2.1. What is an OU?

An Organizational Unit (OU) is similar to a folder that subdivides and organizes network resources within a domain.

- An OU can contain other OUs or any type of object type, such as users, computers, and printers.
- OUs can be nested to logically organize network resources.
    - *Parent* OUs are OUs that contain other OUs.
    - *Child* OUs are OUs within other OUs.
- OUs are typically organized by the following:
    - Physical location, such as a country or city.
    - Organizational structure, such as the HR, Sales, and IT departments.
    - Object type, such as user accounts or computers.
    - Hybrid of location, organizational structure, and object type.

Be aware of the following considerations for managing OUs:

Feature	Description
Group Policy	One of the biggest reasons to use OUs is for the application of Group Policy. Create OUs for each group of objects that need to have different Group Policy settings. • Group Policy objects (GPOs) can be linked to OUs. Policy settings apply to all objects within the OU. • Through *inheritance*, settings applied to the domain or parent OUs apply to all child OUs and objects within those OUs. ***Note:*** *A generic container is not an OU and can't have group policy objects assigned to it. A good practice is to move objects out of generic containers and into an OU. For example, you can move the computers out of the Computers container and into an OU where group policy can be applied.*

Preventing accidental deletion	Objects in Active Directory can be accidentally deleted through Active Directory Users and Computers and other management tools. The following types of deletions are most common: • *Leaf-node deletion* is when a user selects and deletes a leaf object. • *Organizational Unit (OU) deletion* is when a user selects and deletes an OU that has subordinate objects. Deleting the OU deletes all objects within the OU (including any child OUs and their objects). To protect objects from accidental deletion: • In Active Directory Users and Computers or Active Directory Sites and Services, edit the properties and do one of the following: o On the **Object** tab, select the **Protect object from accidental deletion** check box. (This option is only seen with **Advanced Features** selected from the **View** menu.) o On the **Security** tab, select the **Deny Delete All Child Objects** advanced permission for Everyone. • When you create an organizational unit, leave the **Protect container from accidental deletion** check box selected. This is the default. Other types of objects do not have this default setting and must be manually configured. To delete on abject that is protected, first clear the **Protect container from accidental deletion** setting, then delete the object.
Delegating authority	Delegating authority is the assignment of administrative tasks, such as resetting passwords or creating new users, to appropriate users and groups. You should be aware of the following facts about delegating control: • You can delegate control of any part of an OU or object at any level with the Delegation of Control Wizard or through the Authorization Manager console.

	• An object-based design allows you to delegate control based on the types of objects in each OU. For example, you can delegate control over specific object types (such as user objects). • A task-based design allows you to delegate control based on the types of administrative tasks that need to be done. Some examples of administrative tasks are: o User account management, such as creation and deletion. o Password management, such as resetting and forcing password changes. o Group membership and permissions management

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

2.2. Default Containers

When you install Active Directory, several default containers and Organizational Units (OUs) are automatically created. The following table lists the default containers and their contents:

Container or OU	Contents
Builtin	The Builtin container holds default service administrator accounts and domain local security groups. These groups are pre-assigned permissions needed to perform domain management tasks.
Computers	The Computers container holds all computers joined to the domain without a computer account. It is the default location for new computer accounts created in the domain.
Domain Controllers	The Domain Controllers OU is the default location for the computer accounts for domain controllers.
ForeignSecurityPrincipals	The ForeignSecurityPrincipals container holds proxy objects for security principals in NT 4.0 domains or domains outside of the forest.
LostAndFound	The LostAndFound container holds objects moved or created at the same time an Organizational Unit is deleted. Because of Active Directory replication, the parent OU can be deleted on one domain controller while administrators at other domain controllers can add or move objects to the deleted OU before the change has been replicated. During replication, new objects are placed in the LostAndFound container.
NTDS Quotas	The NTDS Quotas container holds objects that contain limits on the number of objects users and groups can own.
Program Data	The Program Data container holds application-specific data created by other programs. This container is

	empty until a program designed to store information in Active Directory uses it.
System	The System container holds configuration information about the domain including security groups and permissions, the domain SYSVOL share, DFS configuration information, and IP security policies.
Users	The Users container holds additional predefined user and group accounts (besides those in the Builtin container). Users and groups are pre-assigned membership and permissions for completing domain and forest management tasks.

