

## Active Directory Users and Group

Active Directory® Users and Computers is a Microsoft Management Console (MMC) snap-in that you can use to administer and publish information in the directory.

In this handout we will discuss the users and group object.

1. Managing Users
2. Managing Groups

### 1. Managing Users

You can use Active Directory Users and Computers to create new user accounts or manage existing user accounts.

- a. Understanding User Accounts
- b. Create a New User Account
- c. Reset a User Password
- d. Copy a User Account
- e. Move a User Account
- f. Set Logon Hours
- g. Disable or Enable a User Account
- h. Map a Certificate to a User Account
- i. Change a User's Primary Group
- j. Delete a User Account

#### a. Understanding User Accounts

Active Directory user accounts represent physical entities, such as people. You can also use user accounts as dedicated service accounts for some applications.

User accounts are also referred to as security principals. Security principals are directory objects that are automatically assigned security identifiers (SIDs), which can be used to access domain resources. A user account primarily:

- Authenticates the identity of a user.
- A user account enables a user to log on to computers and domains with an identity that the domain can authenticate. Each user who logs on to the network should have his or her own unique user account and password. To maximize security, avoid having multiple users sharing one account.
- Authorizes or denies access to domain resources.
- After a user is authenticated, the user is authorized or denied access to domain resources based on the explicit permissions that are assigned to that user on the resource.

### User accounts

The Users container in the Active Directory Users and Computers snap-in displays the three built-in user accounts: **Administrator**, **Guest**, and **HelpAssistant**. These built-in user accounts are created automatically when you create the domain.

Each built-in account has a different combination of rights and permissions. The Administrator account has the most extensive rights and permissions over the domain, while the Guest account has limited rights and permissions. The following table describes each default user account on domain controllers running the Windows Server® 2008 R2 operating system.

Default user account	Description
Administrator	<p>The Administrator account has full control of the domain. It can assign user rights and access control permissions to domain users as necessary. Use this account only for tasks that require administrative credentials. We recommend that you set up this account with a strong password.</p> <p>The Administrator account is a default member of the following Active Directory groups: Administrators, Domain Admins, Enterprise Admins, Group Policy Creator Owners, and Schema Admins. The Administrator account can never be deleted or removed from the Administrators group, but it can be renamed or disabled. Because the Administrator account is known to exist on many versions of Windows, renaming or disabling this account will make it more difficult for malicious users to try to gain access to it.</p> <p>The Administrator account is the first account that is created when you set up a new domain with the Active Directory Domain Services Installation Wizard.</p> <div data-bbox="435 590 1471 762" style="border: 1px solid gray; padding: 5px;"> <p><b>Important</b></p> <p>When the Administrator account is disabled, it can still be used to gain access to a domain controller with Safe Mode.</p> </div>
Guest	<p>People who do not have an actual account in the domain can use the Guest account. A user whose account is disabled (but not deleted) can also use the Guest account. The Guest account does not require a password.</p> <p>You can set rights and permissions for the Guest account just like any user account. By default, the Guest account is a member of the built-in Guests group and the Domain Guests global group, which allows a user to log on to a domain. The Guest account is disabled by default, and we recommend that it stay disabled.</p>
HelpAssistant (installed with a Remote Assistance session)	<p>The primary account for establishing a Remote Assistance session. This account is created automatically when you request a Remote Assistance session. It has limited access to the computer. The HelpAssistant account is managed by the Remote Desktop Help Session Manager service. This account is automatically deleted if no Remote Assistance requests are pending.</p>

## Securing user accounts

If built-in account rights and permissions are not modified or disabled by a network administrator, they can be used by a malicious user (or service) to illegally log on to a domain using the Administrator account or Guest account. A good security practice for protecting these accounts is to rename or disable them. Because it retains its SID, a renamed user account retains all its other properties, such as its description, password, group memberships, user profile, account information, and any assigned permissions and user rights.

To obtain the security advantages of user authentication and authorization, use Active Directory Users and Computers to create an individual user account for each user who will participate in your network. You can then add each user account (including the Administrator account and Guest account) to a group to control the rights and permissions that are assigned to the account. When you have accounts and groups that are appropriate for your network, you ensure that you can identify users that log on to your network and that they have access only to the permitted resources.

You can help defend your domain from attackers by requiring strong passwords and implementing an account lockout policy. Strong passwords reduce the risk of intelligent password guessing and dictionary attacks on passwords. An account lockout policy decreases the possibility of an attacker compromising your domain through repeated logon attempts. An account lockout policy determines how many failed logon attempts a user account can have before it is disabled.

## Account options

Each Active Directory user account has a number of account options that determine how someone logging on with that particular user account is authenticated on the network. You can use the options in the following table to configure password settings and security-specific information for user accounts.

Account option	Description
<b>User must change password at next logon</b>	Forces a user to change his or her password the next time that the user logs on to the network. Enable this option when you want to ensure that the user will be the only person that knows the password.
<b>User cannot change password</b>	Prevents a user from changing his or her password. Enable this option when you want to maintain control over a user account, such as a Guest account or temporary account.
<b>Password never expires</b>	Prevents a user password from expiring. We recommend that service accounts have this option enabled and use strong passwords.
<b>Store passwords using reversible encryption</b>	Allows a user to log on to a Windows network from Apple computers. If a user is not logging on from an Apple computer, do not enable this option.
<b>Account is disabled</b>	Prevents a user from logging on with the selected account. Many administrators use disabled accounts as templates for common user accounts.
<b>Smart card is required for interactive logon</b>	Requires that a user possess a smart card to log on to the network interactively. The user must also have a smart card reader attached to their computer and a valid personal identification number (PIN) for the smart card. When this option is enabled, the password for the user account is automatically set to a random and complex value and the <b>Password never expires</b> account option is set.
<b>Account is trusted for delegation</b>	<p>Allows a service running under this account to perform operations on behalf of other user accounts on the network. A service running under a user account (otherwise known as a service account) that is trusted for delegation can impersonate a client to gain access to resources on the computer where the service is running or to resources on other computers. In a forest that is set to the Windows Server 2008 R2 functional level, this option is on the <b>Delegation</b> tab. It is available only for accounts that have been assigned service principal names (SPNs), as set with the <b>setspn</b> command in Windows Server 2008 R2. (Open a command window, and then type <b>setspn</b>.) This is a security-sensitive capability; assign it cautiously.</p> <p>This option is available only on domain controllers running Windows Server 2008 R2 where the domain functionality is set to Windows® 2000 mixed or Windows 2000 native. On domain controllers running Windows Server 2008 and Windows Server 2008 R2 where the domain functional level is set to the Windows Server 2008 or Windows Server 2008 R2 forest functional Level, use the <b>Delegation</b> tab in the user properties dialog box to configure delegation settings. The <b>Delegation</b> tab appears only for accounts that have an assigned SPN.</p>

