

# 2

## CHAPTER TWO

# Administering Computer Accounts and Resources in Active Directory

---

### Terms you'll need to understand:

- ✓ Domains
- ✓ Domain Trees
- ✓ Domain Forests
- ✓ Computer accounts
- ✓ Run As feature
- ✓ Globally unique identifiers (GUIDs)
- ✓ Organizational units (OUs)
- ✓ Microsoft Management Console (MMC) 3.0
- ✓ Active Directory Users and Computers console

---

### Techniques you'll need to master:

- ✓ Adding and removing computer accounts
- ✓ Prestaging computer accounts
- ✓ Using command-line tools for modifying Active Directory objects
- ✓ Using the Action Pane in the MMC 3.0
- ✓ Enabling full functionality for MMC 3.0
- ✓ Managing resources using the Run As command

Microsoft introduced Active Directory with the debut of Windows 2000 Server in February 2000. Active Directory provides a directory service for Microsoft-based networks in the same way that Novell Directory Services (NDS) provides a directory service for NetWare environments. For Windows Server 2003, Microsoft enhanced and refined Active Directory by making the directory service more flexible, more scalable, and more manageable than its Windows 2000 predecessor. Active Directory is a vital element in Windows Server 2003, and its many benefits can offer a compelling reason to upgrade, especially if you are coming from a Windows NT Server environment.

Understanding how to manage objects within Active Directory is critical for a successful deployment and reliable day-to-day operations of a Windows Server 2003 Active Directory–based network. In this chapter, we introduce you to Active Directory for Windows Server 2003. You’ll discover how to add, remove, and manage computer accounts in Active Directory. Unfortunately, network administration doesn’t always go smoothly, so you’ll also learn about how to troubleshoot computer accounts in Windows Server 2003 and Active Directory.

Microsoft released Windows Server 2003 Service Pack 1 (SP1) on March 2004, as a major update. In December 2005, Microsoft published the R2 (Release 2) Edition of Windows Server 2003, in 32-bit (x86) and 64-bit (x64) versions. This chapter and this book covers all of these different permutations of the Windows Server 2003 operating system—the original Release to Manufacturing (RTM) version, SP1, and R2 in both the 32-bit (x86) and 64-bit (x64) flavors. The functionality and features covered in this book apply to all of these editions, except where noted.

## Introduction to Active Directory

The many improvements to Active Directory encompass some of the major feature enhancements of Windows Server 2003. Active Directory is a replicated and distributed database that stores computer-related information such as usernames, passwords, phone numbers, addresses, email addresses, group names, and computer names, to name a few. Active Directory is called a directory service because it provides users and computers with the ability to look up information in a similar way that you look up information using a telephone book directory.

Special servers called domain controllers (DCs) are designated to store a copy of the Active Directory database, and these DCs are responsible for synchronizing the Active Directory database with all of the other DCs that share the database. Server computers, as well as workstation computers that are members of an Active Directory domain, perform several Active Directory queries (or lookups) in their day-to-day operations. For example, Active Directory domain-member computers need to know where nearby DCs are for authentication purposes.

Active Directory is based on open, Internet-related standards, such as the Transmission Control Protocol/Internet Protocol (TCP/IP), the Domain Name System (DNS), the Kerberos authentication protocol, and the Lightweight Directory Access Protocol (LDAP), among many others. In fact, you cannot install Active Directory without TCP/IP and DNS installed and functioning within the network environment. You must name Active Directory domains using a full DNS name such as `examcram2.informit.com`.

## Domains, Domain Trees, and Domain Forests

A Windows Server 2003 computer (or a Windows 2000 Server computer) becomes a DC when an administrator runs the Active Directory Installation Wizard. You can run the wizard by clicking Start, Run; typing `dcpromo.exe`; and clicking OK. This process promotes a server to a DC. The wizard makes several changes to the server computer to prepare it to become a DC. One of the major changes is the creation of the Active Directory database file itself. This file is named `ntds.dit`, and it must reside on a hard disk partition or volume that is formatted as NTFS. The default location for the `ntds.dit` file is the `%systemroot%\ntds` folder (for example, `c:\windows\ntds`).

The very first Windows Server 2003 (or Windows 2000 Server) DC that you promote creates the *root domain*. For example, if you promote a DC and name the domain `examcram2.net`, this domain becomes the root domain within the new Active Directory forest. The basic logical components of Active Directory are as follows:

- ▶ *Domain*—One or more DC servers and a group of users and computers that share the same Active Directory database for authentication and can share common server resources.
- ▶ *Domain Tree*—One or more Active Directory domains that share a common hierarchical DNS namespace (parent-child-grandchild and so on). For example, `examcram2.net` could be the parent domain, `northamerica.examcram2.net` could be the child domain, `us.northamerica.examcram2.net` could be the grandchild domain, and so on.
- ▶ *Domain Forest*—One or more Active Directory domain trees (each tree has its own DNS namespace) that share the same Active Directory database. An Active Directory forest is a logical container for one or more related domains.

### No Primary or Backup Domain Controllers

Windows NT Server 3.5x and Windows NT Server 4.0 used the concept of one primary DC (PDC) and backup DCs (BDCs), where only one of the DCs could act as the PDC at any one time. The PDC stores the read/write copy of the security

accounts manager (SAM) database, whereas each BDC stores a read-only copy of the SAM database. Instead, Active Directory uses a technique called *multimaster replication* to distribute copies of the Active Directory database to all other DCs that share the same Active Directory namespace. This replication technology means that administrators can make additions, changes, or deletions to the Active Directory database from any DC, and those modifications get synchronized with all of the other DCs within an Active Directory domain and the GCs within the entire AD forest. Active Directory assigns the role of PDC Emulator to the first DC to come online in an Active Directory forest. The DC that has the PDC Emulator role can communicate between Active Directory and down-level PDCs and BDCs running on Windows NT Server 3.5x and Windows NT Server 4.0.

