Properties
General	Computer name, DNS name, description, and role
Operating System	Name and version of the operating system running on the computer and the latest service pack installed
Member Of	The groups in the local domain and any groups to which the computer belongs
Location	The location of the computer
Managed By	Name, office location, street, city, state or province, country or region, telephone number, and fax number of the person that manages the computer
Object	The canonical name of the object, object class, the date it was created, the date it was last modified, and update sequence numbers (USNs)
Security	The users and groups who have permissions for the computer
Dial-in	Remote access permission, callback options, and routing options

How to Modify User and Computer Account Properties



Introduction

As a systems administrator, you must be able to modify user and computer account properties to manage the network efficiently.

Procedure

To modify user and computer accounts:

1. In Active Directory Users and Computers, in the console tree, navigate to the container that contains the user or computer account that you want to modify.
2. In the details pane, select the user or computer account that you want to modify, right-click the selection, and then click **Properties**.
3. In the **Properties** dialog box, modify the properties of the account as necessary.

Note To perform this procedure, you must be a member of the Account Operators, Domain Admins, or 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

You can use the **dsmod** command to modify attributes of one or more existing users or computers in Active Directory. To modify the attributes of a user account:

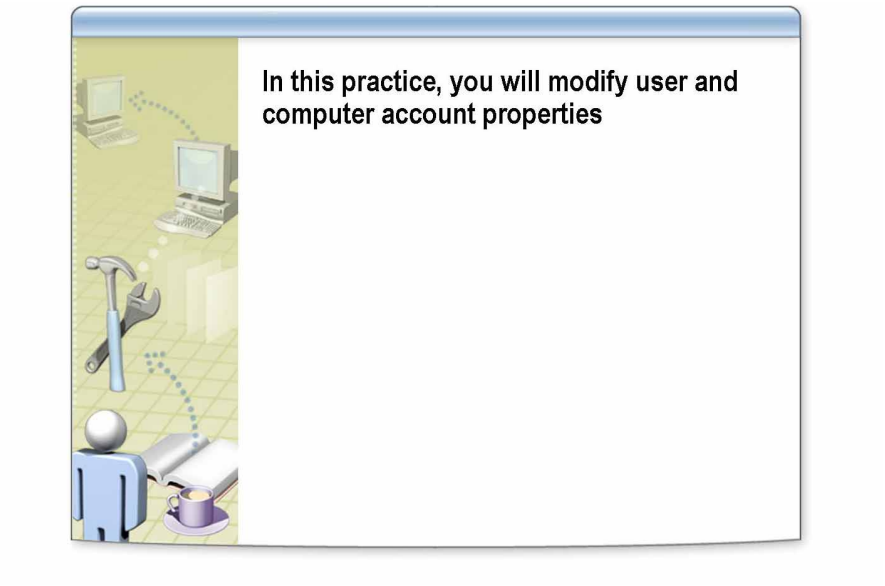
1. Open a command prompt.
2. For a user account, type **dsmod user** *UserDN ...* [**-upn** *UPN*] [**-fn** *FirstName*] [**-mi** *Initial*] [**-ln** *LastName*] [**-display** *DisplayName*] [**-empid** *EmployeeID*] [**-pwd** (*Password* | *****)] [**-desc** *Description*] [**-office** *Office*] [**-tel** *PhoneNumber*] [**-email** *E-mailAddress*] [**-hometel** *HomePhoneNumber*] [**-pager** *PagerNumber*] [**-mobile** *CellPhoneNumber*] [**-fax** *FaxNumber*] [**-iptel** *IPPhoneNumber*] [**-webpg** *WebPage*] [**-title** *Title*] [**-dept** *Department*] [**-company** *Company*] [**-mgr** *Manager*] [**-hmdir** *HomeDirectory*] [**-hmdrv** *DriveLetter:*] [**-profile** *ProfilePath*] [**-loscr** *ScriptPath*] [**-mustchpwd** {**yes** | **no**}] [**-canchpwd** {**yes** | **no**}] [**-reversiblepwd** {**yes** | **no**}] [**-pwdneverexpires** {**yes** | **no**}] [**-acctexpires** *NumberOfDays*] [**-disabled** {**yes** | **no**}] [{**-s** *Server* | **-d** *Domain*}] [**-u** *UserName*] [**-p** {*Password* | *****}] [**-c**] [**-q**] [{**-uc** | **-uco** | **-uci**}]

   −or−

   For a computer account, type **dsmod computer** *ComputerDN ...* [**-desc** *Description*] [**-loc** *Location*] [**-disabled** {**yes** | **no**}] [**-reset**] [{**-s** *Server* | **-d** *Domain*}] [**-u** *UserName*] [**-p** {*Password* | *****}] [**-c**] [**-q**] [{**-uc** | **-uco** | **-uci**}]

Note For the complete syntax of the dsmod command, at a command prompt, type **dsmod user /?** or **dsmod computer /?**.

Practice: Modifying User and Computer Account Properties



Objective

In this practice, you will modify user and computer account properties.

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 for Northwind Traders are working on integrating Active Directory with the payroll system. You must create a user in the IT Test organizational unit and set user account properties that the payroll system will use to identify the user. Because this is a test account, you will not mandate the user to change the password. Also, because the systems engineers will use this account later, you should disable the account.

Practice: Modify user account properties

► **Create a user account**

- In Active Directory Users and Computers, create a user account with the following parameters:
  - First name: *ComputerName* (Example: London)
  - Last name: **Payroll**
  - Full name: *ComputerName* **Payroll** (Example: London Payroll)
  - User logon name: *ComputerName***Payroll** (Example: LondonPayroll)
  - User logon name [pre-Windows 2000]: *ComputerName***Payroll** (Example: LondonPayroll)
  - Password: **P@ssw0rd**

► **Modify the user account**

- In Active Directory Users and Computers, modify the following parameters of the *ComputerName*Payroll user account:
  - Description: **Account for AD and Payroll Test**
  - Office: **Payroll**
  - Telephone number: **973-555-0198**
  - E-mail: *ComputerName***Payroll@nwtraders.msft**
  - Title: **Payroll Test Account**
  - Department: **Payroll Test**
  - Company: **Payroll Test**
  - Manager: **User0002**
  - Home Telephone number: **555-0101**

Scenario

The systems engineers for Northwind Traders want to test your ability to track and search for computer assets by using the **Location** property of a computer account. You must create a computer account in the IT Test organizational unit and edit the **Location** property to match your city location.

Practice: Modifying computer account properties

► **Create a computer account**

- In Active Directory Users and Computers, create a computer account whose computer name is **Server***ComputerName* (Example: ServerLondon).

► **Modify the computer account**

- In Active Directory Users and Computers, change the **Location** property of the Server*ComputerName* computer account to *ComputerName*.

Scenario

The systems engineers for Northwind Traders are modifying user accounts with command-line tools. You must create a user and modify its properties.

Practice: Using a command line to modify user accounts

► **Add a user account**

- Using **dsadd**, add a user account with a user name of *ComputerName***Dsmod**.

  Example: dsadd user "cn=londonDsmod,ou=it test,dc=nwtraders,dc=msft"

► **Modify the user account**

- Using **dsmod**, modify the following parameters of the user account:
  - First name: *ComputerName*
  - Last name: **Dsmod**
  - Full name: *ComputerName* **Dsmod**
  - User logon name: *ComputerName***Dsmod**
  - Password: **P@ssw0rd**
  - Description: **Account for AD and Dsmod Test**
  - Office: **DataCenter**
  - Telephone number: **555-0101**
  - E-mail: *ComputerName***Dsmod@nwtraders.msft**
  - Title: **Dsmod Test Account**
  - Department: **Data Center**
  - Company: **NWTraders**
  - Home Telephone number: **555-0101**

  Example: dsmod user "cn=Londondsmod,ou=it test,dc=nwtraders,dc=msft" -upn Londondsmod@nwtraders.msft -fn London -ln dsmod -display Londondsmod -office DataCenter -tel 555-0101 -title Title ITAdmin -dept DataCenter -company NWTraders -hometel 555-0101

Scenario

The systems engineers for Northwind Traders want to test your ability to track and search for computer assets by using the **Location** property of the Active Directory computer account. You need to create a computer account in the IT Test organizational unit and edit the **Location** property to match your city location.

Practice: Using a command line to modify computer accounts

► **Add a computer account**

1. Click **Start**, click **Run**, and then type **runas /user:nwtraders***ComputerName***Admin cmd**
2. When prompted for the password, type **P@ssw0rd** and then press **ENTER**.
3. In the command prompt, using **dsadd**, add a computer account with the following parameters:
   - Computer name: **dsmod***ComputerName*
   - Organizational unit: IT Test

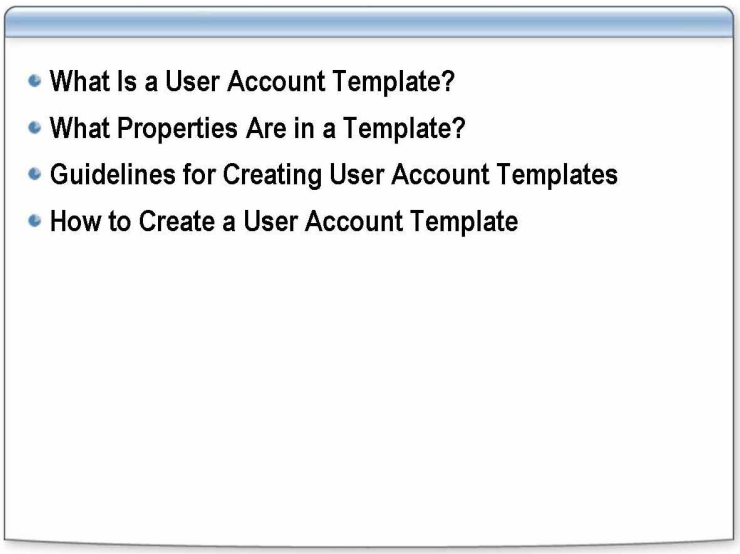
Example: dsadd computer "cn=dsmodlondon,ou=it test,dc=nwtraders,dc=msft"

► **Modify the location attribute for a computer account**

- Using **dsmod**, modify the computer account **dsmod***ComputerName* with the following attribute:
  - Location: *ComputerName*

Example: dsmod computer "cn=serverlondon,ou=it test,dc=nwtraders,dc=msft" -loc London

Lesson: Creating a User Account Template



Introduction

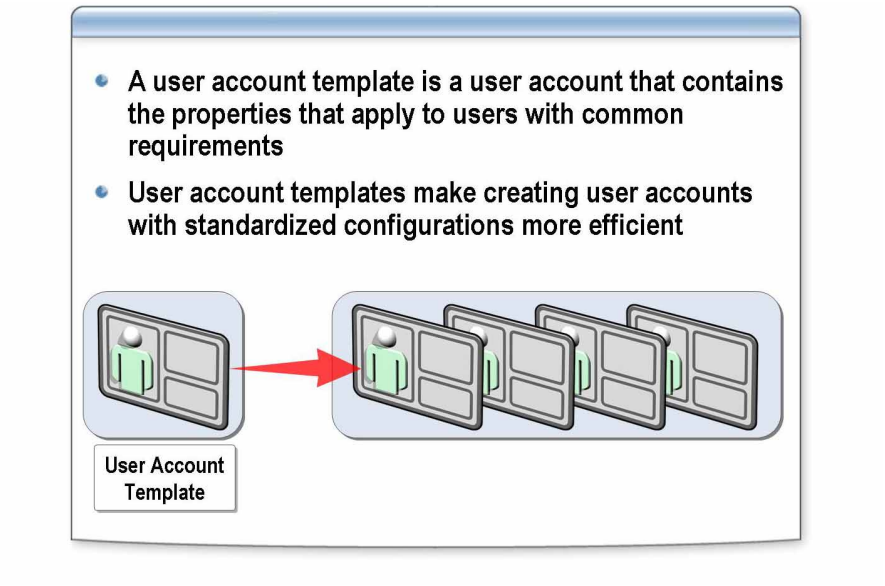
The information in this lesson presents the skills and knowledge that you need to create a user account template.