<b>Account is sensitive and cannot be delegated</b>	You can use this option if the account, for example a Guest or temporary account, cannot be assigned for delegation by another account.
<b>Use DES encryption types for this account</b>	Provides support for the Data Encryption Standard (DES). DES supports multiple levels of encryption, including Microsoft Point-to-Point Encryption (MPPE) Standard (40-bit), MPPE Standard (56-bit), MPPE Strong (128-bit), Internet Protocol security (IPsec) DES (40-bit), IPsec 56-bit DES, and IPsec Triple DES (3DES)
<b>Do not require Kerberos preauthentication</b>	Provides support for alternative implementations of the Kerberos protocol. However, use caution when you enable this option, because Kerberos preauthentication provides additional security and requires time synchronization between the client and the server.

## b. Create a New User Account

To manage domain users, create user accounts in Active Directory Domain Services (AD DS). In contrast, to manage users that are specific to one computer, create local user accounts.

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

Review details about using the appropriate accounts and group memberships in the following table.

### Local and Domain Default Groups

Default groups are created when you install Windows client or server operating systems and Active Directory Domain Services (AD DS) domains. Domain member computers and stand-alone computers have default local groups that are created automatically in their local security accounts database. Domain controllers are an exception: they use the central Active Directory database to create default groups. All domain member computers can access the central Active Directory database.

### Default local groups

The Groups folder in the Local Users and Groups Microsoft Management Console (MMC) snap-in displays the default local groups as well as the local groups that you create. Belonging to a local group gives a user the rights and abilities to perform various tasks on the local computer. You can add local user accounts, domain user accounts, computer accounts, and group accounts to local groups. However, you cannot add local user accounts and local group accounts to domain group accounts.

The following table describes the default groups in the Groups folder, and it lists the default user rights for each group. These user rights are assigned in the local security policy.

Group	Description	Default user rights
Administrators	<p>Members of this group have full control of the server, and they can assign user rights and access control permissions to users as necessary. The Administrator account is also a default member of this group. When this server is joined to a domain, the Domain Admins group is automatically added to this group. Because this group has full control of the server, add users to this group with caution.</p>	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Adjust memory quotas for a process</li> <li>• Allow logon locally</li> <li>• Allow logon through Terminal Services</li> <li>• Back up files and directories</li> <li>• Bypass traverse checking</li> <li>• Change the system time</li> <li>• Create a pagefile</li> <li>• Debug programs</li> <li>• Force shutdown from a remote system</li> <li>• Increase scheduling priority</li> <li>• Load and unload device drivers</li> <li>• Manage auditing and security log</li> <li>• Modify firmware environment variables</li> <li>• Perform volume maintenance tasks</li> <li>• Profile single process</li> <li>• Profile system performance</li> <li>• Remove computer from docking station</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> <li>• Take ownership of files or other objects</li> </ul>
Backup Operators	<p>Members of this group can back up and restore files on the server, regardless of any permissions that protect those files. This is because the right to perform a backup takes precedence over all file permissions. Members of this group cannot change security settings.</p>	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Allow logon locally</li> <li>• Back up files and directories</li> <li>• Bypass traverse checking</li> </ul>

		<ul style="list-style-type: none"> <li>• Restore files and directories</li> <li>• Shut down the system</li> </ul>
DHCP Administrators (installed with the DHCP Server service)	Members of this group have administrative access to the Dynamic Host Configuration Protocol (DHCP) Server service. This group provides a way to assign limited administrative access to the DHCP server role only, while not providing full access to the server. Members of this group can administer DHCP on a server by using the DHCP console or the <b>netsh</b> command, but they are not able to perform other administrative actions on the server.	No default user rights
DHCP Users (installed with the DHCP Server service)	Members of this group have read-only access to the DHCP Server service. This access allows members to view information and properties that are stored at a specified DHCP server. This information is useful to support staff when they need to obtain DHCP status reports.	No default user rights
Guests	A member of this group will have a temporary profile created when they log on, and when they log off, the profile will be deleted. The Guest account (which is disabled by default) is also a default member of this group.	No default user rights
HelpServicesGroup	Administrators can use this group to set rights that are common to all support applications. By default, the only group member is the account that is associated with Microsoft support applications, such as Remote Assistance. Do not add users to this group.	No default user rights
Network Configuration Operators	Members of this group can make changes to TCP/IP settings, and they can renew and release TCP/IP addresses. This group has no default members.	No default user rights
Performance Monitor Users	Members of this group can monitor performance counters on the server, locally and from remote clients, without being members of the Administrators or Performance Log Users groups.	No default user rights
Performance Log	Members of this group can manage	No default user rights

Users	performance counters, logs, and alerts on the server, locally and from remote clients, without being members of the Administrators group.	
Power Users	Members of this group can create user accounts and then modify and delete the accounts that they created. They can create local groups and then add or remove users from the local groups that they created. They can also add or remove users from the Power Users, Users, and Guests groups. Members can create shared resources and administer the shared resources that they created. They cannot take ownership of files, back up or restore directories, load or unload device drivers, or manage security and auditing logs.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Allow logon locally</li> <li>• Bypass traverse checking</li> <li>• Change the system time</li> <li>• Profile single process</li> <li>• Remove computer from docking station</li> <li>• Shut down the system</li> </ul>
Print Operators	Members of this group can manage printers and print queues.	No default user rights
Remote Desktop Users	Members of this group can log on remotely to a server. For more information, see Enabling users to connect remotely to the server ( <a href="http://go.microsoft.com/fwlink/?LinkID=136310">http://go.microsoft.com/fwlink/?LinkID=136310</a> ).	Allow log on through Terminal Services
Replicator	The Replicator group supports replication functions. The only member of the Replicator group should be a domain user account that is used to log on the Replicator services of a domain controller. Do not add user accounts of actual users to this group.	No default user rights
Terminal Server Users	This group contains any users who are currently logged on to the system with Terminal Server. Any program that a user can run with Windows NT 4.0 will run for a member of the Terminal Server User group. The default permissions that are assigned to this group enable its members to run most earlier programs.	No default user rights
Users	Members of this group can perform common tasks, such as running applications, using local and network printers, and locking the server. Users cannot share directories or create local printers. By default, the Domain Users, Authenticated Users, and Interactive groups are	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Allow logon locally</li> <li>• Bypass traverse checking</li> </ul>

	members of this group. Therefore, any user account that is created in the domain becomes a member of this group.	
WINS Users (installed with WINS service)	Members of this group are permitted read-only access to Windows Internet Name Service (WINS). This allows members of the group to view information and properties that are stored at a specified WINS server. This information is useful to support staff when they need to obtain WINS status reports.	No default user rights

### Default domain groups

Default groups, such as the Domain Admins group, are security groups that are created automatically when you create an Active Directory domain. You can use these predefined groups to help control access to shared resources and to delegate specific domain-wide administrative roles.