## Organizational Units

To improve network administration, Microsoft created organizational units (OUs) to provide for logical groupings of users, groups, computers, and other objects within a single domain. You can delegate administrative authority over each OU to other administrators for distributing network-management chores. The delegated authority can be limited in scope, if necessary, so that you can grant junior administrators just specific administrative powers—not complete administrator-level authority. In addition, you can apply specific group policy object (GPO) settings at the OU level, allowing users and computers to be managed differently according to the OU in which they are placed.

## The Microsoft Management Console (MMC)

The MMC is the standard interface for hosting all of the various GUI tools and utilities that administrators use to manage the Windows and Active Directory environments. The MMC is a shell that houses MMC snap-ins—the snap-ins actually provide the functionality. The MMC provides a consistent and standardized *look and feel* for all the snap-in tools. MMC snap-in files use the file extension `.msc`. You can see several of the default snap-ins if you browse the `%systemroot%\system32` folder on a Windows Server 2003 computer.

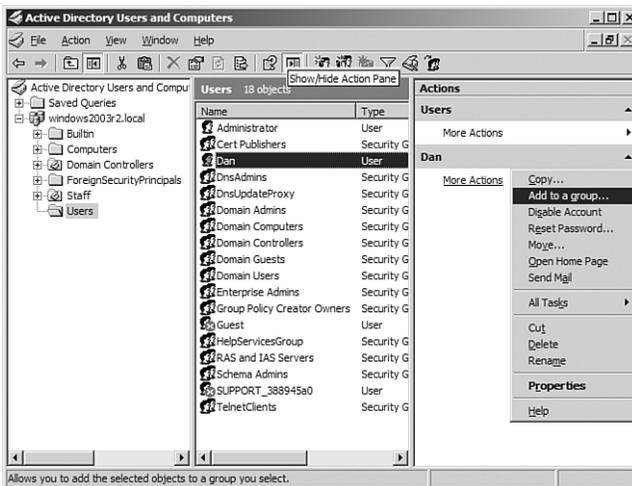
For example, on a domain controller, you can run the Active Directory Users and Computers (ADUC) snap-in by double-clicking the `dsa.msc` file in the `%systemroot%\system32` folder. Alternatively, you can run the ADUC snap-in by clicking Start, Run, typing in `dsa.msc`, and clicking OK. You must include the `.msc` file extension for the snap-in to run. You also have the option of clicking Start, Run, typing in `mmc`, and clicking OK to display an empty console; you can then click File, Add/Remove Snap-in to load the snap-in(s) of your choice.

## MMC 3.0

**New to R2**

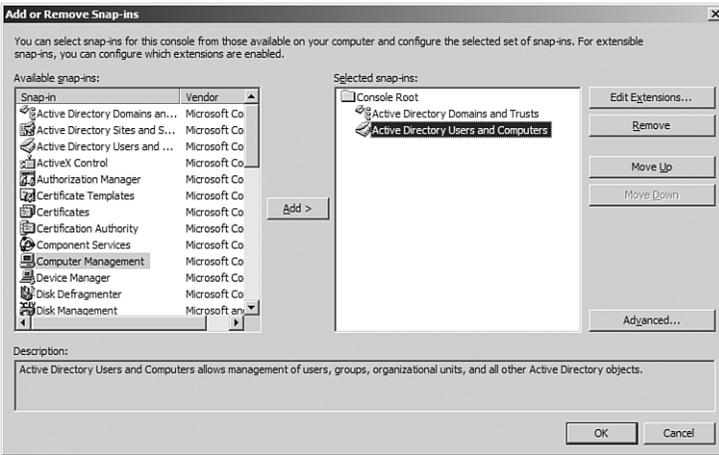
When you upgrade Windows Server 2003 to the R2 Edition, the MMC gets upgraded to version 3.0 automatically. The MMC 3.0 sports three major improvements over its previous versions:

- ▶ *The Action pane*—The Action pane is displayed on the right side of the console when it is not hidden. (It is usually hidden by default on most snap-ins.) The *Show/Hide Action Pane* toolbar icon shown in Figure 2.1 is similar to the *Show/Hide Console Tree* toolbar icon. The Action pane displays the actions that can be performed on the currently selected item in the console tree (left pane) or in the results pane (center pane). You can view the same list of actions by right-clicking an item.



**FIGURE 2.1** A view of the Action pane for the ADUC snap-in under MMC 3.0 and Windows Server 2003 R2.

- ▶ *Enhanced Error Handling*—MMC 3.0 notifies you when errors occur within loaded snap-ins that could cause the MMC shell to stop responding. When the MMC 3.0 detects an error, it offers you some options to deal with the error.
- ▶ *Improved Add or Remove Snap-in dialog box*—The redesigned Add or Remove Snap-in dialog box for the MMC 3.0 makes it easier to add, remove, and organize snap-ins (see Figure 2.2).



**FIGURE 2.2** The Add or Remove Snap-ins dialog box under MMC 3.0 and Windows Server 2003 R2.

### EXAM ALERT

To enable MMC 3.0 features such as the new *Add or Remove Snap-in* dialog box, you must add a new subkey to the Windows Registry.

*Always have a good, recent backup of your system before you endeavor to make any change to the Registry.*

Using `regedit.exe`, the Windows Registry editor tool, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC`. You must add a new subkey named `UseNewUI` under this existing Registry key to turn on the enhancements to MMC 3.0. No reboot is necessary; the change is effective immediately.

### TIP

#### New to R2

MMC 3.0 supports a wider range of functionality than previous versions of the MMC; however, MMC snap-ins must support the new MMC 3.0 features for the enhanced functionality to be available.

## Administering Computer Accounts in Active Directory

Computers, such as workstations and member servers, must be authenticated to access Active Directory resources under Windows Server 2003, just as they must be authenticated under Active Directory in Windows 2000 Server. To become a

participant in an Active Directory domain, Windows NT, Windows 2000, Windows XP, and other Windows Server 2003 computers must formally join a domain by establishing a computer account within the domain. Windows 95 and Windows 98 (Windows 9x) computers cannot formally join a domain; however, users can log on to a Windows Server 2003 Active Directory domain and access resources as if it were a Windows NT 4.0 domain under both the Windows 2000 mixed and the Windows 2000 native domain functional levels. Windows Server 2003 domain functional levels are discussed in Chapter 5, “Managing Access to Resources.”