Lesson objectives

After completing this lesson, you will be able to:

- Explain the purpose of a user account template.
- Describe the properties of a user account template.
- Create a user account template.

What Is a User Account Template?



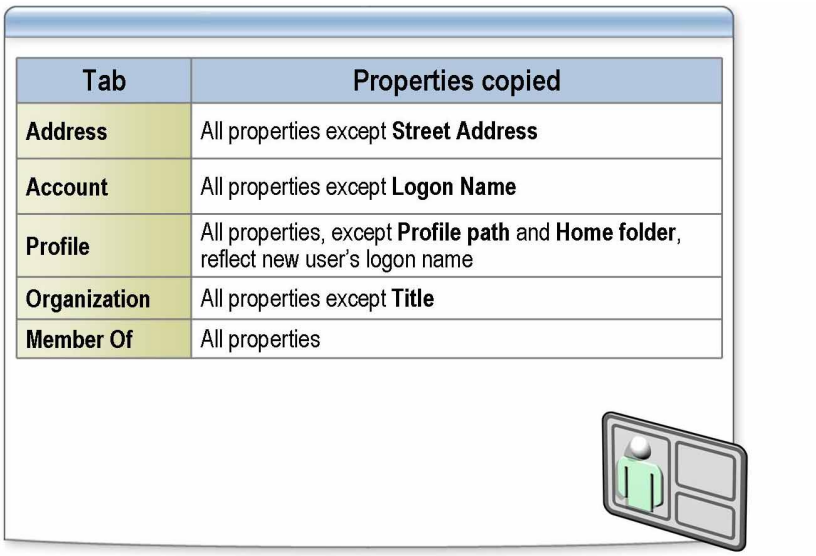
Definition

You can simplify the process of creating domain user accounts by creating a user account template. A user account template is an account that has commonly used settings and properties already configured.

Using account templates

For each new user account, you only need to add the information that is unique to that user account. For example, if all sales personnel must be a member of 15 sales groups and have the same manager, you can create a template that includes membership to all the groups and the reporting manager. When the template is copied for a new salesperson, it retains the group memberships and manager that were in the template.

What Properties Are in a Template?



Properties

There are numerous properties associated with each account. However, only a limited number of properties can be copied in a template. The following table lists the user properties that can be copied from an existing domain user account to a new domain user account.

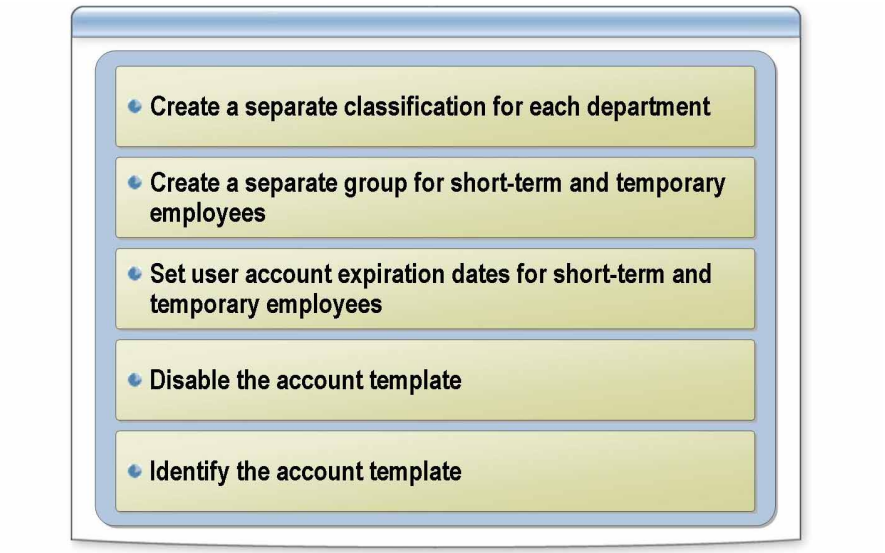
Properties tab	Properties copied to new domain user account
Address	All properties, except **Street Address**, are copied.
Account	All properties, except **Logon Name**, which is copied from the **Copy Object – User** dialog box, are copied.
Profile	All properties, except the **Profile path** and **Home folder** entries, are modified to reflect the new user's logon name.
Organization	All properties, except **Title**, are copied.
Member Of	All properties are copied.

Additional reading

For more information about profiles, see article 324749, "HOW TO: Create a Roaming User Profile in Windows Server 2003" in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=324749.

Form more information about home folders, see article 325853, "HOW TO: Use Older Roaming User Profiles with Windows Server 2003" in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=325853.

Guidelines for Creating User Account Templates

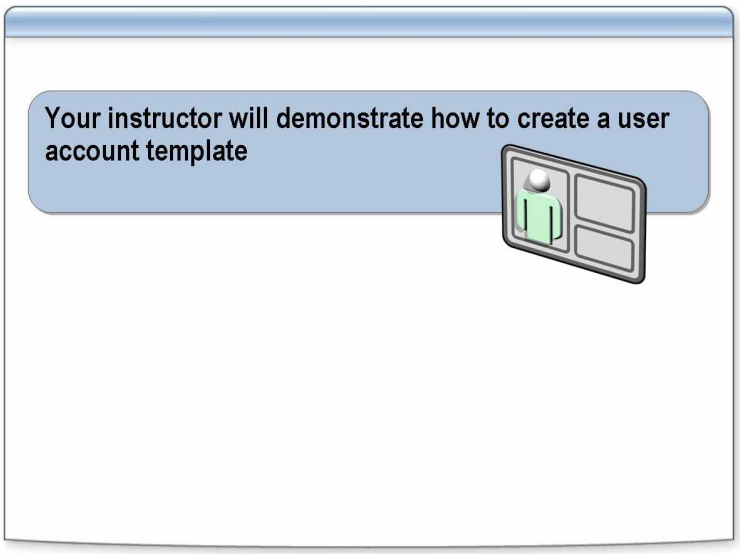


Guidelines

Consider the following best practices for creating user account templates:

- Create a separate classification for each department in your business group.
- Create a separate group for short-term and temporary employees with logon and workstation restrictions.
- Set user account expiration dates for short-term and temporary employees to prevent them from accessing the network when their contracts expire.
- Disable the account template.
- Identify the account template. For example, place a T_ before the name of the account to identify the account as an account template.

How to Create a User Account Template



Introduction

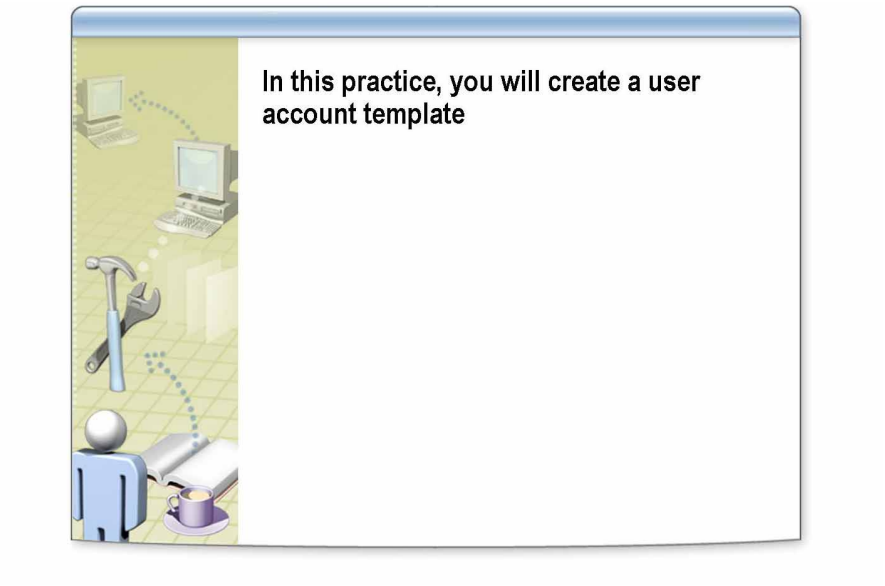
To create an account that you can use as a template, you create a user account, configure the settings that you want, disable the account, and then copy the account when you need to create a new user.

Procedure

To create a new user account template:

1. Create a new domain user account, or copy an existing domain user account.
2. Type the user name and user logon name information for the new user account, and then click **Next**.
3. Type and confirm the password, set the password requirements, select the **Account is disabled** check box, if necessary, and then click **Next**.
4. Verify the new user account information, and then click **Finish**.

Practice: Creating a User Account Template



Objective

In this practice, you will create and copy a user account template.

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

Your manager asks you to research the values to be copied from an account template. You must create an account template with the following parameters, copy the account to a user account, and document the variables that were copied and the variables that were not copied.

Practice: creating a user account template

► **Create a user account template**

- Create a user account template with the following parameters.

Parameter	Properties	Example
First name	*ComputerName*	London
Last name	**Template**	
Full name	*ComputerName* **Template**	London Template
User logon name	_*ComputerName***Template**	_LondonTemplate
Password	**P@ssw0rd**	

► Modify the user account template

- Modify the following parameters of the *ComputerName*Template user account.

Parameter	Properties	Example
Description	**Telemarketing User**	
Office	**Telemarketing**	
Telephone number	**555-1000**	
E-mail	*ComputerName***Template@ nwtraders.msft**	LondonTemplate@ nwtraders.msft
City	**Redmond**	
Street	**One Microsoft Way**	
State	**Washington**	
Zip	**98052**	
Country/region	**United States**	
Home Telephone number	**555-0101**	
Title	**Telemarketing User**	
Department	**Telemarketing**	
Company	**NWTraders**	
Manager	**User 0001**	
Member (group membership)	**G NWTraders Telemarketing Personnel**	
Account is disabled		

Scenario

You must create accounts for the Telemarketing team at Northwind Traders. The Telemarketing team has a high turnover of employees. For security reasons, Northwind Traders does not want to rename and reuse user accounts. You must create a user account template that meets the needs of the Telemarketing team.