Many default groups are automatically assigned a set of user rights that authorize members of the group to perform specific actions in a domain, such as logging on to a local system or backing up files and folders. For example, a member of the Backup Operators group has the right to perform backup operations for all domain controllers in the domain.

When you add a user to a group, the user receives all the user rights that are assigned to the group and all the permissions that are assigned to the group on any shared resources.

You can manage groups by using the Active Directory Users and Computers snap-in. Default groups are located in the Builtin container and the Users container. The Builtin container contains groups that are defined with domain local scope. The Users container contains groups that are defined with global scope and groups that are defined with domain local scope. You can move groups that are located in these containers to other groups or organizational units (OUs) within the domain, but you cannot move them to other domains.

### Groups in the Builtin container

The following table provides descriptions of the default groups that are located in the Builtin container, and it lists the assigned user rights for each group.

Group	Description	Default user rights
Account Operators	Members of this group can create, modify, and delete accounts for users, groups, and computers that are located in the Users or Computers containers and OUs in the domain, except the Domain Controllers OU. Members of this group do not have permission to modify the Administrators or the Domain Admins groups, nor do they have permission to modify the accounts for members of those groups. Members of this group can log on locally to domain controllers in the domain and shut them	<ul style="list-style-type: none"> <li>• Allow logon locally</li> <li>• Shut down the system</li> </ul>

	down. Because this group has significant power in the domain, add users to this group with caution.	
Administrators	Members of this group have full control of all domain controllers in the domain. By default, the Domain Admins and Enterprise Admins groups are members of the Administrators group. The Administrator account is also a default member of the Administrators group. Because this group has full control in the domain, add users to this group with caution.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Adjust memory quotas for a process</li> <li>• Back up files and directories</li> <li>• Bypass traverse checking</li> <li>• Change the system time</li> <li>• Create a pagefile</li> <li>• Debug programs</li> <li>• Enable computer and user accounts to be trusted for delegation</li> <li>• Force a shutdown from a remote system</li> <li>• Increase scheduling priority</li> <li>• Load and unload device drivers</li> <li>• Allow logon locally</li> <li>• Manage auditing and security log</li> <li>• Modify firmware environment values</li> <li>• Profile single process</li> <li>• Profile system performance</li> <li>• Remove computer from docking station</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> <li>• Take ownership of files or other objects</li> </ul>
Backup Operators	Members of this group can back up and restore all files on domain controllers in the domain, regardless of their own individual permissions on those files. Backup Operators can also log on to domain controllers and shut them down. This group has no default members. Because this group has significant power on domain controllers, add users to this group with caution.	<ul style="list-style-type: none"> <li>• Back up files and directories</li> <li>• Allow logon locally</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> </ul>
Guests	By default, the Domain Guests group is a member of this group. The Guest account (which is disabled by default) is also a	No default user rights

	default member of this group.	
Incoming Forest Trust Builders (appears only in the forest root domain)	Members of this group can create one-way, incoming forest trusts to the forest root domain. For example, members of this group that reside in Forest A can create a one-way, incoming forest trust from Forest B. This one-way, incoming forest trust allows users in Forest A to access resources in Forest B. Members of this group are granted the permission Create Inbound Forest Trust on the forest root domain. This group has no default members.	No default user rights
Network Configuration Operators	Members of this group can make changes to TCP/IP settings and renew and release TCP/IP addresses on domain controllers in the domain. This group has no default members.	No default user rights
Performance Monitor Users	Members of this group can monitor performance counters on domain controllers in the domain, locally and from remote clients, without being members of the Administrators or Performance Log Users groups.	No default user rights
Performance Log Users	Members of this group can manage performance counters, logs, and alerts on domain controllers in the domain, locally and from remote clients, without being members of the Administrators group.	No default user rights
Pre-Windows 2000 Compatible Access	Members of this group have read access on all users and groups in the domain. This group is provided for backward compatibility for computers running Windows NT 4.0 and earlier. By default, the special identity Everyone is a member of this group.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Bypass traverse checking</li> </ul>
Print Operators	Members of this group can manage, create, share, and delete printers that are connected to domain controllers in the domain. They can also manage Active Directory printer objects in the domain. Members of this group can log on locally to domain controllers in the domain and shut them down. This group has no default members. Because members of	<ul style="list-style-type: none"> <li>• Allow logon locally</li> <li>• Shut down the system</li> </ul>

	this group can load and unload device drivers on all domain controllers in the domain, add users to this group with caution.	
Remote Desktop Users	Members of this group can log on remotely to domain controllers in the domain. This group has no default members.	No default user rights
Replicator	This group supports directory replication functions. The File Replication service uses this group on domain controllers in the domain. This group has no default members. Do not add users to this group.	No default user rights
Server Operators	On domain controllers, members of this group can log on interactively, create and delete shared resources, start and stop some services, back up and restore files, format the hard disk, and shut down the computer. This group has no default members. Because this group has significant power on domain controllers, add users to this group with caution.	<ul style="list-style-type: none"> <li>• Back up files and directories</li> <li>• Change the system time</li> <li>• Force shutdown from a remote system</li> <li>• Allow logon locally</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> </ul>
Users	Members of this group can perform most common tasks, such as running applications, using local and network printers, and locking the server. By default, Domain Users, Authenticated Users, and Interactive are members of this group. Therefore, any user account that is created in the domain becomes a member of this group.	No default user rights

### Groups in the Users container

The following table describes the default groups that are located in the Users container, and it lists the assigned user rights for each group.