## The Active Directory Client for Windows 9x and Windows NT 4.0

The Windows 2000 mixed domain functional level supports the NTLM (NT LAN Manager) authentication protocol that is used by Windows NT BDCs to authenticate users and computers. The older LM (LAN Manager) authentication protocol and the NTLM protocol are responsible for authenticating Windows 9x- and Windows NT-based computers. Windows 2000 mixed also supports the newer Kerberos authentication protocol that is used by the Windows 2000 native and the Windows Server 2003 domain functional levels. In addition to Kerberos, the Windows 2000 native and the Windows Server 2003 functional levels support the newer NTLM version 2 (NTLM v2) authentication protocol. Windows 9x computers do not natively support NTLM v2, nor do Windows NT 4.0 computers unless they have Service Pack 4 (SP4) or higher installed. Windows 9x and Windows NT 4.0 computers can natively log on to a Windows Server 2003 Active Directory domain in the following circumstances:

- ▶ The Windows Server 2003 domain is set at Windows 2000 mixed and either a PDC emulator or a Windows NT 4.0 BDC is available.
- ▶ The Windows Server 2003 domain is set at Windows 2003 interim and either a PDC emulator or a Windows NT 4.0 BDC is available.

### NOTE

When Windows 9x computers log on to a Windows NT 4.0 domain, they can only access Active Directory resources via one-way trust relationships that have been set up by network administrators with Windows Server 2003 Active Directory domains.

To add support for Windows 9x and Windows NT 4.0 computers to access Active Directory resources, you can install the Active Directory client software so that

these legacy clients can access resources stored in Windows Server 2003 domains. The Active Directory client software (`dscclient.exe`) for Windows 9x computers is located on the Windows 2000 Server CD-ROM (it's *not* on the Windows Server 2003 CD-ROM) in the `Clients\Win9x` folder. The Windows NT 4.0 version of the Active Directory client is available from Microsoft's website at <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp>.

## Creating Computer Accounts

You can create computer accounts in one of three ways:

- ▶ Log onto each (Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, or Windows Server 2003) computer and join it to the domain.
- ▶ Prestage the computer accounts on a DC using the Active Directory Users and Computers (ADUC) MMC snap-in.
- ▶ Prestage the computer accounts on a DC using the `dsadd.exe` command-line utility.
- ▶ Prestage the computer accounts on a DC using some other scripted or command-line utility.

For computers running Windows NT, Windows 2000, Windows XP, Windows Vista, and Windows Server 2003, you create accounts for those computers when you join them to the Windows Server 2003 Active Directory domain, provided that computer accounts for those computers have not been prestaged. For example, on a Windows 2000 (Professional or Server) system, you join the computer to a domain by following these steps:

1. Double-click the System icon in the Control Panel.
2. Click the Network Identification tab from the System Properties window.
3. Click the Properties button.
4. Click the Domain option button, type in the name of the Active Directory domain that you want to join, and click OK.
5. Type in the name and password for a user account in the domain that has administrative-level permission to join computers to this domain and click OK (see Figure 2.3).
6. Click OK for the Welcome message box that confirms you have successfully joined the computer to the domain.



**FIGURE 2.3** Joining a Windows 2000 computer to a Windows Server 2003 Active Directory domain.

## Troubleshooting Joining a Computer to a Domain

If you have difficulty joining the domain, be sure to check the computer for any physical network connectivity problems. If you verify that the physical network connection is functioning properly, use the TCP/IP ping command at a command prompt window to test the connectivity to a domain controller by pinging the DC's IP address. For example, you can type `ping 192.168.0.10` at a command prompt if the DC's IP address is 192.168.0.10. If that works, attempt to ping the DC by its fully qualified domain name (FQDN)—for example, `ping dc1.windows2003.local`.

Using the FQDN for the DC should uncover a DNS name resolution problem, if one exists. If you simply try to ping the server's NetBIOS or hostname by typing `ping dc1`, the name could be resolved by a NetBIOS broadcast, making you think that DNS name resolution is not a problem. If pinging the FQDN does not work, you might very well have a DNS name-resolution problem. You should check the computer's DNS server settings as well as the network's DNS setup. Perhaps the computer is not registered with an appropriate DNS server on your network. If you verify that the computer's DNS server settings are pointed to the appropriate DNS server(s), you can remedy a DNS registration issue on Windows 2000/XP/Vista/2003 computers by performing these steps:

1. Open a command prompt window.
2. Type `ipconfig /flushdns` and press Enter.
3. Type `ipconfig /registerdns` and press Enter.
4. Restart the computer to ensure that these changes take effect.

## Prestaging Computer Accounts from the GUI

You can use the ADUC console to view, add, modify, and delete computer accounts, user accounts, and groups from the Windows GUI. On a Windows Server 2003 DC computer, click Start, Administrative Tools, Active Directory Users and Computers to launch the ADUC console. You can also click Start, Run; type `dsa.msc`; and click OK to run the ADUC console. By creating a computer account in Active Directory before the computer joins the domain, you can

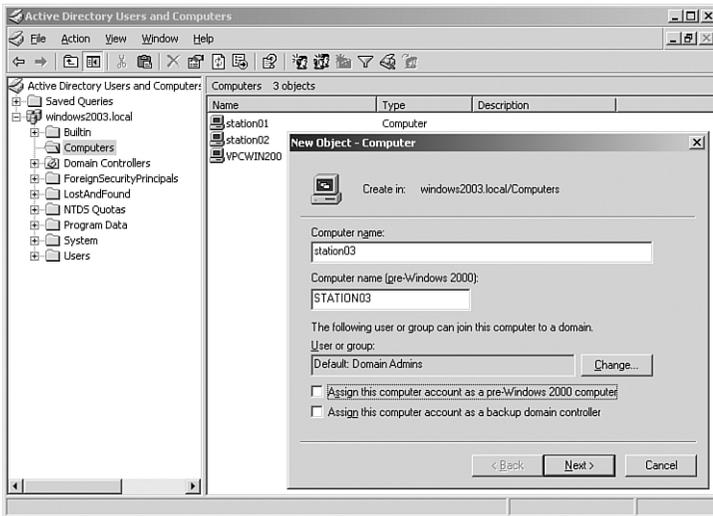
determine exactly where in the directory the computer account will be placed. The default location for computers joined to a domain without prestaging is the Computers container. In addition, prestaging computer accounts gives administrators more control over Remote Installation Services (RIS) installations. You can specify that only prestaged computer accounts can be installed via RIS.