Be aware of the following when managing the default containers:

- Default containers are automatically created and cannot be deleted.
- The Domain Controllers OU is the only default organizational unit object. All other containers are just containers, not OUs. As such, you cannot apply a GPO to any default container except for the Domain Controllers OU.
- To apply Group Policy specifically to objects within a default container (except for the Domain Controllers OU), move the objects into an OU that you create, then link the GPO.
- The LostAndFound, NTDS Quotas, Program Data, and System containers are hidden in Active Directory Users and Computers. To view these containers, click **Advanced Features** from the **View** menu.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

2.3. User Account

A user account identifies a single user, such as an employee. Windows has the following types of user accounts:

Type	Description
Local	A *local* user account is created and stored on a local system and is not distributed to any other system. • Local user accounts are created with the Computer Management console. • The local Security Accounts Manager (SAM) manages the user account information. • Only local resources are accessible with local user accounts.
Domain	A *domain* user account is created and centrally managed through Active Directory, and is replicated between domain controllers in the domain. • Domain user accounts are created with Active Directory Users and Computers, command line tools, and PowerShell. • Each domain user account has a unique security identifier (SID) to identify the user. A user can log on to the domain from any computer that is a member of the domain and can access resources on that computer or on other computers for which the domain user account has permissions. • Domain user accounts have a variety of properties, such as user information, group membership, user profiles, and dial-in settings.

***Note**: External users which need an e-mail account, can be represented through a contact object. A contact object is an account that does not have any security permissions. Users represented as contact objects cannot log on to the domain. Use contacts to add information about individuals, such as e-mail or phone number, to Active Directory. Applications, such as Exchange, can search for attributes of contact objects.*

Active Directory uses the following name types to recognize each object:

Type	Description
User or Logon Name	The user or logon name is the name of the user account. It is typically a combination of the *given name* (first name) and *surname* (last name) of the user. For example, Andy Waters may have the following logon name, **awaters**.
User Principle Name (UPN)	The User Principle Name (UPN) combines the user account name with the DNS domain name. For example, account **awaters** in the **westsim.com** domain would have **awaters@westsim.com** as the UPN. • The UPN format is also known as the *SMTP address* format. • The DNS domain name in the UPN is known as the *UPN suffix*. • By default, the domain that holds the user account is selected for the UPN suffix. However, you can configure different UPN suffixes to use instead of the domain name.
LDAP Distinguished Name (DN)	The LDAP Distinguished Name (DN) references the domain and related container(s) where the object resides. It has three basic attributes: • Domain Component (DC) • Organizational Unit (OU) • Common Name (CN) An example LDAP Distinguished Name (DN) is: CN=awaters, OU=sales, DC=westsim, DC=com
Relative Distinguished Name (RDN)	The Relative Distinguished Name (RDN) is used to identify the object within its container. The RDN needs to be unique only within the object's container. In the example above, the RDN is **CN=awaters**.

2.4. User Account Management

Keep in mind the following recommendations when managing user accounts:

- Use Active Directory Users and Computers from a domain controller or workstation with Administrative Tools installed to configure domain accounts.
- To modify properties on multiple user accounts at once, use the **Shift** or **Ctrl** keys to select all users, then edit the necessary properties. Properties such as the logon name or password cannot be modified in this way.
- You can move user accounts to add them to the appropriate OUs. Grouping users within OUs allows you to apply Group Policy settings to groups of users.
- When creating a new user account or resetting a forgotten password, a common practice is to reset the user account password, then select **User must change password at next logon**. This forces the user to reset the password immediately following logon, ensuring that the user will be the only person who knows the password.
- Enable the **User cannot change password** option when you want to maintain control over a Guest, service, or temporary account. For example, many applications use service accounts for performing system tasks. The application must be configured with the user account name and password. If you allow changing the user account password for the service account, you would also need to change the password within every application that uses that account.
- To reset the user account password, right-click the user object and select **Reset Password**.
- An account which has been locked out because too many incorrect passwords have been entered must be *unlocked*. To unlock an account, go to the **Account** tab in the account object's Properties dialog box, and select the **Unlock Account** box. Resetting the password on the account also unlocks a user account.
- You can configure an expiration date for temporary user accounts. Once the account is expired, it cannot be used for logon.
- If a user will be gone for an extended period of time, disable the account. This prevents the account from being used during the user's absence. Enable the account when the user returns.