Group	Description	Default user rights
Cert Publishers	Members of this group are permitted to publish certificates for users and computers. This group has no default members.	No default user rights
DnsAdmins (installed with Domain Name	Members of this group have administrative access to the DNS Server service. This	No default user rights

System (DNS))	group has no default members.	
DnsUpdateProxy (installed with DNS)	Members of this group are DNS clients that can perform dynamic updates on behalf of other clients, such as DHCP servers. This group has no default members.	No default user rights
Domain Admins	Members of this group have full control of the domain. By default, this group is a member of the Administrators group on all domain controllers, all domain workstations, and all domain member servers at the time that they are joined to the domain. By default, the Administrator account is a member of this group. Because the group has full control in the domain, add users to this group with caution.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Adjust memory quotas for a process</li> <li>• Back up files and directories</li> <li>• Bypass traverse checking</li> <li>• Change the system time</li> <li>• Create a pagefile</li> <li>• Debug programs</li> <li>• Enable computer and user accounts to be trusted for delegation</li> <li>• Force a shutdown from a remote system</li> <li>• Increase scheduling priority</li> <li>• Load and unload device drivers</li> <li>• Allow logon locally</li> <li>• Manage auditing and security log</li> <li>• Modify firmware environment values</li> <li>• Profile single process</li> <li>• Profile system performance</li> <li>• Remove computer from docking station</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> <li>• Take ownership of files or other objects</li> </ul>
Domain Computers	This group contains all workstations and servers that are joined to the domain. By default, any computer account that is created becomes a member of this group automatically.	No default user rights
Domain Controllers	This group contains all domain controllers in the domain.	No default user rights

Domain Guests	This group contains all domain guests.	No default user rights
Domain Users	This group contains all domain users. By default, any user account that is created in the domain becomes a member of this group automatically. This group can be used to represent all users in the domain. For example, if you want all domain users to have access to a printer, you can assign permissions for the printer to this group. (Or you can add the Domain Users group to a local group—on the print server—that has permissions for the printer.)	No default user rights
Enterprise Admins (appears only in the forest root domain)	Members of this group have full control of all domains in the forest. By default, this group is a member of the Administrators group on all domain controllers in the forest. By default, the Administrator account is a member of this group. Because this group has full control of the forest, add users to this group with caution.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Adjust memory quotas for a process</li> <li>• Back up files and directories</li> <li>• Bypass traverse checking</li> <li>• Change the system time</li> <li>• Create a pagefile</li> <li>• Debug programs</li> <li>• Enable computer and user accounts to be trusted for delegation</li> <li>• Force shutdown from a remote system</li> <li>• Increase scheduling priority</li> <li>• Load and unload device drivers</li> <li>• Allow logon locally</li> <li>• Manage auditing and security log</li> <li>• Modify firmware environment values</li> <li>• Profile single process</li> <li>• Profile system performance</li> <li>• Remove computer from docking station</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> </ul> <ul style="list-style-type: none"> <li>• Take ownership of files or other objects</li> </ul>
Group Policy Creator Owners	Members of this group can modify Group Policy in the domain. By default, the Administrator account is a member of this	No default user rights

	group. Because this group has significant power in the domain, add users to this group with caution.	
IIS_WPG (installed with IIS)	The IIS_WPG group is the Internet Information Services (IIS) 6.0 worker process group. IIS 6.0 contains worker processes that serve specific namespaces. For example, www.microsoft.com is a namespace that is served by one worker process, which can run under an identity that is added to the IIS_WPG group, such as MicrosoftAccount. This group has no default members.	No default user rights
RAS and IAS Servers	Servers in this group are permitted access to the remote access properties of users.	No default user rights
Schema Admins (appears only in the forest root domain)	Members of this group can modify the Active Directory schema. By default, the Administrator account is a member of this group. Because this group has significant power in the forest, add users to this group with caution.	No default user

### Creating a new user account

- Using the Windows interface

#### To create a new user account using the Windows interface

2. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
3. In the console tree, right-click the folder in which you want to add a user account.
4. Point to **New**, and then click **User**.
5. For interoperability with other directory services, you can click **InetOrgPerson** instead.
6. In **First name**, type the user's first name.
7. In **Initials**, type the user's initials.
8. In **Last name**, type the user's last name.
9. Modify **Full name** to add initials or reverse the order of first and last names.
10. In **User logon name**, type the user logon name, click the user principal name (UPN) suffix in the drop-down list, and then click **Next**.
11. If the user will use a different name to log on to computers running Microsoft® Windows® 95, Windows 98, or Windows NT® operating systems, you can change the user logon name as it appears in **User logon name (pre-Windows 2000)** to the different name.
12. In **Password** and **Confirm password**, type the user's password, and then select the appropriate password options.

## **Additional considerations**

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in AD DS, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- A new user account with the same name as a previously deleted user account does not automatically assume the permissions and group memberships of the previously deleted account because the security identifier (SID) for each account is unique. If you want to duplicate a deleted user account, you must recreate all permissions and memberships manually.
- When you create a new user account, the **full name** attribute is created in the **FirstNameLastName** format by default. The **full name** attribute also governs the display name format that is shown in the global address list. You can change the display name format by using ADSI Edit. If you change the display name format, the full name format will also change.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell™. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### **c. Reset a User Password**

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### **Resetting a user password**

- Using the Windows interface

#### **To reset a user password using the Windows interface**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.

#### **Where?**

- Active Directory Users and Computers\*domain node*\Users

Or, click the folder that contains the user account.

3. In the details pane, right-click the user whose password you want to reset, and then click **Reset Password**.
4. Type and then confirm the password.
5. If you want to require the user to change this password at the next logon process, select the **User must change password at next logon** check box.

## **Additional considerations**

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- Services that are authenticated with a user account must be reset if the password for the service's user account is changed.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### **d. Copy a User Account**

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### **To copy a user account**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.

#### **Where?**

- Active Directory Users and Computers\*domain node*\Users

3. In the details pane, right-click the user account that you want to copy, and then click **Copy**.
4. In **First name**, type the user's first name.
5. In **Last name**, type the user's last name.
6. Modify **Full name** to add initials or reverse the order of the first and last names.
7. In **User logon name**, type the user logon name, click the user principal name (UPN) suffix in the drop-down list, and then click **Next**.

If the user will use a different name to log on to computers running Windows 95, Windows 98, or Windows NT, you can change the user logon name as it appears in **User logon name (pre-Windows 2000)** to the different name.

8. In **Password** and **Confirm password**, type the user's password, and then select the appropriate password options.

If the user account from which the new user account was copied was disabled, click **Account is disabled** to enable the new account.

### e. Move a User Account

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### Moving a user account

- Using the Windows interface

#### To move a user account using the Windows interface

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.

#### Where?

- Active Directory Users and Computers\domain node\Users

Or, click the folder that contains the user account.