**TIP**

You can install the Windows Server 2003 Administration Tools Pack on a Windows XP Professional computer with SP1 or higher or on a Windows Server 2003 member server so that you can manage Active Directory without physically logging on to a DC. You can download the Windows Server 2003 Administration Tools Pack from Microsoft's website at <http://microsoft.com/downloads/details.aspx?familyid=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en>.

For a new Active Directory domain, the default containers are Built-in, Computers, Domain Controllers, Foreign Security Principals, and Users. If you click the ADUC's View menu and select Advanced Features, you can view the advanced containers that are hidden by default. The advanced containers are LostAndFound, NTDS Quotas, Program Data, and System. To create a new computer account in the ADUC, follow these steps:

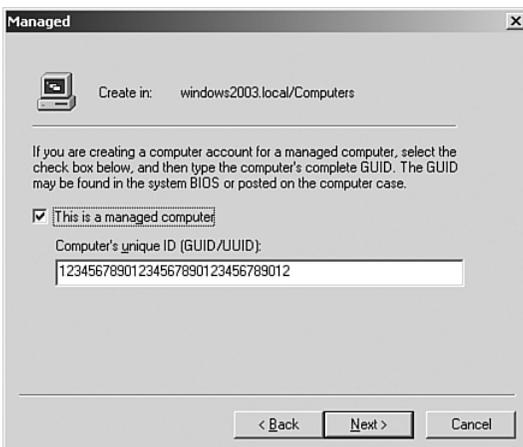
1. Open the ADUC MMC snap-in (console).
2. Right-click the container or OU into which you want to place the computer account, select New, and then click Computer.
3. Type in the computer name.
4. Type in the pre-Windows 2000 computer name, if different from the computer name.
5. To change the user or group that has permission to join computers to the domain, click the Change button. The default group is the Domain Admins group: Any member of this group has authority to join computer accounts to the domain.
6. If this computer account is a Windows NT computer, mark the Assign This Computer Account as a Pre-Windows 2000 Computer check box.
7. If this computer account is for a Windows NT BDC computer, mark the Assign This Computer Account as a Backup Domain Controller check box (see Figure 2.4).



**FIGURE 2.4** Creating a new computer account in ADUC.

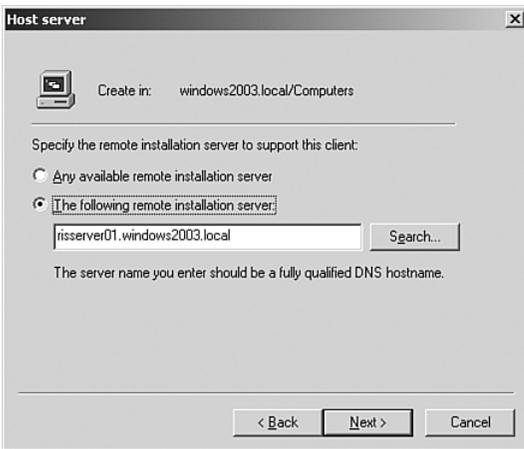
8. Click Next.

9. If you are prestaging the computer account for later installation via RIS, mark the **This Is a Managed Computer** check box and type in the computer's unique ID (GUID/UUID), referred to as its globally unique identifier or its universally unique identifier. This extra security measure prevents unauthorized RIS client installations because only computers with matching GUIDs are allowed to be installed via RIS when you follow this procedure. You can find the GUID or UUID in the computer's BIOS or by using a third-party software utility (see Figure 2.5).



**FIGURE 2.5** Specifying a computer's GUID for prestaging a computer account.

10. Click Next.
11. Select an option for specifying the type of RIS server support for this computer account:
  - ▶ Any Available Remote Installation Server
  - ▶ The Following Remote Installation Server
12. To specify a particular RIS server, select The Following Remote Installation Server option and type in the fully qualified DNS hostname, or click the Search button to locate the server (see Figure 2.6).



**FIGURE 2.6** Specifying the RIS server's name for prestaging a computer account.

13. Click Next.
14. Click Finish for the New Object-Computer summary window.

## Prestaging Computer Accounts from the Command Line

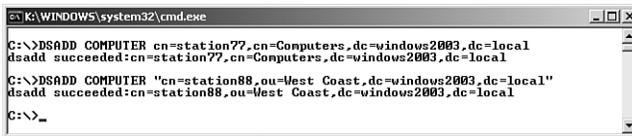
Windows Server 2003 offers several new command-line tools for working with Active Directory. For a detailed list of these commands and their functions, see the section “Using Command-Line Utilities for Active Directory Objects” later in this chapter. You can use the `dsadd.exe` tool to add Active Directory objects such as computer accounts from any Windows Server 2003 command prompt. With `dsadd.exe`, you can add one computer account at a time from the command line, or you can redirect standard input for `dsadd.exe` and use a text file that contains the computer account that you want added. For parameters with embedded spaces, such as names of OUs, surround the DN with quotes. The following two examples in Table 2.1 and in Figure 2.7 demonstrate some of the possibilities and their associated syntax for adding computer accounts via the command line.

**TABLE 2.1** Examples of the `dsadd.exe` Command

<b>dsadd Command</b>	<b>dsadd Results</b>
<code>dsadd computer cn=station77,cn=Computers, dc=windows2003,dc=local</code>	Adds a computer account named <code>station77</code> to Active Directory in the <code>Computers</code> container for the domain named <code>windows2003.local</code> .
<code>dsadd computer "cn=station88,ou=west coast, dc=windows2003,dc=local"</code>	Adds a computer account named <code>station88</code> to Active Directory in the <code>West Coast</code> OU for the domain named <code>windows2003.local</code> .