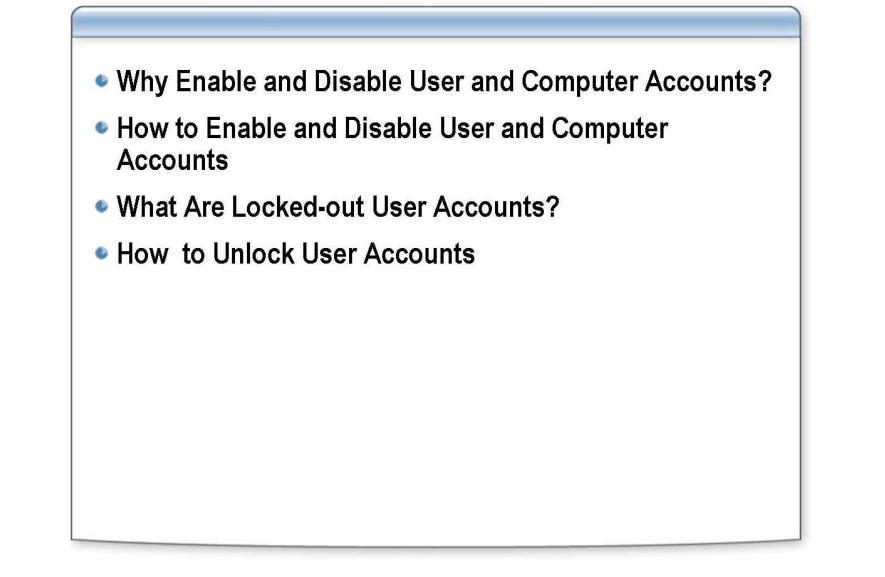
Practice: copying a user account template

► Copy the user account template

- Copy the *ComputerName*Template account that has the following parameters.

Parameter	Properties	Example
First name	*ComputerName*	London
Last name	**User**	
Full name	*ComputerName* **User**	London User
User logon name	*ComputerName***Template**	LondonTemplate
Password	**P@ssw0rd**	

Lesson: Enabling and Unlocking User and Computer Accounts



Introduction

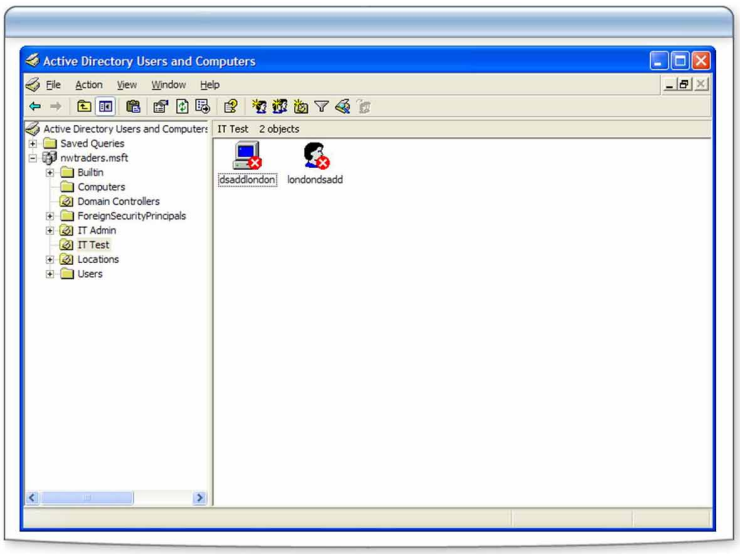
The information in this lesson presents the skills and knowledge that you need to enable and disable user and computer accounts.

Lesson objectives

After completing this lesson, you will be able to:

- Explain why you enable and disable user and computer accounts.
- Enable and disable user and computer accounts.
- Explain how user accounts can become locked-out.
- Unlock user accounts.

Why Enable or Disable User and Computer Accounts?



Introduction

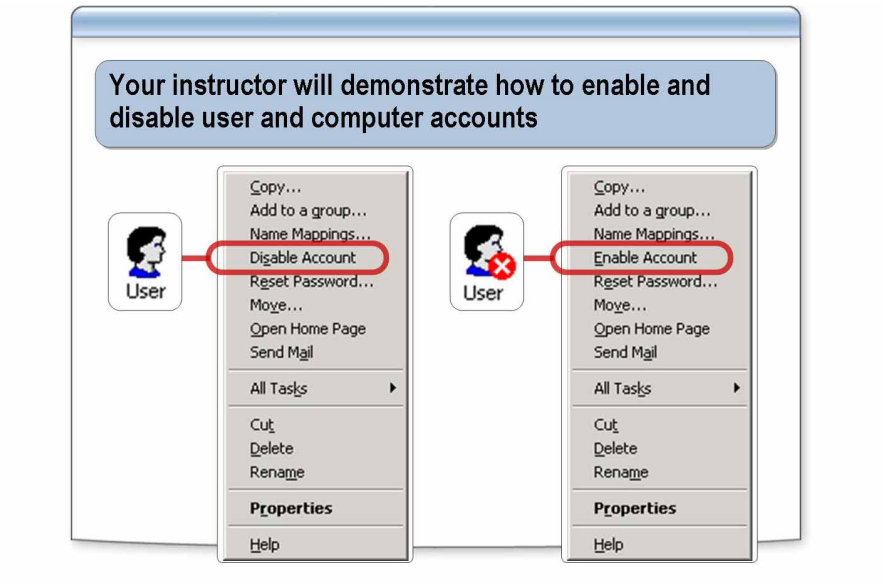
After creating user accounts, you perform frequent administrative tasks to ensure that the network continues to meet the organization's needs. These administrative tasks include enabling and disabling user and computer accounts. When you enable or disable an account, you give or restrict access to the account.

Scenarios for enabling and disabling accounts

To provide a secure network environment, a systems administrator must disable user accounts when users do not need their accounts for an extended period, but need to use them later. The following are examples of when you need to enable or disable user accounts:

- If the user takes a two-month leave of absence from work, you disable the account when the user leaves and then enable the account when the user returns.
- When you add accounts in the network that will be used in the future or for security purposes, you disable the accounts until they are needed.
- Disable an account when you do not want users to be authenticated from a shared computer.

How to Enable and Disable User and Computer Accounts



Introduction

When an account is disabled, the user cannot log on. The account appears in the details pane with an X on the account icon.

Procedure

To enable and disable a user or computer account by using Active Directory Users and Computers:

1. In Active Directory Users and Computers, in the console tree, select the container or the user that contains the account to be enabled or disabled.
2. In the details pane, right-click the user account.
3. To disable, click **Disable Account**.
4. To enable, click **Enable Account**.

To disable or enable a local user account by using Computer Management:

1. In Computer Management, expand **System Tools**.
2. In System Tools, expand **Local Users and Groups**, and then click **Users**.
3. Right-click the user account, and then click **Properties**.
4. In the **Properties** dialog box, to disable, select the **Account is Disabled** check box, and then click **OK**.
5. To enable, clear the **Account is Disabled** check box.

Note To enable and disable user and computer accounts, you must be a member of the Account Operators group, 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

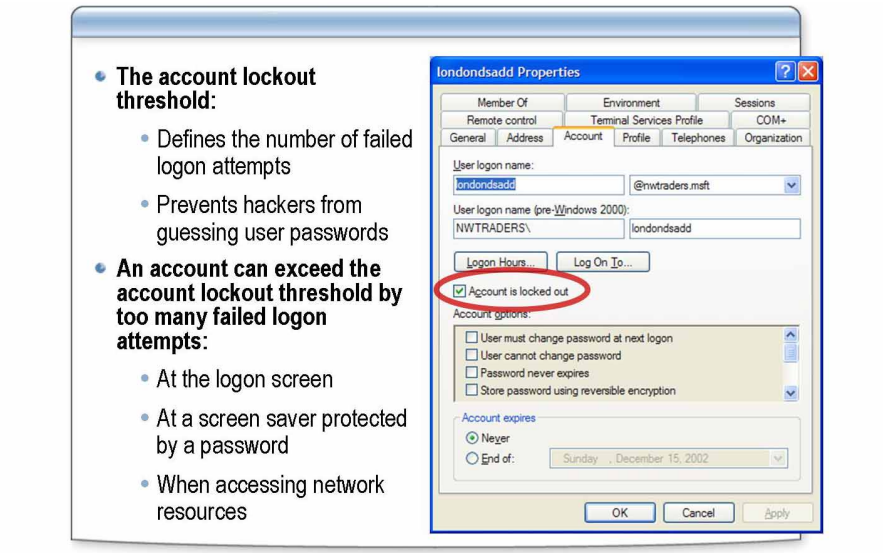
You can also enable or disable accounts by using the **dsmod** command. As a security best practice, consider using **runas** to perform this procedure.

To enable or disable accounts by using **dsmod**:

1. Open a command prompt with the **runas** command.
2. Type **dsmod user** *UserDN* **-disabled {yes|no}**

Value	Description
UserDN	Specifies the distinguished name of the user object to be disabled or enabled
{**yes**|**no**}	Specifies whether the user account is disabled for log on (**yes**) or enabled (**no**)

What Are Locked-out User Accounts?



Introduction

A user account is locked out because the account has exceeded the account lockout threshold for a domain. This may be because the user has attempted to access the account with an incorrect password too many times or because a computer hacker has attempted to guess users' passwords and invoked the lockout policy on the account.

Account lockout threshold

Authorized users can lock themselves out of an account by mistyping or forgetting their password or by changing their password on a computer while they are logged on to another computer. The computer with the incorrect password continuously tries to authenticate the user. Because the password it is using to authenticate is incorrect, the user account is eventually locked out.

A security setting in Active Directory determines the number of failed logon attempts that causes a user to be locked out. A user cannot use a locked-out account until an administrator resets the account or until the lockout duration for the account expires. When a user account is locked out, an error message appears, and the user is not allowed any further logon attempts.

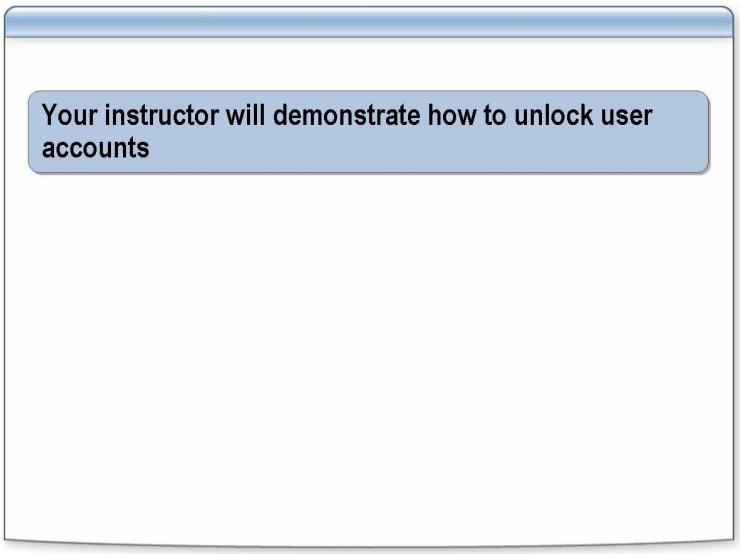
What is a failed logon attempt?