3. In the details pane, right-click the user that you want to move, and then click **Move**.
4. In the **Move** dialog box, click the folder to which you want to move the user account.

#### *Additional considerations*

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- f. You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### g. Set Logon Hours

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### To set logon hours using the Windows interface

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.

#### Where?

- Active Directory Users and Computers\*domain node*\Users
3. Right-click the user account, and then click **Properties**.
  4. On the **Account** tab, click **Logon Hours**, and then set the permitted or denied logon hours for the user.

#### **Additional considerations**

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- To modify the logon hours for multiple users, press and hold down CTRL, and then click each user. Right-click the selected users, and then click **Properties**. On the **Account** tab, click **Logon Hours**, and then set the permitted or denied logon hours for the user.

You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

#### **h. Disable or Enable a User Account**

- To prevent a particular user from logging on for security reasons, you can disable user accounts rather than deleting them.

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### **Disabling or enabling a user account**

- Using the Windows interface

#### **To disable or enable a user account using the Windows interface**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.

#### **Where?**

- Active Directory Users and Computers\*domain node*\Users

Or, click the folder that contains the user account.

3. In the details pane, right-click the user.
4. Depending on the status of the account, do one of the following:
  - To disable the account, click **Disable Account**.

- To enable the account, click **Enable Account**.

#### i. **Change a User's Primary Group**

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

##### **To change a user's primary group**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.

##### **Where?**

- Active Directory Users and Computers\*domain node*\Users

Or, click the folder that contains the user account.

3. In the details pane, right-click the user that you want to change, and then click **Properties**.
4. On the **Member Of** tab, click the group that you want to set as the user's primary group, and then click **Set Primary Group**.

#### j. **Delete a User Account**

Updated: December 30, 2008

Applies To: Windows Server 2008, Windows Server 2008 R2

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

##### **Deleting a user account**

- Using the Windows interface

##### **To delete a user account using the Windows interface**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.

##### **Where?**

- Active Directory Users and Computers\*domain node*\Users

Or, click the folder that contains the user account.

3. In the details pane, right-click the user account, and then click **Delete**.

## Managing Groups

You can use Active Directory Users and Computers to create new groups or manage existing groups.

- a. Understanding Group Accounts
- b. Create a New Group
- c. Add a Member to a Group
- d. Convert a Group to Another Type
- e. Change Group Scope
- f. Delete a Group
- g. Find Groups in Which a User is a Member
- h. Assign User Rights to a Group in AD DS

### a. Understanding Group Accounts

A group is a collection of user and computer accounts, contacts, and other groups that can be managed as a single unit. Users and computers that belong to a particular group are referred to as group members.

Groups in Active Directory Domain Services (AD DS) are directory objects that reside in a domain and in organizational unit (OU) container objects. AD DS provides a set of default groups at installation. It also provides an option to create groups.

You can use groups in AD DS to:

- Simplify administration by assigning permissions on a shared resource to a group, rather than to individual users. Assigning permissions to a group assigns the same access to the resource to all members of that group.
- Delegate administration by assigning user rights once to a group through Group Policy. You can then add members to the group that you want to have the same rights as the group.
- Create e-mail distribution lists.

Groups are characterized by their scope and their type. The scope of a group determines the extent to which the group is applied within a domain or forest. The group type determines whether you can use a group to assign permissions from a shared resource (for security groups) or use a group for e-mail distribution lists only (for distribution groups).

There are also groups for which you cannot modify or view the memberships. These groups are referred to as special identities. They represent different users at different times, depending on the circumstances. For example, the Everyone group is a special identity that represents all current network users, including guests and users from other domains.

The following sections provide additional information about group accounts in AD DS.

### Understanding default groups

Default groups, such as the Domain Admins group, are security groups that are created automatically when you create an Active Directory domain. You can use these predefined groups to help control access to shared resources and delegate specific domain-wide administrative roles.

Many default groups are automatically assigned a set of user rights that authorize members of the group to perform specific actions in a domain, such as logging on to a local system or backing up files and folders. For example, a member of the Backup Operators group has the right to perform backup operations for all domain controllers in the domain.

When you add a user to a group, the user receives the following:

- All the user rights that are assigned to the group
- All the permissions that are assigned to the group on any shared resources

Default groups are located in the Builtin container and the Users container. The default groups in the Builtin container have a group scope of Builtin Local. Their group scope and group type cannot be changed. The Users container contains groups that are defined with global scope and groups that are defined with domain local scope. You can move groups that are located in these containers to other groups or OUs within the domain, but you cannot move them to other domains.

### **Understanding group scope**

Groups are characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest. There are three group scopes: domain local, global, and universal.

### **Understanding domain local groups**

Members of domain local groups can include other groups and accounts from Windows Server 2003, Windows 2000, Windows NT, Windows Server 2008, and Windows Server 2008 R2 domains. Members of these groups can be assigned permissions only within a domain.

Groups with domain local scope help you define and manage access to resources within a single domain. These groups can have the following as their members:

- Groups with global scope
- Groups with universal scope
- Accounts
- Other groups with domain local scope
- A mixture of any of the above

For example, to give five users access to a particular printer, you can add all five user accounts in the printer permissions list. If, however, you later want to give the five users access to a new printer, you again have to specify all five accounts in the permissions list for the new printer.

With a little planning, you can simplify this routine administrative task by creating a group with domain local scope and assigning it permission to access the printer. Put the five user accounts in a group with global scope and add this group to the group that has domain local scope. When you want to give the five users access to a new printer, assign the group with domain local scope permission to access the new printer. All members of the group with global scope automatically receive access to the new printer.

### **Understanding global groups**

Members of global groups can include other groups and accounts only from the domain in which the group is defined. Members of these groups can be assigned permissions in any domain in the forest.

Use groups with global scope to manage directory objects that require daily maintenance, such as user and computer accounts. Because groups with global scope are not replicated outside their own domain, you can change accounts in a group having global scope frequently without generating replication traffic to the global catalog.

Although rights and permissions assignments are valid only within the domain in which they are assigned, by applying groups with global scope uniformly across the appropriate domains, you can consolidate references to accounts with similar purposes. This simplifies and rationalizes group management across domains. For example, in a network with two domains, Europe and UnitedStates, if there is a group with global scope called GLAccounting in the UnitedStates domain, there should also be a group called GLAccounting in the Europe domain (unless the accounting function does not exist in the Europe domain).

#### ◆ Important

We strongly recommend that you use global groups or universal groups instead of domain local groups when you specify permissions on domain directory objects that are replicated to the global catalog.