**NOTE**

Computer account NetBIOS names cannot be longer than 15 characters and these names are resolved by network broadcasts, local LMHOSTS file entries, or by Windows Internet Naming Service (WINS) servers; computer account host names can be up to 63 characters in length and these names are resolved via the Domain Name System (DNS) or local HOSTS file entries. A fully qualified domain name (FQDN) for a computer account can be up to 255 characters in length, such as `server01.sales.northamerica.microsoft.com`.



```

C:\K:\WINDOWS\system32\cmd.exe
C:\>DSADD COMPUTER cn=station77,cn=Computers,dc=windows2003,dc=local
dsadd succeeded:cn=station77,cn=Computers,dc=windows2003,dc=local
C:\>DSADD COMPUTER "cn=station88,ou=West Coast,dc=windows2003,dc=local"
dsadd succeeded:cn=station88,ou=West Coast,dc=windows2003,dc=local
C:\>_

```

**FIGURE 2.7** Adding computer accounts using the `dsadd.exe` command.

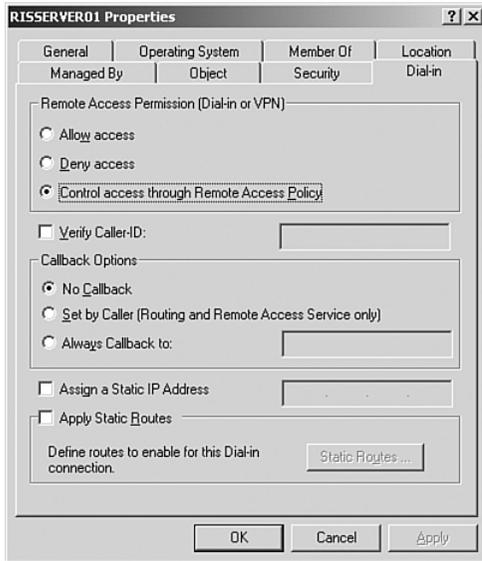
## Managing and Troubleshooting Computer Accounts

You can manage problems with computer accounts from the ADUC console. To modify the properties of a computer account, right-click the computer name listed in the ADUC console and select `Properties`. From the properties sheet, you can make several changes to the account such as trusting the computer for delegation, viewing which operating system the computer is running, adding or removing group memberships, and modifying security permissions and dial-in permissions (see Figure 2.8), among other options.

### Administering and Troubleshooting Computer Accounts

You can easily move one or several computer accounts from one container to another container under Windows Server 2003. The ADUC console supports both cut and paste and drag-and-drop functionality by default. You can select one or more computer accounts, right-click the accounts, and select `Cut` from the right-click menu. Alternatively, you can click and drag one or more selected

computer accounts and drop the accounts into a different container. As a third option, you can select one or more computer accounts, right-click the accounts, and select Move. When the Move dialog box appears, select the Active Directory container where you want the accounts moved and click OK.



**FIGURE 2.8** Working with dial-in properties for a computer account.

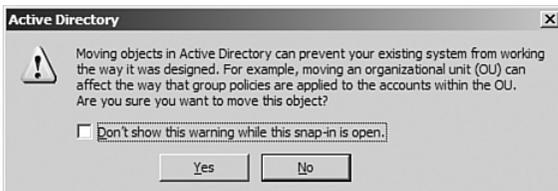
## EXAM ALERT

New to **SP1**

New to **R2**

Under the SP1 and R2 updates to Windows Server 2003, you now receive a confirmation message box, by default, each time that you drag and drop one or more Active Directory objects within the ADUC console (see Figure 2.9). You can turn off this default message by marking the Don't show this warning while this snap-in is open check box.

An administrator also has the option to *disable* drag and drop functionality within the ADUC under SP1 and R2 by setting the *flags* attribute for the *Display Specifiers* container. You can use the *ADSIedit.msc* MMC snap-in tool to set the *flags* attribute in Active Directory at the following location: *CN=DisplaySpecifiers,CN=Configuration,DC=<domain name>*. Setting the *flags* attribute to *any* value disables drag and drop functionality. The default configuration for SP1 and R2 is that the value is *not* set, which enables administrators to drag and drop objects in the ADUC.



**FIGURE 2.9** An Active Directory confirmation message box appears by default whenever you attempt to drag and drop one or more objects in the ADUC under Windows Server 2003 SP1 and R2.

In addition to working with the properties sheet for each computer account, you have several administrative tasks available to you when you right-click a computer account, including the following:

- ▶ *Name Mappings*—This option maps X.509 security certificates and Kerberos names for the computer account.
- ▶ *Disable Account*—This option prevents any users from logging on to the domain from the computer account. After you select this option, it toggles to read *Enable Account*, which you can later use for re-enabling the computer account.
- ▶ *Reset Account*—This option changes the computer account password that is used to authenticate the computer on the domain. If you reset a computer account, you must rejoin the computer to the domain.
- ▶ *Move*—This option allows you to relocate the computer account to a different container or OU.
- ▶ *Manage*—This option launches the Computer Management console for remotely administering the selected computer.
- ▶ *All Tasks, Resultant Set of Policy (Planning)*—This option lets you view simulated policy settings for a selected computer or a selected user.
- ▶ *All Tasks, Resultant Set of Policy (Logging)*—This option lets you view policy settings for a specific computer on the network.

## TIP

Windows 2000, Windows XP Professional, Windows Vista, and Windows Server 2003 computers that are members of an Active Directory domain communicate with a DC using what's known as a secure channel. The secure channel's password is stored with the computer account on the domain controller. For Windows 2000, Windows XP, and Windows Server 2003 computers, the system-generated computer account password is automatically changed every 30 days by default. If, for some reason, the password stored on the domain member computer cannot be validated against the password stored on the DC, the Netlogon service generates one or both of the following errors on the domain member computer:

*The session setup from the computer DOMAINMEMBER failed to authenticate. The name of the account referenced in the security database is DOMAINMEMBER\$. The following error occurred: Access is denied.*

*NETLOGON Event ID 3210:*

*Failed to authenticate with \\DOMAINDC, a Windows NT domain controller for domain DOMAIN.*

Either one or both of these errors indicate that you need to reset the computer account.