A user can be locked out of an account if there are too many failed password attempts. Failed password attempts happen when:

- A user logs on at the logon screen and supplies a bad password.
- A user logs on with a local account and supplies a domain user account and a bad password while accessing network resources.
- A user logs on with a local account and supplies a domain user account and a bad password while accessing resources with the **runas** command.

By default, domain account lockout attempts are not recorded when unlocking a workstation (using a password protected screen saver). You can change this behavior by modifying the **Interactive logon: Require Domain controller authentication to unlock workstation** Group Policy setting.

How to Unlock User Accounts



Introduction

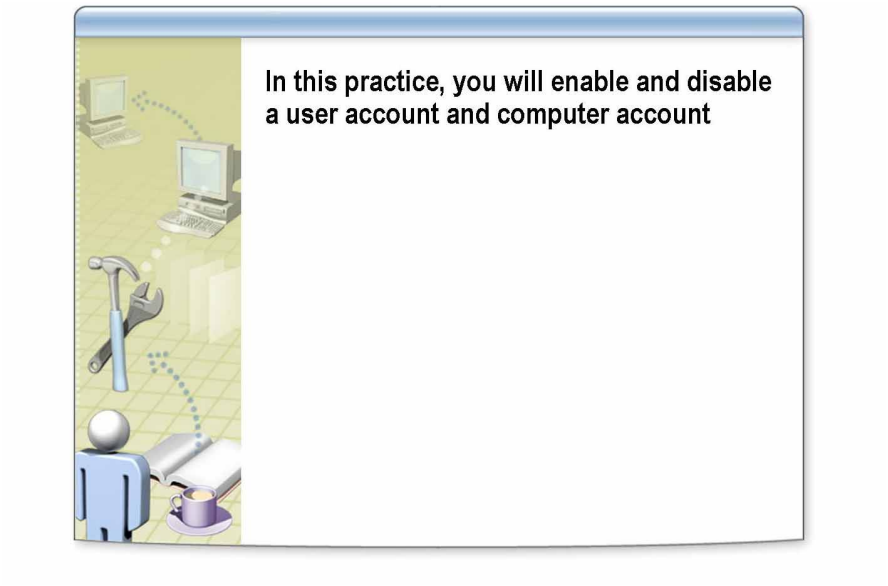
After an account is locked out, you must unlock the account to maintain and manage the account.

Procedure

To unlock an account:

1. In Active Directory Users and Computers, in the console tree, select the organizational unit that contains the user account that you want to unlock.
2. In the details pane, select the user account you want to unlock.
3. Right-click the selected account and then click **Unlock**.

Practice: Enabling and Disabling User and Computer Accounts



Objective

In this exercise, you will disable and enable a user account and a computer account.

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 security policy of Northwind Traders states that the user accounts of employees going on extended leave must be disabled for the duration of their leave. This is one of your job tasks. You must create an account in the IT Test organizational unit, disable the account, and log on as the user to verify that the account is disabled.

Practice: Disabling a user account

► **Create a disabled user account**

- Create a user account with the following parameters:
  - Organizational Unit: **IT Test**
  - User name: *ComputerName***Disabled**
  - Password: **P@ssw0rd**
  - The account is disabled

► **Test the disabled user account**

- Try to log on as the new user to verify that you cannot log on.

Scenario

You have just disabled a user account and verified that the user cannot log on. You want to verify that there are no other problems with the account, so you must enable the user account and log on to verify that the user account is activated.

Practice: Enabling a user account

► **Enable the user account**

- Enable the user account that has the following parameters:
  - Organizational unit: IT Test
  - User name: *ComputerName*Disabled

► **Test the enabled user account**

1. Log on with the *ComputerName*Disabled user account to verify that you can log on.
2. Log on with a password of P@ssw0rd.

Scenario

A systems engineer is concerned that an unauthorized user is attempting to use a kiosk computer after business hours. The systems engineer asks you to disable the computer account until they can look at the log files on the computer. You must disable the computer account.

Practice: Disabling a computer account

► **Create a disabled computer account**

- Create a disabled computer account with the following parameters:
  - Organizational unit: IT Test
  - Computer name: *ComputerName***Kiosk**
  - The account is disabled

Scenario

The systems engineer discovers that the nightly security guard was trying to log on to the kiosk computer without a domain account. The security guard has been notified that they should not attempt to log on to the kiosk computer. The systems engineer wants you to enable the kiosk computer for your city location.

Practice: Enabling a computer account

► **Enable the computer account**

- Enable the computer account that has the following parameters:
  - Organizational unit: IT Test
  - Computer name: *ComputerName*Kiosk

Practice: Using a command line

► **Disable a user account by using dsmod**

- Disable a user account in the IT Test organizational unit by using **dsmod**.

  Example: Dsmod user "cn=London user,ou=it test,dc=nwtraders,dc=msft" -disabled yes

► **Enable a user account by using dsmod**

- Enable a user account in the IT Test organizational unit by using **dsmod**.

  Example: Dsmod user "cn=London user,ou=it test,dc=nwtraders,dc=msft" -disabled no

Lesson: Resetting User and Computer Accounts

Introduction

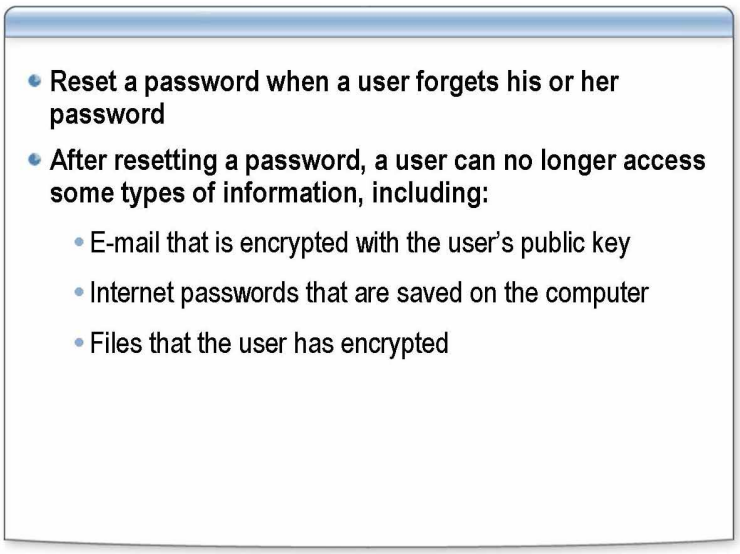
Resetting passwords and accounts are common administrative tasks. Be aware of the impact of performing these procedures.

Lesson objectives

After completing this lesson, you will be able to:

- Explain the situations that require you to reset passwords and the potential data loss resulting from resetting passwords.
- Reset passwords for domain and local accounts.
- Determine when to reset computer accounts.
- Reset computer accounts.

When to Reset User Passwords



Introduction

People occasionally forget their passwords. Without their passwords, these people cannot access their user accounts. Administrators can reset users' passwords so that users can access their accounts again. Before attempting to reset local or domain passwords, verify that you have the appropriate level of authority.

Consequences of resetting passwords

After a user's password is reset, some types of information are no longer accessible, including the following:

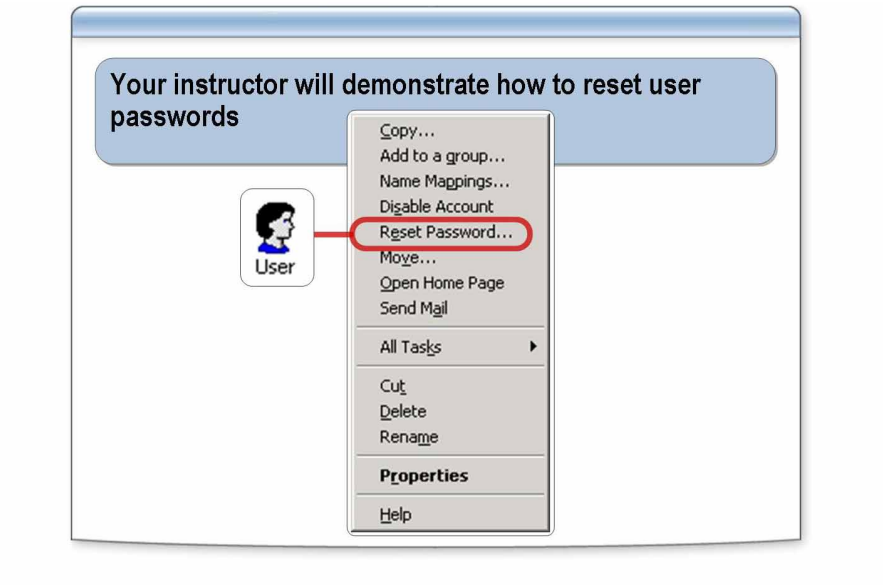
- E-mail that is encrypted with the user's public key
- Internet passwords that are saved on the computer
- Files that the user has encrypted

Additional reading

For more information about resetting a domain controller account and resetting a computer account with a script, see article 325850, "HOW TO: Use Netdom.exe to Reset Machine Account Passwords of a Windows Server 2003 Domain Controller," in the Microsoft Knowledge Base at: http://support.microsoft.com/?kbid=325850.

For more information about how Windows data protection API handles stored passwords, see "Windows Data Protection" at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/windataprotection-dpapi.asp.

How to Reset User Passwords



Introduction

When you need to reset a user password, you must remember that only local administrators are authorized to reset local user passwords and that only domain administrators are authorized to reset domain user passwords.