### Understanding universal groups

Members of universal groups can include other groups and accounts from any domain in the domain tree or forest. Members of these groups can be assigned permissions in any domain in the domain tree or forest.

Use groups with universal scope to consolidate groups that span domains. To do this, add the accounts to groups with global scope and nest these groups within groups having universal scope. When you use this strategy, any membership changes in the groups that have global scope do not affect the groups with universal scope.

For example, in a network with two domains, Europe and UnitedStates, and a group that has global scope called GLAccounting in each domain, create a group with universal scope called UAccounting that has as its members the two GLAccounting groups, UnitedStates\GLAccounting and Europe\GLAccounting. You can then use the UAccounting group anywhere in the enterprise. Any changes in the membership of the individual GLAccounting groups will not cause replication of the UAccounting group.

Do not change the membership of a group with universal scope frequently. Any changes to the membership of this type of group cause the entire membership of the group to be replicated to every global catalog in the forest.

### Understanding group types

There are two types of groups in AD DS: distribution groups and security groups. You can use distribution groups to create e-mail distribution lists and security groups to assign permissions to shared resources.

You can use distribution groups only with e-mail applications (such as Microsoft Exchange Server 2007) to send e-mail to collections of users. Distribution groups are not security enabled, which means that they cannot be listed in discretionary access control lists (DACLS). If you need a group for controlling access to shared resources, create a security group.

When they are used with care, security groups provide an efficient way to assign access to resources on your network. By using security groups, you can:

- Assign user rights to security groups in AD DS.

User rights are assigned to a security group to determine what members of that group can do within the scope of a domain (or forest). User rights are automatically assigned to some security groups at the time that AD DS is installed to help administrators define a person's administrative role in the domain. For example, a user who is added to the Backup Operators group in Active Directory has the ability to back up and restore files and directories on each domain controller in the domain.

- Assign permissions to security groups on resources.

Permissions are different from user rights. Permissions determine who can access a shared resource, and they determine the level of access, such as Full Control. You can use security groups to manage access and permissions to a shared resource. Some permissions that are set on domain objects are automatically assigned to allow various levels of access to default security groups, such as the Account Operators group or the Domain Admins group.

Like distribution groups, security groups can also be used as e-mail entities. Sending an e-mail message to the group sends the message to all the members of the group.

### **Special identities**

In addition to the groups in the Users container and Builtin container, servers running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 include several special identities. For convenience, these identities are generally referred to as groups. These special groups do not have specific memberships that can be modified. However, they can represent different users at different times, depending on the circumstances. The following groups represent special identities:

- **Anonymous Logon**  
This group represents users and services that access a computer and its resources through the network without using an account name, password, or domain name. On computers running Windows NT and earlier, the Anonymous Logon group is a default member of the Everyone group. On computers running Windows Server 2008 R2, Windows Server 2008 or Windows Server 2003, the Anonymous Logon group is not a member of the Everyone group by default.
- **Everyone**  
This group represents all current network users, including guests and users from other domains. Whenever a user logs on to the network, the user is added automatically to the Everyone group.
- **Network**  
This group represents users who are currently accessing a given resource over the network, as opposed to users who access a resource by logging on locally at the computer where the resource is located. Whenever a user accesses a given resource over the network, the user is added automatically to the Network group.
- **Interactive**

This group represents all users who are currently logged on to a particular computer and who are accessing a given resource that is located on that computer, as opposed to users who access the resource over the network. Whenever a user accesses a given resource on the computer to which they are currently logged on, the user is added automatically to the Interactive group.

Although the special identities can be assigned rights and permissions to resources, the memberships cannot be modified or viewed. Group scopes do not apply to special identities. Users are assigned automatically to these special identities whenever they log on or access a particular resource.

### **Understanding where groups can be created**

In AD DS, groups are created in domains. You use Active Directory Users and Computers to create groups. With the necessary permissions, you can create groups in the root domain of the forest, in any other domain in the forest, or in an OU.

Besides the domain in which it is created, a group is also characterized by its scope. The scope of a group determines the following:

- The domain from which members can be added
- The domain in which the rights and permissions that are assigned to the group are valid

Choose the particular domain or OU where you create a group based on the administration that is required for the group. For example, if your directory has multiple OUs, each of which has a different administrator, you may want to create groups with global scope within those OUs so that the administrators can manage group membership for users in their respective OUs. If groups are required for access control outside the OU, you can nest the groups in the OU into groups with universal scope (or other groups with global scope) that you can use elsewhere in the forest.

If the domain functional level is set to Windows 2000 native or higher, the domain contains a hierarchy of OUs, and administration is delegated to administrators at each OU, it may be more efficient to nest groups with global scope. For example, if OU1 contains OU2 and OU3, a group with global scope in OU1 can have as its members groups with global scope in OU2 and OU3. In OU1, the administrator can add or remove group members from OU1, and the administrators of OU2 and OU3 can add or remove group members for accounts from their own OUs without having administrative rights for the group with global scope in OU1.

#### Note

You can move groups within a domain. However, only groups with universal scope can be moved from one domain to another. The rights and permissions that are assigned to a group with universal scope are lost when the group is moved to another domain, and new assignments must be made.

### b. Create a New Group

Updated: January 4, 2010

Applies To: Windows Server 2008, Windows Server 2008 R2

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### Creating a new group account

- Using the Windows interface

#### To create a new group account using the Windows interface

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, right-click the folder under which you want to create a new group.
  - a. **Where?**
    - b. Active Directory Users and Computers\*domain node*\*folder*
3. Point to **New**, and then click **Group**.
4. Type the name of the new group.
  - a. By default, the name that you type is also entered as the pre–Windows 2000 name of the new group.
5. In **Group scope**, click one of the options.
6. In **Group type**, click one of the options.

### ***Additional considerations***

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- To add a group, you can also click the folder in which you want to add the group, and then click the new group icon on the toolbar.
- If the domain in which you are creating the group is set to the domain functional level of Windows 2000 mixed, you can select only the **Security** group type with **Domain local** or **Global scopes**.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.
- A group name cannot be identical to any other group name in the domain.
- A group name (CN) can contain up to 64 uppercase or lowercase characters.
- A group name (CN) cannot consist solely of spaces.
- A group name (pre–Windows 2000) (**samAccountName** object attribute) can contain up to 256 uppercase or lowercase characters except for the following:

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

- A group name (pre–Windows 2000) (**samAccountName** object attribute) cannot consist solely of periods or spaces.
- In Active Directory Users and Computers and in Active Directory Administrative Center, by default, the name that you type is also entered as the pre–Windows 2000 name of the new group.