# Using Command-Line Utilities for Active Directory Objects

Microsoft added several useful command-line tools for managing Active Directory and Active Directory objects. In this chapter, you've already learned how to use the `dsadd` command for adding new computers, but `dsadd` can do more than just add computers and groups. You can use these new command-line utilities for Active Directory both locally and remotely, provided that you possess the necessary security permissions for the task that you are trying to complete. The following list details the commands that are available and discusses how you can use them:

- ▶ ***DSADD.exe***—This command adds a single computer, contact, group, OU, user, or quota specification to Active Directory. For help with the specific parameters and syntax for each type of object, type `dsadd ObjectType /?` at a command prompt. For example, `dsadd user /?` displays the available parameters (options) and syntax for adding a user to Active Directory.
- ▶ ***DSGET.exe***—This command displays the properties for computers, contacts, groups, OUs, partitions, quotas, servers (DCs), sites, subnets, and users in Active Directory. For help with the specific parameters and syntax for each type of object, type `dsget ObjectType /?` at a command prompt. For example, `dsget server /?` displays the available parameters (options) and syntax for viewing the properties of a specific domain controller.
- ▶ ***DSMOD.exe***—This command modifies the properties of a single computer, contact, group, OU, partition, quota, server, or user. For help with the specific parameters and syntax for each type of object, type `dsmod ObjectType /?` at a command prompt. For example, `dsmod group /?` displays the available parameters (options) and syntax for changing the properties of a specific group, including the ability to change the group type and group scope and adding or removing users.
- ▶ ***DSMOVE.exe***—This command moves or renames a single object within Active Directory. For help with the specific parameters and syntax for this command, type `dsmove /?` at a command prompt.
- ▶ ***DSQUERY.exe***—This command allows you to perform a search to locate computers, contacts, groups, OUs, partitions, quotas, servers (DCs), sites, subnets, or users within Active Directory. You can specify search criteria for finding Active Directory objects. The `dsquery *` command can find any type of Active Directory object. For help with the specific

parameters and syntax for each type of object, type `dsquery ObjectType /?` at a command prompt. For example, `dsquery computer /?` displays the available parameters (options) and syntax for finding computers in Active Directory.

- ▶ *DSRM.exe*—This command removes (deletes) objects within Active Directory. For help with the specific parameters and syntax for this command, type `dsrcm /?` at a command prompt.
- ▶ *CSVDE.exe*—This command exports data from Active Directory and imports data into Active Directory using the comma-separated values (CSV) file format. Programs such as Microsoft Excel and Microsoft Exchange Server administration utilities can read and write to CSV files. This tool is Microsoft's preferred method for automating the creation of user accounts in Active Directory using a bulk importing procedure. For help with the specific parameters and syntax for this command, type `csvde` (with no parameters) at a command prompt.
- ▶ *LDIFDE.exe*—This command exports data from Active Directory and imports data into Active Directory using the Lightweight Directory Access Protocol (LDAP) Data Interchange Format (LDIF) file format. The LDIF files use the `.ldf` extension, and you can view and edit them using any simple text editor such as Notepad. For help with the specific parameters and syntax for this command, type `ldifde` (with no parameters) at a command prompt. This tool is not Microsoft's preferred method for automating the creation of user accounts in Active Directory using a bulk importing procedure.

**TIP**

Although it's been around for a long time, the `net` command can still prove useful. To view a list of all the available `net` command options, type `net` and press Enter at a command prompt. To get help on usage, type `net command_name /?` and press Enter. For example, you can view a list of user accounts for the domain by typing `net user` and pressing Enter.

## Managing Resources Using the Run As Command

The Run As feature gives administrators (and other users) the ability to run programs and system utilities under the security credentials of one user while being logged on to the server as a different user. For example, an administrator named DanB can be logged on to a server or a workstation with an ordinary user account

that is only a member of the Domain Users group. While logged on as the ordinary user, DanB, he can right-click any MMC snap-in tool, such as ADUC (`dsa.msc`), and select Run As from the pop-up menu. The Run As dialog box appears with two options to run this program—Current User (with Restricted Access) and the Following User. By selecting the second option and typing in the appropriate administrative username and password (see Figure 2.10), DanB can log in using the alternate credentials without logging out of the machine.



**FIGURE 2.10** Running a program as a different user with the Run As right-click menu option.

You can use the Run As command for all types of programs, utilities, and even Control Panel applets. For using Run As on Control Panel tools, hold down the Shift key while you right-click a Control Panel icon to display the Run As option. You might need to hold down the Shift key while you right-click to access the Run As option for other applications as well. Using Run As is a more secure way for accessing security-sensitive utilities rather than always logging on to systems as a user who is a member of the Administrators group.

You can even use the Run As command to launch an instance of the Windows Explorer under the security credentials of a different user. For example, if you are currently logged on as JoeUser, at a command prompt or at the Start, Run box, you can type `runas /nopprofile /user:domain1\administrator explorer.exe` to launch an Explorer window under the security context of Domain1's Administrator account. Any folders or files that you access from *that* Explorer window are subject to the Access Control List (ACL) for the Administrator user account, not the ACL for JoeUser.

**EXAM ALERT**

Unfortunately, you cannot use the Run As feature for all administrative chores. For instance, if you right-click a network connection icon in the Network Connections folder, Windows Server 2003 does not offer you the Run As option; right-clicking the Printers and Faxes icon in Control Panel does not provide you with the Run As menu option either. So, remember, as convenient as the Run As tool is, you cannot use it in every situation.

## Using Run As from the Command Line

You can also use the Run As feature from a command window, both for GUI tools as well as for command-line tools. For example, you can run the Computer Management console as the administrator for the `Windows2003.local` domain by clicking Start, Run; typing `runas /user:windows2003\administrator "mmc %windir%\system32\compmgmt.msc"` in the Open box; and clicking OK. From a command prompt, you can type `runas /?` and press Enter to view the many options and syntax for this command.