Procedure for resetting local user passwords

To reset local user passwords:

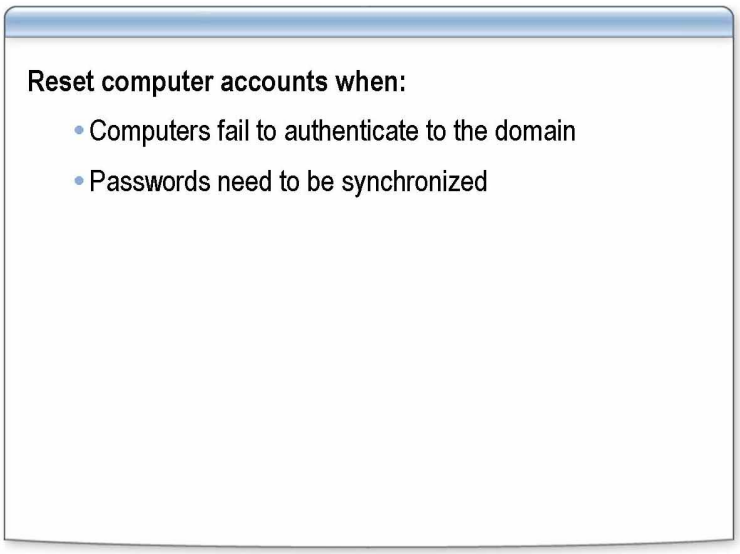
1. In Computer Management, in the console tree, double-click **Local Users and Groups**, and then click **Users**.
2. In the details pane, right-click the user name, and then click **Set Password**.
3. Read the warning message. If you want to continue, click **Proceed**.
4. In the **New password** and **Confirm password** boxes, type the new password, and then click **OK**.

Procedure for resetting domain user passwords

To reset domain user passwords:

1. In Active Directory Users and Computers, in the console tree, click **Users**.
2. In the details pane, right-click the user name, and then click **Reset Password**.
3. In the **New Password** and **Confirm New Password** boxes, type a new password, and then click **OK**.

When to Reset Computer Accounts



Introduction

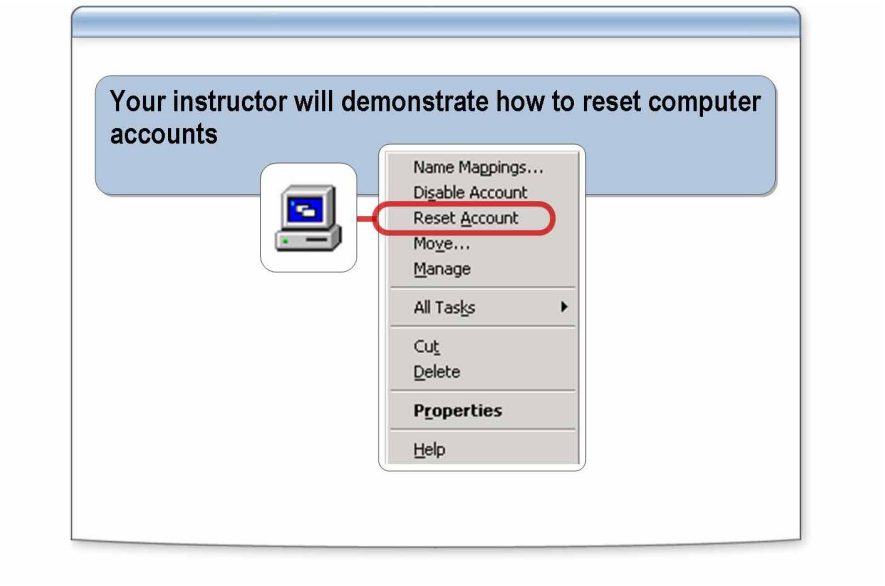
As a systems administrator, you occasionally need to reset computer accounts. For example, suppose your network went through a full backup seven days ago. The computer relayed information to the domain controller that changed the password on the computer account. However, the computer's hard drive crashed, and the computer was restored from tape backup. The computer now has an outdated password, and the user cannot log on because the computer cannot authenticate to the domain. You now need to reset the computer account.

Considerations

There are two items that you must consider before resetting the computer account:

- To perform this procedure, you must be a member of the Account Operators group, 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.
- When you reset a computer account, you break the computer's connection to the domain, and you must rejoin it to the domain.

How to Reset Computer Accounts



Introduction

To perform this procedure, you must be a member of the Account Operators group, 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.

Procedure

To reset computer accounts:

1. In Active Directory Users and Computers, in the console tree, click **Computers** or the container that contains the computer that you want to reset.
2. In the details pane, right-click the computer, and then click **Reset Account**.

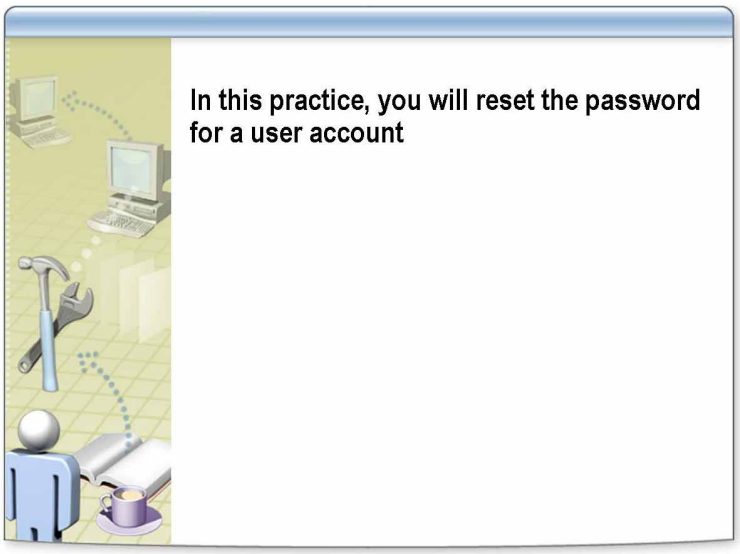
Using a command line

You can use the **dsmod** command to reset computer accounts. As a security best practice, consider using **runas** to perform this procedure.

1. Open a command prompt by using the **runas** command.
2. Type **dsmod computer** *ComputerDN* **–reset**

Value	Description
ComputerDN	Specifies the distinguished names of one or more computer objects that you want to reset

Practice: Resetting a User Account Password



Objective

In this practice, you will reset a user account so that the user can log on to the domain.

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

You are notified that a user in your city recently forgot their password. You have followed company policy and verified the user is who they say they are. You must reset the password on their account and make them change their password at next logon.

Practice

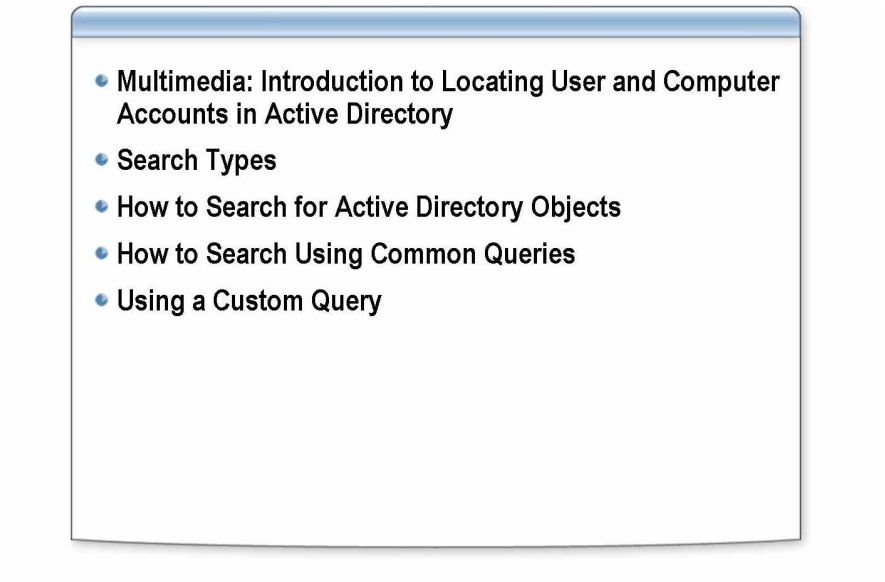
► **Reset the user account**

1. In Active Directory Users and Computer, find the *ComputerName*User account in the Users organizational unit.
2. Reset the password to **P@ssw0rd1** and make the user change the password at next logon.
3. Close all programs and log off.

► **Test the new password**

1. Log on as *ComputerName*User with a password of P@ssw0rd1.
2. Change the password to **P@ssword2**

Lesson: Locating User and Computer Accounts in Active Directory



Introduction

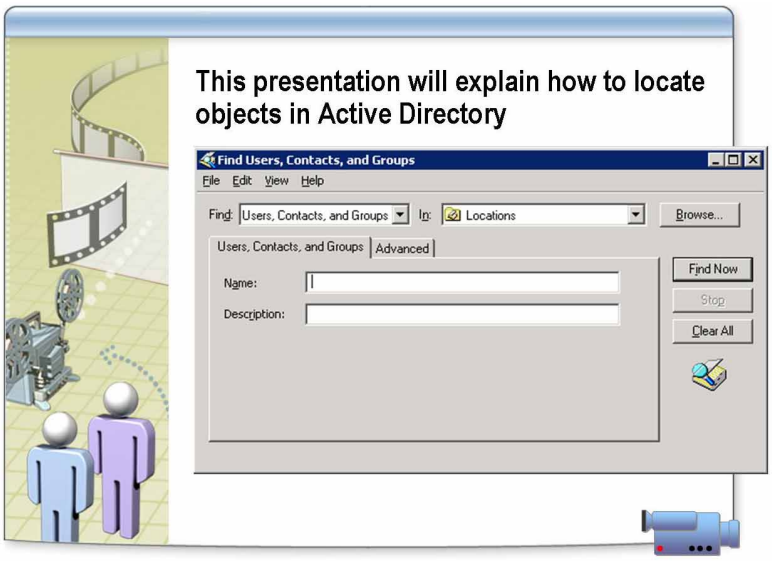
The information in this lesson presents the skills and knowledge that you need to use common and custom queries.

Lesson objectives

After completing this lesson, you will be able to:

- Explain the criteria for locating a user or computer account.
- Describe the types of common queries.
- Explain the uses of custom queries.
- Locate user and computer accounts in Active Directory.

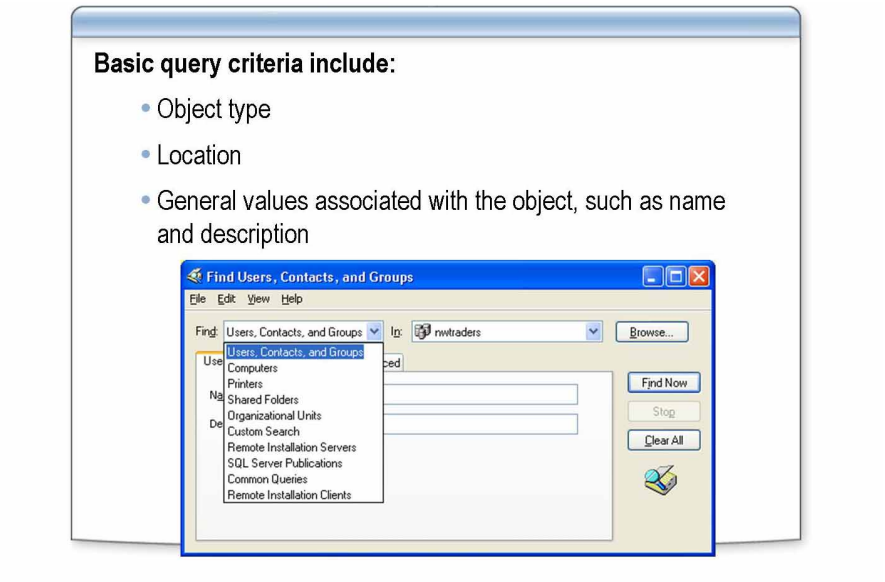
Multimedia: Introduction to Locating User and Computer Accounts in Active Directory



File location

To view the *Introduction to Locating User and Computer Accounts in Active Directory* 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.