### ***Additional considerations***

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in AD DS, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- If the domain in which you are creating the group is set to the domain functional level of Windows 2000 mixed, you can select only the **Security** group type with **Domain local** or **Global scopes**.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.
- A group name cannot be identical to any other group name in the domain.
- A group name (CN) can contain up to 64 uppercase or lowercase characters.
- A group name (CN) cannot consist solely of spaces.
- A group name (pre–Windows 2000) (**samAccountName** object attribute) can contain up to 256 uppercase or lowercase characters except for the following:

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

- A group name (pre–Windows 2000) (**samAccountName** object attribute) cannot consist solely of periods or spaces.

## Note

When you use **net group** to create a new group account (**net group <group\_name> /add /domain**, for example, **net group Group1 /add /domain**), if you specify a group name that is longer than 64 characters, the directory service sets the group's CN to the automatically generated **objectSID** of the newly created group account and the **samAccountName** object attribute assumes the name that you specify in the **net group** command.

### c. Add a Member to a Group

Updated: January 4, 2010

Applies To: Windows Server 2008, Windows Server 2008 R2

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### Adding a member to a group

- Using the Windows interface

#### To add a member to a group using the Windows interface

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click the folder that contains the group to which you want to add a member.

#### Where?

- Active Directory Users and Computers\*domain node*\*folder that contains the group*
3. In the details pane, right-click the group, and then click **Properties**.
  4. On the **Members** tab, click **Add**.
  5. In **Enter the object names to select**, type the name of the user, group, or computer that you want to add to the group, and then click **OK**.

#### Additional considerations

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- In addition to users and computers, group members can include contacts and other groups.
- Another way to add members to a group is to select the desired object and then click the **Adds the selected objects to a group you specify** toolbar icon. You can also drag a member object to a group, or right-click the object, and then click **Add to a group**.

- When you administer a domain, security principals in the parent domain or other trusted domains are not visible on the **Member Of** tab in a domain user's properties. The only domain accounts that you can add or view are the present domain groups. Only domain groups in the present domain are shown, even if the member belongs to other trusted domain groups.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

#### ***Additional considerations***

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in AD DS, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- In addition to users and computers, group members can include contacts and other groups.

You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

#### **d. Convert a Group to Another Type**

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### **Converting a group to another group type**

- Using the Windows interface

#### **To convert a group to another group type using the Windows interface**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click the folder that contains the group that you want to convert to another group type.
  - a. **Where?**
  - b. Active Directory Users and Computers\*domain node*\*folder that contains the group*
3. In the details pane, right-click the group, and then click **Properties**.
4. On the **General** tab, under **Grouptype**, click the group type.

#### ***Additional considerations***

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- To convert a group, the domain functional level must be set to Windows 2000 native or higher. Groups cannot be converted when the domain functional level is set to Windows 2000 mixed.

- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### To convert a group to another group type using a command line

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type the following command, and then press ENTER:

#### **Additional considerations**

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in AD DS, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- To convert a group, the domain functional level must be set to Windows 2000 native or higher. Groups cannot be converted when the domain functional level is set to Windows 2000 mixed.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

#### **e. Change Group Scope**

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### **Changing group scope**

- Using the Windows interface

#### **To change group scope using the Windows interface**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click the folder that contains the group for which you want to change the group scope.
  - a. **Where?**
  - b. Active Directory Users and Computers\*domain node*\*folder that contains the group*
3. In the details pane, right-click the group, and then click **Properties**.
4. On the **General** tab, under **Group scope**, select the group scope.

#### **Additional considerations**

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.

- You can change group scopes only when the domain functional level is set to Windows 2000 native or higher.
- Changing the scope of a group from universal to domain local can only be done on a global catalog server. An error message appears if the domain controller is not a global catalog server.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### ***Additional considerations***

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in AD DS, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- You can change group scopes only when the domain functional level is set to Windows 2000 native or higher.
- Changing the scope of a group from universal to domain local can only be done on a global catalog server. An error message appears if the domain controller is not a global catalog server.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

#### **f. Delete a Group**

Updated: December 30, 2008

Applies To: Windows Server 2008, Windows Server 2008 R2

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

### **Deleting a group account**

- Using the Windows interface

#### **To delete a group account using the Windows interface**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click the folder that contains the group that you want to delete.
  - a. **Where?**
  - b. Active Directory Users and Computers\*domain node*\*folder that contains the group*
3. In the details pane, right-click the group, and then click **Delete**.

### ***Additional considerations***

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- Deleting a group is a permanent operation.

- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### ***Additional considerations***

- To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in AD DS, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- Deleting a group is a permanent operation.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### **g. Find Groups in Which a User is a Member**

#### **Finding a groups in which a user is a member**

- Using the Windows interface

#### **To find groups in which a user is a member using the Windows interface**

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, click **Users**.
  - a. **Where?**
  - b. Active Directory Users and Computers\*domain node*\Users
  - c. Or, click the folder that contains the user account whose group membership you want to view.
3. In the details pane, right-click a user account, and then click **Properties**.
4. Click the **Member Of** tab.

### ***Additional considerations***

- Performing this task does not require you to have administrative credentials. Therefore, as a security best practice, consider performing this task as a user without administrative credentials.
- Another way to open Active Directory Users and Computers is to click **Start**, click **Run**, and then type **dsa.msc**.
- The **Member Of** tab for a user displays a list of groups in the domain in which the user's account is located. Active Directory Domain Services (AD DS) does not display groups that reside in trusted domains where the user is a member.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

### ***Additional considerations***

- Performing this task does not require you to have administrative credentials. Therefore, as a security best practice, consider performing this task as a user without administrative credentials.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.

#### **h. Assign User Rights to a Group in AD DS**

Updated: December 30, 2008

Applies To: Windows Server 2008, Windows Server 2008 R2

Membership in **Account Operators**, **Domain Admins**, or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure.

#### **To assign user rights to a group in Active Directory Domain Services**

1. To open Group Policy Management, click **Start**, click **Run**, type **gpmc.msc**, and then click **OK**.
2. In the console tree, right-click **Default Domain Controllers Policy**, and then click **Edit**.
  - a. **Where?**
  - b. *Domains\Current Domain Name\Group Policy objects\Default Domain Controllers Policy*
3. In the console tree, click **User Rights Assignment**.
  - a. **Where?**
  - b. *Windows Settings\Security Settings\Local Policies\User Rights Assignment*
4. In the details pane, double-click the user right that you want to assign.
5. Click **Add User or Group**.
  - a. If the button appears dimmed, select the **Define these policy settings** check box.
6. Type the name of the group to which you want to assign this right.