You can also open a command-prompt window as a different user—as the administrator for a domain named `Windows2003.local`, for example—by clicking Start, Run; typing `runas /user:windows2003\administrator cmd.exe` in the Open box; and clicking OK. In addition, you can create shortcuts to administrative tools that require the administrator's password to run. For an example of how to create such a shortcut, follow these steps:

1. Right-click the Windows desktop and select New, Shortcut.
2. Type a command string such as `runas /user:windows2003\administrator "mmc %windir%\system32\compmgmt.msc"` in the Type the Location of the Item box.
3. Click Next.
4. Input a name for the shortcut in the Type a Name for This Shortcut box, such as Admin Computer Mgmt.
5. Click Finish.

When you double-click the shortcut, you are prompted for the administrator password. If you do not type in the correct password for the administrator user account, the program (Computer Management, in this example) does not run.

# Exam Prep Questions

1. What is the default behavior in Windows Server 2003 RTM (Released to Manufacturing) version (pre-SP1 and pre-R2) when you attempt to drag and drop a computer account from the Computers container into an organizational unit using the Active Directory Users and Computers (ADUC) console? (Choose the best answer.)
  - A. Drag and drop functionality is not supported in this version.
  - B. The computer account is moved.
  - C. You are prompted by a message box to confirm or cancel your action.
  - D. It depends on whether an administrator has disabled the drag and drop feature.
2. Which of the following methods can you use to create computer accounts in Active Directory under Windows Server 2003? (Choose three.)
  - A. Log on to a domain from a Windows 98 computer.
  - B. Join a domain from a Windows NT 4.0 computer.
  - C. Prestage a computer account from the ADUC console.
  - D. Prestage a computer account using the `dsget computer` command.
  - E. Prestage a computer account using the `dsadd computer` command.
  - F. Join a domain from a Windows 95 computer with the Active Directory client software installed.
3. How can you take advantage of the increased functionality under MMC 3.0? Choose two. Both answers are required for a complete solution.
  - A. Install SP1 for Windows Server 2003.
  - B. Install R2 for Windows Server 2003.
  - C. Download and install MMC 2.0 from Microsoft's website.
  - D. Add the Value `UseNewUI` to the Windows Registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC`.
  - E. Enable the new functionality by selecting the Add or Remove Snap-in dialog box from the File menu under MMC 3.0.
  - F. Add the subkey `UseNewUI` to the Windows Registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC`.
4. As an administrator for the ExamCram.corp domain, how can you run the Active Directory Users and Computers MMC snap-in? (Choose two.)
  - A. Double-click the file `dsa.mmc` in the `%systemroot%\system32` folder from Windows Explorer.

- B. Click Start, Run, type `aduc.msc`, and click OK.
  - C. Double-click the file `dsa.msc` in the `%systemroot%\system32` folder from Windows Explorer.
  - D. Double-click the file `aduc.msc` in the `%systemroot%\system32` folder from Windows Explorer.
  - E. Click Start, Run, type `mmc`, and click OK. Click File, Add/Remove Snap-in, select Active Directory Users and Computers from the list of available snap-ins, click Add, and then click OK.
5. What happens if you attempt to run an application program using the Run option as a different user than the user who is currently logged on, but you type in an incorrect user name or password? (Choose the best answer.)
- A. The program runs using the security credentials of the currently logged-on user.
  - B. You see a logon failure error message box appear on the screen.
  - C. The Run As option gives you three more chances to type in the correct password before it logs off the current user.
  - D. At the Run As dialog box, you must type in the correct username and password for the currently logged-on user if you want to run the program after entering an incorrect username or password.
6. Which of the following features are *not* new in MMC 3.0? (Choose three.)
- A. Improved error handling
  - B. The Results pane
  - C. Redesigned Add or Remove Snap-in dialog box
  - D. The Console Tree
  - E. The Windows Registry key  
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC`
  - F. The Action Pane
7. How can you perform a bulk import of users into Active Directory to create many user accounts at one time?
- A. Use the `dsadd.exe` command.
  - B. Use the ADUC console.
  - C. Use the `net user` command.
  - D. Use the `csvde.exe` command.
  - E. Use the `dsmod.exe` command.

8. Which of the following commands can perform bulk imports and exports into and out of Active Directory using a file format that is compatible with the Lightweight Directory Access Protocol?
- A. The `dsquery.exe` command
  - B. The `dsrm.exe` command
  - C. The `net user` command
  - D. The `ldifde.exe` command
  - E. The `notepad.exe` utility
9. Which of the following command-line commands can you use to rename an object within Active Directory?
- A. `dsadd`
  - B. `dsquery`
  - C. `dsmove`
  - D. `dsrm`
  - E. `dsget`
  - F. `net user`
10. While remaining logged on at the console to a Windows Server 2003 computer as Joe User, how can you successfully run the following applets and programs as the domain administrator? (Choose two.)
- A. In Control Panel, right-click the Network Connections icon and select Run As. Select the option button for The Following User, type `domain_name\administrator` in the Username box, type the proper password in the Password box, and click OK.
  - B. Click Start and point to All Programs, right-click the Internet Explorer icon and select Run As. Select the option button for The Following User, type `domain_name\administrator` in the Username box, type the proper password in the Password box, and click OK.
  - C. In Control Panel, hold down the Shift key, right-click the Printers and Faxes icon and select Run As. Select the option button for The Following User, type `domain_name\administrator` in the Username box, type the proper password in the Password box, and click OK.
  - D. In Control Panel, hold down the Shift key, right-click the Display icon and select Run As. Select the option button for The Following User, type `domain_name\administrator` in the Username box, type the proper password in the Password box, and click OK.
  - E. Click Start and point to All Programs, Administrative Tools, and click Active Directory Users and Computers. When prompted, select the option button for The Following User, type `domain_name\administrator` in the Username box, type the proper password in the Password box, and click OK.