Search Types



Introduction

Because all user accounts reside in Active Directory, administrators can search for the user account that they administer. By searching Active Directory for user accounts, you do not need to browse through hundreds or thousands of user accounts in Active Directory Users and Computers.

In addition to searching for user accounts, you can also search for other Active Directory objects, such as computers, printers, and shared folders. After locating these objects, you can administer these objects from the **Search Results** box.

Administering objects from Search Results

After a successful search, the results are displayed, and you can then perform administrative functions on the found objects. The administrative functions that are available depend on the type of object you find. For example, if you search for user accounts, you can rename and delete the user account, disable the user account, reset the password, move the user account to another organizational unit, or modify the user account's properties.

To administer an object from the **Search Results** box, right-click the object and select an action from the menu.

Find Users, Contacts and Groups

Active Directory provides information about all objects on a network, which includes people, groups, computers, printers, shared folders, and organizational units. It is easy to search for users, contacts, and groups by using the **Find Users, Contacts, and Groups** dialog box.

Find Computers

Use **Find Computers** to search for computers in Active Directory by using criteria such as the name assigned to the computer or the operating system on which the computer runs. After you find the computer you want, you can manage it by right-clicking the computer in the **Search Results** box, and then clicking **Manage**.

Find Printers

When a shared printer is published in Active Directory, you can use **Find Printers** to search for it by using criteria such as its asset number, the printer language it uses, or whether it supports double-sided printing. After you find the printer you want, you can easily connect to it by right-clicking the printer in the **Search Results** box, and then clicking **Connect**, or by double-clicking the printer.

Find Shared Folders

When a shared folder is published in Active Directory, you can use **Find Shared Folders** to search for it by using criteria such as keywords assigned to it, the name of the folder, or the name of the person managing the folder. After you find the folder you want, you can open Windows Explorer to view the files located in the folder by right-clicking the folder in the **Search Results** box, and then clicking **Explore**.

Find Custom Search

In Active Directory, you can search for familiar objects such as computers, printers, and users. You can also search for other objects, such as a specific organizational unit or certificate template. Use **Find Custom Search** to build custom search queries by using advanced search options or build advanced search queries by using LDAP, which is the primary access protocol for Active Directory.

Find Common Queries

You can use **Find Common Queries** to perform common administrative queries in Active Directory. For example, you can quickly search for user or computer accounts that have been disabled.

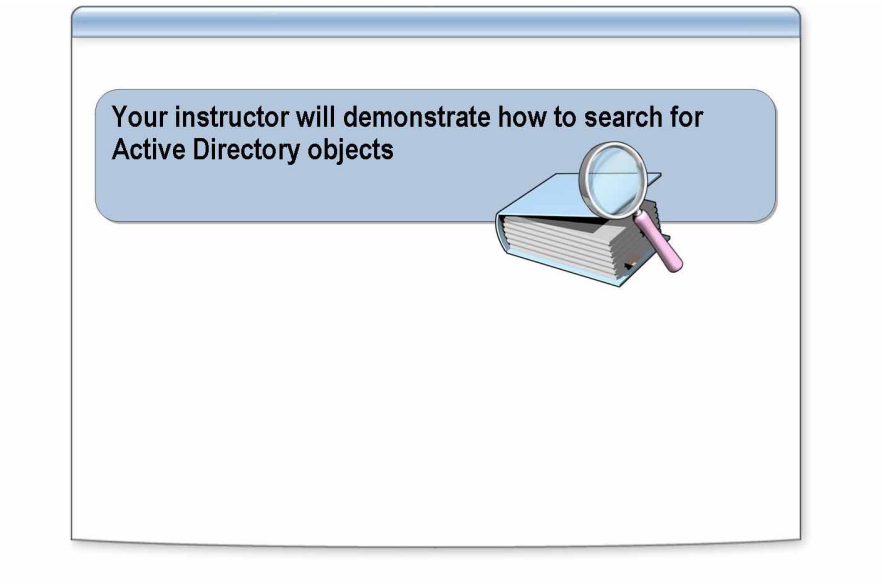
Advanced query options

For each search option except **Find Common Queries**, there is an **Advanced** tab that you can use to create a more detailed search. For example, you can search for all users in a city or zip code from the **Advanced** tab.

Additional reading

For more information about searching Active Directory see “Search Companion overview” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/find_overview.asp.

How to Search for Active Directory Objects



Introduction

To perform administrative tasks on a user or computer account, you must first find the account in Active Directory. This may be difficult if your Active Directory structure is large.

Procedure

To find a user account:

1. Open Active Directory Users and Computers.
2. To search the entire domain, in the console tree, right-click the domain node, and then click **Find**.

   If you know which organizational unit the user is in, right-click the organizational unit, and then click **Find**.
3. In the **Find Users, Contacts, and Groups** dialog box, in the **Name** box, type the name of the user you want to find.
4. Click **Find Now**.

Using a command line

You can use the **dsquery** command to find users and computers in Active Directory that match the specified search criteria. If the predefined search criteria in this command are insufficient, use the more general version of the command, **dsquery ***.

To search for a user by using **dsquery**:

- In a command prompt, type the following:

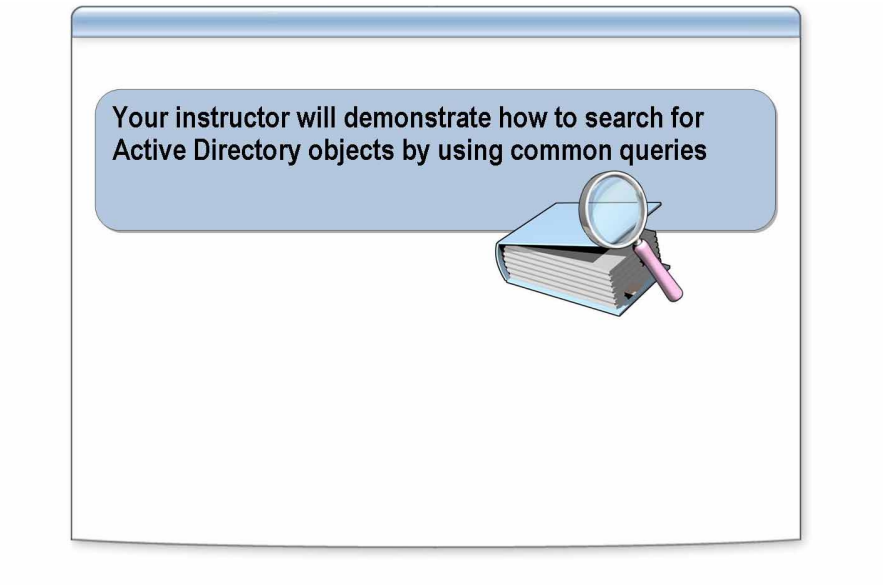
  dsquery user [{*StartNode* | **forestroot** | **domainroot**}] [**-o** {**dn** | **rdn** | **upn** | **samid**}] [**-scope** {**subtree** | **onelevel** | **base**}] [**-name** *Name*] [**-desc** *Description*] [**-upn** *UPN*] [**-samid** *SAMName*] [**-inactive** *NumberOfWeeks*] [**-stalepwd** *NumberOfDays*] [**-disabled**] [{**-s** *Server* | **-d** *Domain*}] [**-u** *UserName*] [**-p** {*Password* | ***}] [**-q**] [**-r**] [**-gc**] [**-limit** *NumberOfObjects*] [{**-uc** | **-uco** | **-uci**}]

To search for a computer by using **dsquery**:

- In a command prompt, type the following:

  dsquery computer [{*StartNode* | **forestroot** | **domainroot**}] [**-o** {**dn** | **rdn** | **samid**}] [**-scope** {**subtree** | **onelevel** | **base**}] [**-name** *Name*] [**-desc** *Description*] [**-samid** *SAMName*] [**-inactive** *NumberOfWeeks*] [**-stalepwd** *NumberOfDays*] [**-disabled**] [{**-s** *Server* | **-d** *Domain*}] [**-u** *UserName*] [**-p** {*Password* | ***}] [**-q**] [**-r**] [**-gc**] [**-limit** *NumberOfObjects*] [{**-uc** | **-uco** | **-uci**}]

How to Search Using Common Queries



Introduction

The search functionality is one of the key features of Active Directory. A search operation enables you to find objects in Active Directory based on selection criteria and to retrieve specified properties for the objects that you find.

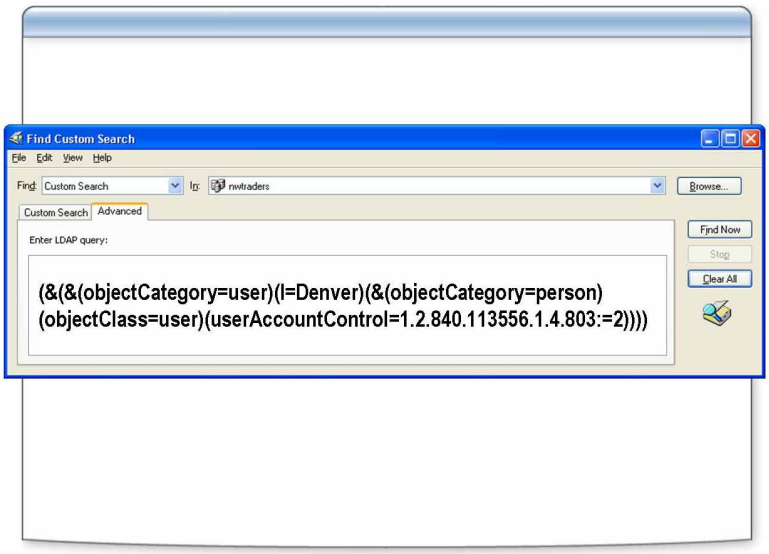
Procedure

To start a basic search operation:

1. In Active Directory Users and Computers, on the **Action** menu, click **Find**.
2. In the **Find Users, Contacts, and Groups** dialog box, in the **Find** box, select the type of object for which you want to search.
3. Enter the search text in the search criteria boxes.

   The types of search criteria that are available vary depending on the type of object that you selected.

Using a Custom Query



Introduction

In Active Directory, you can search for familiar objects, such as computers, printers, and users, and you can also search for other objects, such as a specific organizational units or certificate templates.

Custom Search

Use the **Find Custom Search** dialog box to build custom search queries using advanced search options and to build advanced search queries by using LDAP, which is the primary access protocol for Active Directory.