### ***Additional considerations***

- 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 Domain Services (AD DS), or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.
- To perform this procedure, you must first install Group Policy Management as a feature in Server Manager.
- You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell. To open the Active Directory module, click **Start**, click **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.



Answer the following questions after reading pag1-32 of the handout.

*Match each term with the correct statement below.*

- A. Administrators
- B. Backup Operators
- C. Power Users
- D. Remote Desktop Users
- E. Users

1. Access this computer from the network
2. Adjust memory quotas for a process
3. Allow logon locally
4. Restore files and directories
5. Shut down the system
6. Allow logon locally
7. Bypass traverse checking
8. Change the system time
9. Modify firmware environment variables
10. Perform volume maintenance tasks
11. Profile single process
12. Profile system performance
13. Remove computer from docking station
14. Access this computer from the network
15. Allow logon locally
16. Allow logon through Terminal Services
17. Back up files and directories
18. Bypass traverse checking
19. Change the system time
20. Create a pagefile
21. Debug programs
22. Force shutdown from a remote system
23. Increase scheduling priority
24. Load and unload device drivers
25. Manage auditing and security log
26. Back up files and directories
27. Bypass traverse checking
28. Profile single process
29. Remove computer from docking station
30. Shut down the system
31. Allow log on through Terminal Services
32. Access this computer from the network

The Users container in the Active Directory Users and Computers snap-in displays the three built-in user accounts. What are these users?

Group	Description	Default user rights
Administrators	<p>Members of this group have full control of the server, and they can assign user rights and access control permissions to users as necessary. The Administrator account is also a default member of this group. When this server is joined to a domain, the Domain Admins group is automatically added to this group. Because this group has full control of the server, add users to this group with caution.</p>	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Adjust memory quotas for a process</li> <li>• Allow logon locally</li> <li>• Allow logon through Terminal Services</li> <li>• Back up files and directories</li> <li>• Bypass traverse checking</li> <li>• Change the system time</li> <li>• Create a pagefile</li> <li>• Debug programs</li> <li>• Force shutdown from a remote system</li> <li>• Increase scheduling priority</li> <li>• Load and unload device drivers</li> <li>• Manage auditing and security log</li> <li>• Modify firmware environment variables</li> <li>• Perform volume maintenance tasks</li> <li>• Profile single process</li> <li>• Profile system performance</li> <li>• Remove computer from docking station</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> </ul>

		<ul style="list-style-type: none"> <li>• Take ownership of files or other objects</li> </ul>
Backup Operators	Members of this group can back up and restore files on the server, regardless of any permissions that protect those files. This is because the right to perform a backup takes precedence over all file permissions. Members of this group cannot change security settings.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Allow logon locally</li> <li>• Back up files and directories</li> <li>• Bypass traverse checking</li> <li>• Restore files and directories</li> <li>• Shut down the system</li> </ul>
DHCP Administrators (installed with the DHCP Server service)	Members of this group have administrative access to the Dynamic Host Configuration Protocol (DHCP) Server service. This group provides a way to assign limited administrative access to the DHCP server role only, while not providing full access to the server. Members of this group can administer DHCP on a server by using the DHCP console or the <b>netsh</b> command, but they are not able to perform other administrative actions on the server.	No default user rights
DHCP Users (installed with the DHCP Server service)	Members of this group have read-only access to the DHCP Server service. This access allows members to view information and properties that are stored at a specified DHCP server. This information is useful to support staff when they need to obtain DHCP status reports.	No default user rights
Guests	A member of this group will have a temporary profile created when they log on, and when they log off, the profile will be deleted. The Guest account (which is disabled by default) is also a default member of this group.	No default user rights
HelpServicesGroup	Administrators can use this group to set rights that are common to all support applications. By default, the only group member is the account that is associated with Microsoft support applications, such as Remote Assistance. Do not add users to this group.	No default user rights
Network Configuration	Members of this group can make changes to TCP/IP settings, and they can renew and release TCP/IP addresses. This group has no	No default user rights

Operators	default members.	
Performance Monitor Users	Members of this group can monitor performance counters on the server, locally and from remote clients, without being members of the Administrators or Performance Log Users groups.	No default user rights
Performance Log Users	Members of this group can manage performance counters, logs, and alerts on the server, locally and from remote clients, without being members of the Administrators group.	No default user rights
Power Users	Members of this group can create user accounts and then modify and delete the accounts that they created. They can create local groups and then add or remove users from the local groups that they created. They can also add or remove users from the Power Users, Users, and Guests groups. Members can create shared resources and administer the shared resources that they created. They cannot take ownership of files, back up or restore directories, load or unload device drivers, or manage security and auditing logs.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Allow logon locally</li> <li>• Bypass traverse checking</li> <li>• Change the system time</li> <li>• Profile single process</li> <li>• Remove computer from docking station</li> <li>• Shut down the system</li> </ul>
Print Operators	Members of this group can manage printers and print queues.	No default user rights
Remote Desktop Users	Members of this group can log on remotely to a server. For more information, see Enabling users to connect remotely to the server ( <a href="http://go.microsoft.com/fwlink/?LinkID=136310">http://go.microsoft.com/fwlink/?LinkID=136310</a> ).	Allow log on through Terminal Services
Replicator	The Replicator group supports replication functions. The only member of the Replicator group should be a domain user account that is used to log on the Replicator services of a domain controller. Do not add user accounts of actual users to this group.	No default user rights
Terminal Server Users	This group contains any users who are currently logged on to the system with Terminal Server. Any program that a user can run with Windows NT 4.0 will run for a member of the Terminal Server User group. The default	No default user rights

	permissions that are assigned to this group enable its members to run most earlier programs.	
Users	Members of this group can perform common tasks, such as running applications, using local and network printers, and locking the server. Users cannot share directories or create local printers. By default, the Domain Users, Authenticated Users, and Interactive groups are members of this group. Therefore, any user account that is created in the domain becomes a member of this group.	<ul style="list-style-type: none"> <li>• Access this computer from the network</li> <li>• Allow logon locally</li> <li>• Bypass traverse checking</li> </ul>
WINS Users (installed with WINS service)	Members of this group are permitted read-only access to Windows Internet Name Service (WINS). This allows members of the group to view information and properties that are stored at a specified WINS server. This information is useful to support staff when they need to obtain WINS status reports.	No default user rights