# Answers to Exam Prep Questions

- 1. Answer B is correct.** Drag and drop is the default behavior in the ADUC in the RTM version (as well as in SP1 and R2). Answer A is incorrect because drag and drop has always been supported in the ADUC console under Windows Server 2003. Answer C is incorrect because the RTM version does not provide any confirmation message box for dragging and dropping objects within the ADUC console. Answer D is incorrect because there is no Microsoft-supported method for disabling drag and drop functionality under the RTM version. However, turning off the drag and drop feature is supported under SP1 and R2.
- 2. Answers B, C, and E are correct.** You can create a computer account when you join a computer to a domain from a Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, or Windows Server 2003 computer. You can prestage a computer account by using either the ADUC console or by using the `dsadd computer` command from a command prompt. Answer A is incorrect because logging on to a domain from a Windows 98 computer does not create a computer account in Active Directory. Answer D is incorrect because the `dsget computer` command displays properties of computers in the directory. Answer F is incorrect because you cannot join a Windows 95 computer to a domain, even with the Active Directory client software installed.
- 3. Answers B and F are correct.** MMC 3.0 is automatically installed when you upgrade to Windows Server 2003 R2 Edition. By adding the new subkey `UseNewUI` to the key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC`, you turn on the improved features for MMC 3.0. Answer A is incorrect because MMC 3.0 is not automatically installed when you install SP1. Answer C is incorrect because you cannot enable MMC 3.0 features under MMC 2.0. Answer D is incorrect because adding the *value* `UseNewUI` to the `KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC` Windows Registry key does not enable the enhancements for MMC 3.0. Answer E is incorrect because you cannot enable the new features for MMC 3.0 from the Add or Remove Snap-in dialog box.
- 4. Answers C and E are correct.** The file named `dsa.msc` is the MMC snap-in for the Active Directory Users and Computers console. You can add a snap-in from an empty MMC by running the MMC command from the Run box and then use the Add/Remove Snap-in dialog box to add the appropriate snap-in. Answer A is incorrect because the default filename for the Active Directory Users and Computers snap-in is `dsa.msc`, not `dsa.mmc`. Answers B and C are incorrect because the default filename for the Active Directory Users and Computers snap-in is `dsa.msc`, not `aduc.msc`.
- 5. Answer B is correct.** If you use the Run As option and type the wrong username or password for the different user's security credentials, you receive a message box that states: *Unable to log on: Logon failure: Unknown user name or bad password*. Answer A is incorrect because the program will not run if you type the incorrect username or password for the Run As dialog box. Answer C is incorrect because the Run As option does not limit how many chances you have to type in the correct user credentials after you receive the logon failure message box. Answer D is incorrect because you do not need to type in the username or password to run a program as the currently logged on user; you do not need to use the Run As feature for this purpose.

- 6. Answers B, D, and E are correct.** The Results pane, the Console Tree, and the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC` Windows Registry key are not new features; all of these components existed under the previous MMC version 2.0. Answer A is incorrect because improved error handling is a new feature of MMC 3.0. Answer C is incorrect because the redesigned Add or Remove Snap-in dialog is a new feature of MMC 3.0. Answer F is incorrect because the Action pane is also a new feature of MMC 3.0.
- 7. Answer D is correct.** You can use the `csvde.exe` command from a command prompt to import many users into Active Directory from `.csv` files. Answer A is incorrect because the `dsadd.exe` only creates a single user at a time. Answer B is incorrect because the ADUC console can only create one user at a time. Answer C is incorrect because the `net user` command can only create one user at a time.
- 8. Answer D is correct.** You can use the `ldifde.exe` command from a command prompt to import many users into Active Directory using `.ldf` files and the LDAP Data Interchange Format (LDIF). Answer A is incorrect because the `dsquery.exe` utility performs searches for Active Directory objects. Answer B is incorrect because the `dsrm.exe` command removes objects from Active Directory. Answer C is incorrect because the `net user` command can only create one user at a time. Answer E is incorrect because `notepad.exe` cannot import or export objects; it is only a text viewer and editor.
- 9. Answer C is correct.** You can use the `dsmove` command to move and rename objects in Active Directory. Answer A is incorrect because you cannot rename any Active Directory object with the `dsadd` command; you use it for adding users. Answer B is incorrect because you cannot rename any Active Directory object with the `dsquery` command; you use it for performing search operations. Answer D is incorrect because you cannot rename any Active Directory object with the `dsrm` command; you use it for removing objects. Answer E is incorrect because you cannot rename any Active Directory object with the `dsget` command; you use it for displaying an object's properties. Answer F is incorrect because you cannot rename any Active Directory object with the `net user` command; you use it for adding users and for viewing user information.
- 10. Answers B and D are correct.** You can right-click application programs, such as Internet Explorer, to select the Run As option. Certain other tools and utilities, such as most Control Panel applets, require you to hold down the Shift key and then right-click the icon to display the Run As menu option. Answer A is incorrect because the Network Connections system folder is one of the few Control Panel icons that do not support the Run As feature (even if you hold down the Shift key). Answer C is incorrect because the Printers and Faxes system folder is also one of the few Control Panel icons that do not support the Run As feature (even if you hold down the Shift key). Answer E is incorrect because the Active Directory Users and Computers console does not automatically prompt you to use the Run As option (nor does any other built-in utility).

## Need to Know More?

1. Stanek, William R. *Microsoft Windows Server 2003 Administrator's Pocket Consultant*. Redmond, Washington: Microsoft Press, 2003.
2. Scales, Lee, and John Michell. *MCSA/MCSE 70-290 Training Guide: Managing and Maintaining a Windows Server 2003 Environment*. Indianapolis, Indiana: Que Publishing, 2003.
3. Lewis, Alex, Morimoto, Rand, Noel, Michael. *Microsoft Windows Server 2003 Unleashed (R2 Edition)*. Indianapolis, Indiana: Sams Publishing, 2006.
4. Search the Microsoft Product Support Services Knowledge Base on the Internet: <http://support.microsoft.com>. You can also search through Microsoft TechNet on the Internet: <http://www.microsoft.com/technet>. Find technical information using keywords from this chapter, such as computer accounts, run as, MMC 3.0, service pack 1 (SP1), R2, active directory, action pane, dsadd, and dsmod.