The LDAP query on the slide includes the following items:

- **l=**Denver

  The **l** is the city property or location attribute for a user account.

- **(ObjectClass=user)(ObjectCategory=person)**

  To query for a user, the query must contain the **(&(objectClass=user)(objectCategory=person))** search expression. This is because the computer class is a subclass of the user class. A query containing only **(objectClass=user)** returns user objects and computer objects.

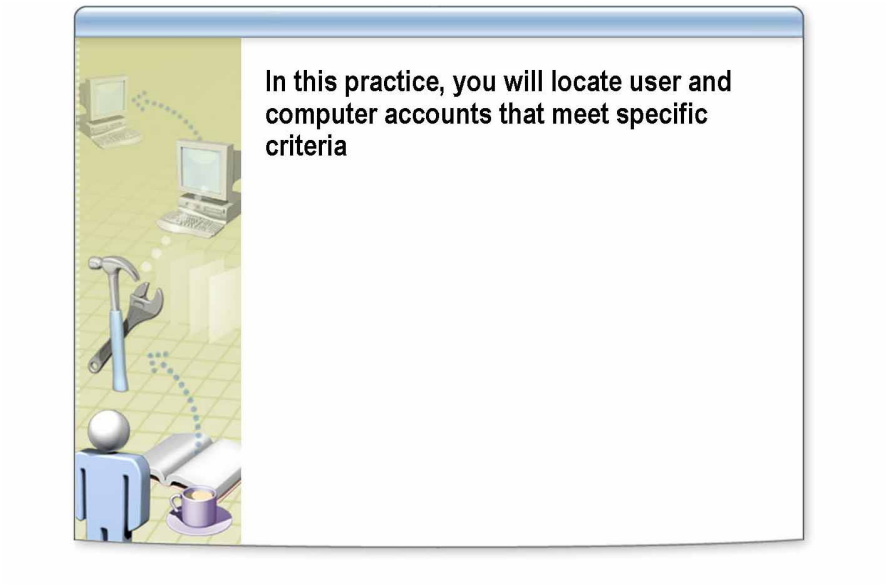
- **UserAccountControl:**1.2.840.113556.1.4.803:=2

  This specifies the flags that control the password, lockout option, disable or enable option, script, and home directory behavior for the user. This property also contains a flag that indicates the account type of the object. The flag used here is for disabled accounts.

Additional reading

For more information about LDAP language, see “Listing Properties to Retrieve for Each Object Found” at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ad/listing_properties_to_retrieve_for_each_object_found.asp.

Practice: Locating User and Computer Accounts



Objective

In this exercise, you will locate:

- User accounts by name.
- Computer accounts by name.
- Disabled accounts.
- Computer accounts by city.
- User and computer accounts by using **dsquery**.

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 bulk importing user accounts into the Users container. They need you to verify that all Sales Manager user accounts were successfully imported into Active Directory.

Practice: locating user accounts by name

► **Locate user accounts by name**

- Locate user accounts:
  - In the Users container in the NWTraders domain.
  - With a description of Sales Manager.

  Your search should produce approximately 24 Sales Manager user accounts.

Scenario

The systems engineers are bulk importing computer accounts into the Computers container. They need you to verify that all computer accounts from your city location were successfully imported into Active Directory. The naming convention used to bulk import computer accounts is the first three to four letters of the city location, followed by **Computer** and an incremental number, for example, CasaComputer2005.

Practice: locating computer accounts by name

► **Locate computer accounts by name**

- Locate a computer account:
  - In the Computers container in the NWTraders domain.
  - With a computer name that is the first three letters of your city location.

  Your search should produce approximately 101 computer accounts.

Scenario

The systems engineers are bulk importing computer accounts into the Computers container. They need you to verify that all computer accounts from your city location have been successfully imported into Active Directory. The naming convention used to bulk import computer accounts is to use the first three to four letters of the city location, followed by **Computer** and an incremental number, for example, CasaComputer2005.

Practice: locating disabled accounts

► **Locate disabled accounts**

- Locate user accounts:
  - In the NWTraders domain.
  - With a description that starts with Sales.
  - That are disabled (*Do not enable the accounts*).

  Your search should produce approximately 240 disabled user accounts.

Scenario

The systems engineers are bulk importing computer accounts into the Computers container. They need you to verify that all computer accounts from your city location were successfully imported into Active Directory. The naming convention used to bulk import computer accounts is to use the first three to four letters of the city location, followed by **Computer** and an incremental number, for example, CasaComputer2005.

Practice: locating computer accounts by city

► **Locate computer accounts by city**

- Locate computer accounts:
  - In the Computers container in the NWTraders domain.
  - With a computer name that is the first three letters of your city location.

Your search should produce approximately 101 computer accounts.

Practice: locating user and computer accounts by using dsquery

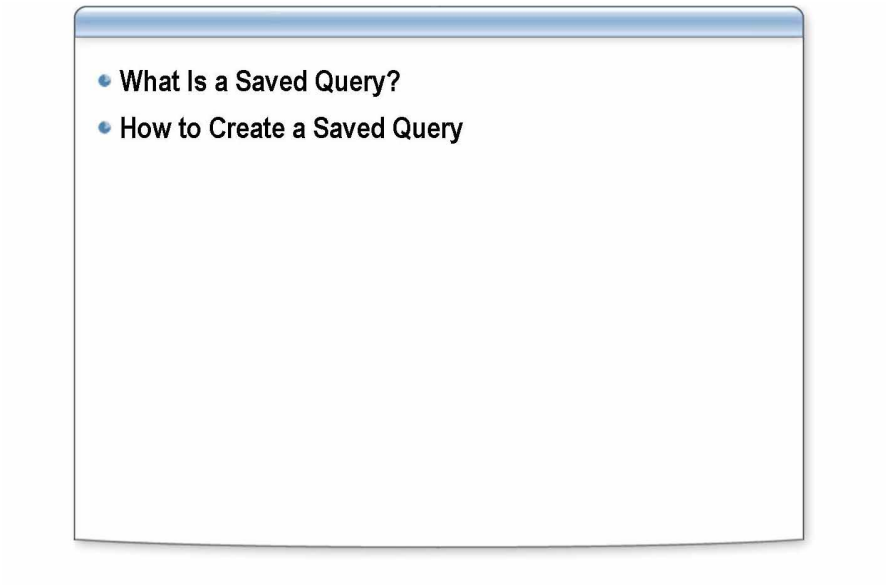
► **Locate all users with the first name of user**

- From a command prompt, type **Dsquery user –**name user*

► **Locate all computers with the first 3 letters lon**

- From a command prompt, type **Dsquery computer –name lon***

Lesson: Saving Queries



Introduction

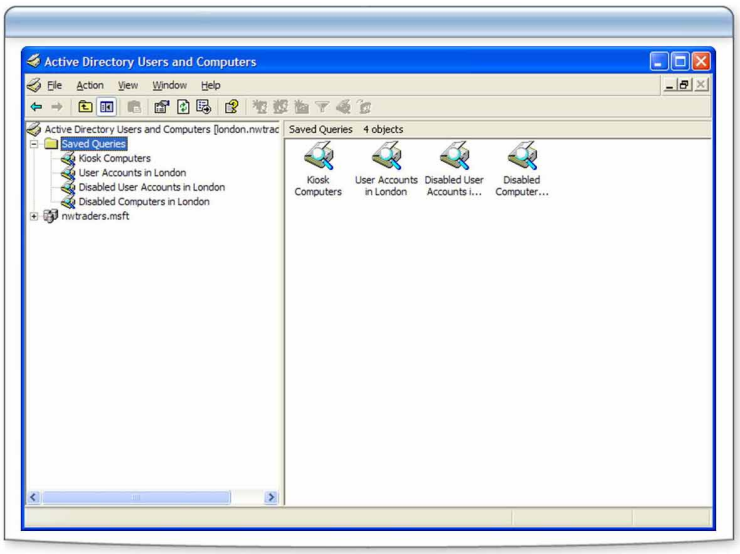
You can use saved queries to quickly and consistently access a common set of Active Directory objects that you want to perform specific tasks on or monitor.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what a saved query is.
- Create a saved query.

What Is a Saved Query?



Introduction

Active Directory Users and Computers has a Saved Queries folder in which you can create, edit, save, and organize saved queries. Before saved queries, administrators were required to create custom Active Directory Services Interfaces (ADSI) scripts that performed a query on common objects. This was an often lengthy process that required knowledge of how ADSI uses LDAP search filters to resolve a query.

Definition

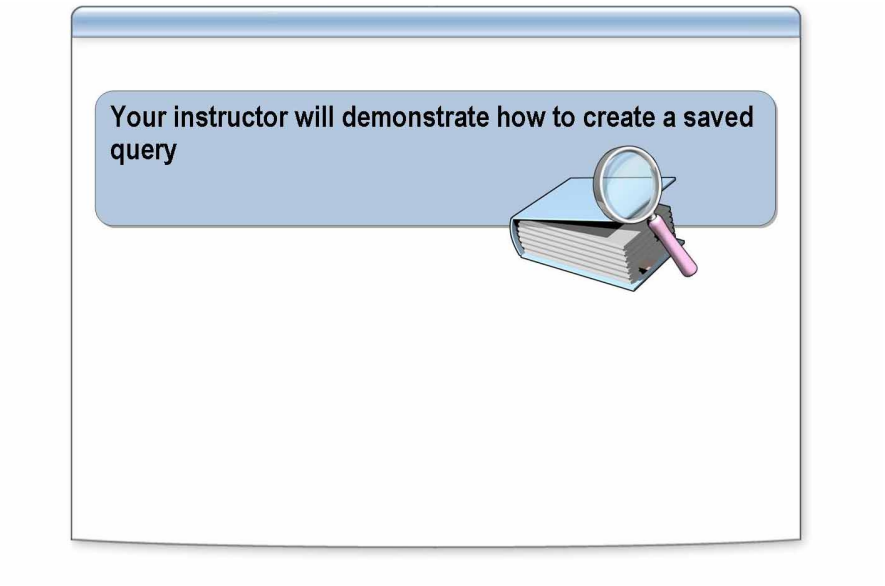
Saved queries use predefined LDAP strings to search only the specified domain partition. You can narrow searches to a single container object. You can also create a customized saved query that contains an LDAP search filter.

All queries are located in the Saved Queries folder called dsa.msc, which is stored in Active Directory Users and Computers. After you successfully create your customized set of queries, you can copy the .msc file to other Windows Server 2003 domain controllers that are in the same domain and reuse the same set of saved queries. You can also export saved queries to an Extensible Markup Language (XML) file. You can then import them into other Active Directory Users and Computers consoles located on Windows Server 2003 domain controllers that are in the same domain.

Additional Reading

For more information about saved queries see “Using saved queries” at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/usingsavedqueries.asp.

How to Create a Saved Query



Introduction

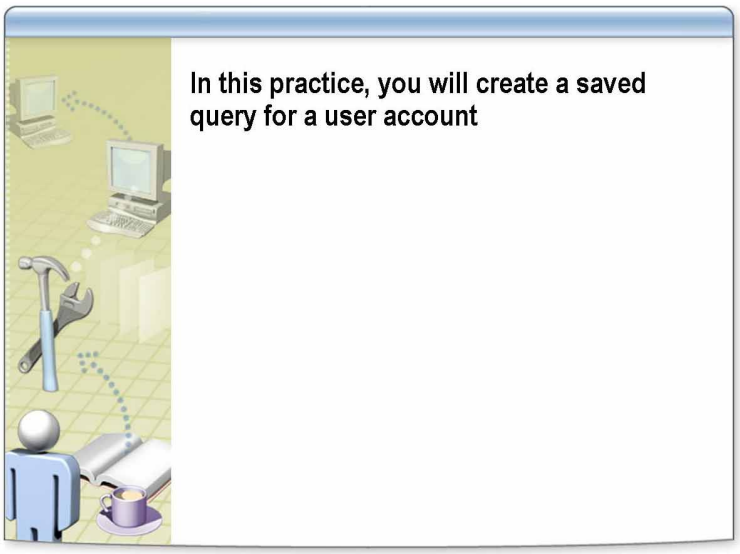
You can save queries to search for disabled user or computer accounts, number of days since the last user logon, users with passwords that do not expire, and many other commonly used queries. After a saved query is executed and the desired objects are displayed, you can then modify each object directly in the **Query results** box.

Procedure

To create a saved query:

1. In Active Directory Users and Computers, in the console tree, right-click **Saved Queries** or any of its subfolders in which you want to save a query, point to **New**, and then click **Query**.
2. In the **New Query** dialog box, in the **Name** box , type a query name.
3. In the **Description** box, type a query description.
4. Click **Browse** to define the container from which to begin your search.
5. To search all subcontainers of the selected container, select the **Include subcontainers** check box.
6. Click **Define Query** to define your query.

Practice: Creating Saved Queries



Objectives

In this practice, you will create a saved query for a user account.

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

You discover that you often search for the same information. You want to save searches for future use. Create a saved query for a user account. The saved query must have the following properties:

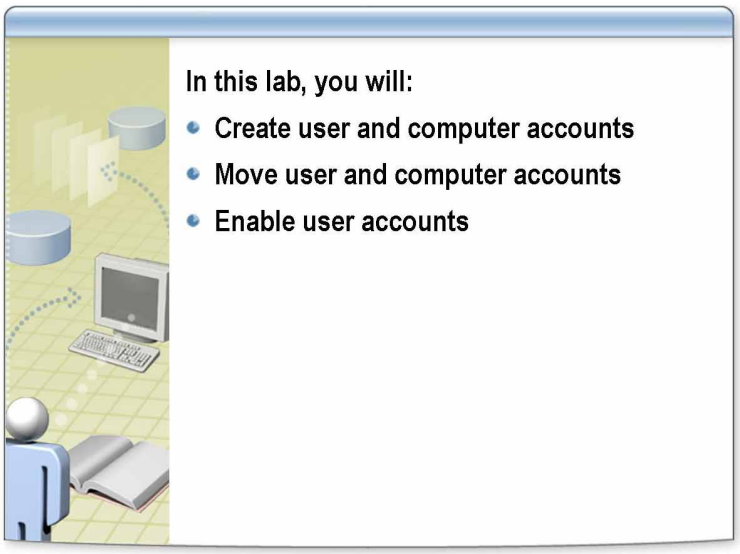
- The saved query is named *ComputerName* User Account.
- The saved query is saved in the Users container in the NWTraders domain.
- The City value equals your computer name that equals your computer name.

Practice

► **Create a saved query**

1. In Active Directory Users and Computers, right-click **Saved Queries**, click **New**, and then click **Query**.
2. In the **New Query** dialog box, create a query with the following parameters:
   - Name: *ComputerName* **User Accounts**
   - Description: *ComputerName* **User Accounts**
3. Click **Define Query**.
4. In the **Find** box, click **Users, Contacts, and Groups**.
5. On the **Advanced** tab, click **Field**, point to **User**, and then click **City**.
6. Verify that **Starts with** is in the **Condition** box.
7. In the **Value** box, type *ComputerName* and then click **Add**.
8. Click **OK** to close the **Find Users, Contacts, and Groups** dialog box.
9. Click **OK** to close the **New Query** dialog box.
10. Right-click the query, and then click **Refresh** to refresh the saved query.

Lab A: Managing User and Computer Accounts



Objectives

After completing this lab, you will be able to:

- Create user and computer accounts.
- Move user and computer accounts to a new organizational unit.
- Enable user accounts.

Lab setup

This lab requires that your computer has:

- 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.
- An organizational unit called Locations/*ComputerName*/Computers/Desktops.
- An organizational unit called Locations/*ComputerName*/Computers/Laptops.

Estimated time to complete this lab: 30 minutes

Exercise 1
Creating User Accounts

In this exercise, you will create two user accounts.

Scenario

You have been given a list of users that need to be added to Active Directory. Find the users on the list that have an office in your city location and add them to the appropriate organizational unit in your city organizational unit.

Tasks	Specific Instructions
1. Create user accounts.	▪ Create user accounts in the nwtraders.msft/Locations/*ComputerName*/Users organizational unit. ▪ Create the accounts for the users in the following table that match your organization's city location by using the following parameters: • First name: *FirstName* • Last name: *LastName* • User logon name: The first three letters of the first name and the first three letters of the last name • User logon name (pre-Windows 2000): The first three letters of the first name and the first three letters of the last name • Password: **P@ssw0rd** • Disable the user account
2. Modify the user accounts.	▪ City: *ComputerName* ▪ Telephone number: **555-2469** ▪ Manager: *ComputerName***User**

Last name, First name	City
Brown, Robert	Acapulco
Browne, Kevin F.	Acapulco
Byham, Richard A.	Auckland
Calafato, Ryan	Auckland
Berg, Karen	Bangalore
Berge, Karen	Bangalore
Barnhill, Josh	Bonn
Barr, Adam	Bonn
Altman, Gary E. III	Brisbane
Anderson, Nancy	Brisbane
Chapman, Greg	Caracas
Charles, Mathew	Caracas

(*continued*)

Last name, First name	City
Bonifaz, Luis	Casablanca
Boseman, Randall	Casablanca
Ackerman, Pilar	Denver
Adams, Jay	Denver
Connelly, Peter	Khartoum
Conroy, Stephanie	Khartoum
Barreto de Mattos, Paula	Lima
Bashary, Shay	Lima
Arthur, John	Lisbon
Ashton, Chris	Lisbon
Bankert, Julie	Manila
Clark, Brian	Manila
Burke, Brian	Miami
Burlacu, Ovidiu	Miami
Chor, Anthony	Montevideo
Ciccu, Alice	Montevideo
Casselman, Kevin A.	Moscow
Cavallari, Matthew J.	Moscow
Cornelsen, Ryan	Nairobi
Cox, Brian	Nairobi
Alberts, Amy E.	Perth
Alderson, Gregory F. (Greg)	Perth
Benshoof, Wanida	Santiago
Benson, Max	Santiago
Bezio, Marin	Singapore
Bischoff, Jimmy	Singapore
Carothers, Andy	Stockholm
Carroll, Matthew	Stockholm
Cannon, Chris	Suva
Canuto, Suzana De Abreu A.	Suva
Combel, Craig M.	Tokyo
Con, Aaron	Tokyo
Bradley, David M.	Tunis
Bready, Richard	Tunis
Abolrous, Sam	Vancouver
Acevedo, Humberto	Vancouver

Exercise 2
Creating Computer Accounts

In this exercise, you will create 10 computer accounts.

Scenario

You are expecting to receive four new laptop computers and five new desktop computers in your location. A consultant with a user account in the domain will add these computers to the domain. Northwind Traders policy states that the laptop and desktop computers will be managed by the administrators of the city organizational unit.

Tasks	Special instructions
1. Create five desktop computers.	▪ Create accounts in the nwtraders.msft/Locations/*ComputerName*/Computers/Desktops organizational unit. ▪ Add the following five computer accounts: 01*ComputerName*Desk, 02*ComputerName*Desk, 03*ComputerName*Desk, 04*ComputerName*Desk, 05*ComputerName*Desk
2. Create five laptop computers.	▪ Create accounts in the nwtraders.msft/Locations/*ComputerName*/Computers/Laptops organizational unit. ▪ Add the following five computer accounts: 01*ComputerName*Lap, 02*ComputerName*Lap, *C*03*omputerName*Lap, 04*ComputerName*Lap, 05*ComputerName*Lap

Exercise 3
Searching for and Moving Users Accounts

In this exercise, you will search for users in your city location and move them to the *ComputerName*/Users organizational unit.

Scenario

The system engineers at NorthWind Traders have imported user accounts for the entire nwtraders domain. The system administrators are responsible for searching for the user accounts that have a city location attribute of their *ComputerName* and move the account to the Users folder in their *ComputerName* organizational unit.

Tasks	Special instructions
1. Search for user accounts by using the following advanced search criteria.	▪ Starting point for the search: nwtraders.msft ▪ Find: **Users, Contacts, and Groups** ▪ Field: **City** ▪ Condition: **Is (exactly)** ▪ Value: *ComputerName*
2. Move user accounts to the following location.	▪ Nwtraders.msft/Locations/*ComputerName*/Users

Exercise 4
Searching for and Moving Computer Accounts

In this exercise, you will search for computer accounts whose names have the first three letters of your computer name and move them to your *ComputerName*/Computers organizational unit.

Scenario

The system engineers at NorthWind Traders have imported computer accounts for the entire nwtraders domain. The system administrators are responsible for searching for the computer accounts that have the first three letters of their *ComputerName* and move the account to the Computers folder in their *ComputerName* organizational unit.

Tasks	Special instructions
1. Search for computer accounts by using the following advanced search criteria.	▪ Starting point for the search: nwtraders.msft ▪ Find: **Computers** ▪ Field: **Computer name (pre-Windows 2000)** ▪ Condition: **Starts with** ▪ Value: The first three letters of your computer name
2. Move computer accounts to the following location.	▪ Nwtraders.msft/Locations/*ComputerName*/Computers

Exercise 5
Searching for and Enabling User Accounts

In this exercise, you will enable user and computer accounts in your city organizational unit.

Scenario

The system engineers at NorthWind Traders have imported user account for the entire nwtraders domain. The system administrators are responsible for searching user accounts that have a city location attribute of their *ComputerName* and then enabling the accounts so that the users can logon.

Tasks	Special instructions
1. Search for disabled user accounts in the following location.	▪ Nwtraders.msft/Locations/*ComputerName*/Users
2. Enable all disabled user accounts.	