- Configure the logon hours for a user account to allow the account to only be used between specific hours.
    - Logon attempts outside of the specified hours will not be allowed.
    - Users who are currently logged on will be allowed to continue working when the logon hours expire.
    - To log a user off when the logon hours pass, configure Group Policy settings to log the user off automatically.
- You can configure a list of workstations that a user is allowed to log on to. When configured, logon to other user accounts will not be allowed.
- The user profile tracks user environment settings, such as program-specific settings, user security settings and desktop settings (including the files, folders, and shortcuts on the desktop).
    - By default, the profile is stored on the local computer. A profile will be created on each computer when a user logs on.
    - To make profile settings consistent across computers, use a roaming user profile (where the profile is saved on a network share). When the user logs on, profile settings are copied from the network to the local computer. Changes made on the local computer are saved back to the network share.
    - To use a roaming profile, edit the user account properties and specify the profile path. To simplify administration, use the **%username%** variable in the **Profile Path**. Active Directory replaces **%username%** with the user logon name.
- If you accidentally delete a user account, restore it from backup rather than creating a new one with the same name. Creating a new account with the same name results in a user account with a different SID and will not automatically assume the permissions and memberships of the previously deleted account.
- *Deprovisioning* is the process of removing access rights for users when they leave your organization.
    - If the user will be replaced by another user, disable the existing account. When the new user starts, rename the account, reset the password, and enable the account. This process preserves all of the permissions and other settings associated with the user.
    - If the user will not be replaced, you can delete the account. Be sure to reassign any permissions to other users, reassign ownership over files, or delete unnecessary files such as the user profile. After a user

account has been deleted, all permissions and memberships that are associated with that user account are permanently deleted. All permissions and memberships must be recreated manually if you want to duplicate a deleted user account.
    - Many third-party tools exist that can simplify the deprovisioning process. For example, you can delete the user account and automatically reassign permissions or file ownership with a single step. You can also create your own deprovisioning solution through a programming language to synchronize accounts between databases or applications.
- To create another user account similar to an existing user, copy the existing user account. You will be prompted for a new name and password. Existing account settings and group memberships will be copied to the new account. Permissions will *not* be copied to the new account.
- If you regularly create user accounts with the same settings, you can create a template account. The template account is a normal user account with the settings you need for subsequent accounts.
    - Copy the account whenever you need to create a new one.
    - New accounts retain group memberships but not direct permission assignments.
    - Disable this account to prevent it from being used for logon.
- Adding a User Principal Name (UPN) suffix to a forest allows the users who join the forest to use a friendly user-logon name that does not match the domain name. To add a UPN suffix to a forest:
    1. Open Active Directory Domains and Trusts.
    2. Right-click **Active Directory Domains and Trusts** in the **Tree** window pane, then select **Properties**.
    3. Type the new UPN suffix that you would like to add to the forest on the **UPN Suffixes** tab.
    4. Click **Add.**
    5. Click **OK**.

2.5. Computer Account

A *computer account* is an Active Directory object that identifies a network computer. The account in Active Directory is associated with a specific hardware device. To identify a specific computer, two processes are required:

- Create a computer account in Active Directory.
- Join a computer to the domain. When you join the domain, the device is associated with the Active Directory computer account.

You can perform these processes in two different ways:

- From Active Directory Users and Computers, create a computer account. This process is called *prestaging* computer accounts. From the workstation, join the domain. The workstation will be associated with the computer account you created previously.
- From the workstation, join the domain. If the computer account does not exist in Active Directory, it will be created automatically. When you join a domain and create a new computer account in one step, the computer account is added to the Computers built-in folder in Active Directory.

Be aware of the following facts about computer accounts and joining a domain:

- Because the Computers folder is not an OU, you cannot link a GPO to this container, meaning that only Group Policy settings in the domain will apply to these computers. For more control over Group Policy settings for computers or groups of computers, move computer accounts to OUs.
- To control where computer accounts are placed when the computer joins the domain, create computer accounts ahead of time before joining the domain from the workstation.
- The following group members can create a computer account:
    - Account Operators
    - Domain Admins
    - Enterprise Admins
- Members of the Authenticated Users group can join up to 10 computers to a domain from a workstation (and create the computer account automatically if it does not already exist). This ability comes from the **Add**

workstations to a domain user right. You can also allow specific users to join specific computers to a domain by selecting **The following user or group can join this computer to a domain** when creating the computer account.

- You can grant other users permissions to create computer accounts by giving them the **Create Computer Objects** right over the Active Directory OU. This permission does not have a limit on the number of accounts that can be created. **Note:** You must grant this right to the domain or specific OUs.
- To join a computer to a domain, you must be a member of the Administrators group on the local computer or be given the necessary rights.
- Use the **dsadd** and **netdom** utilities to create computer accounts from a command prompt or a script. Use **netdom** to rename a computer account. Use **netdom join** to join a computer to a domain.
- After a computer account is created, you must join the computer to the domain before the computer receives Group Policy settings or before Active Directory receives workstation-specific information.

Each computer has a password that is automatically-generated when the computer joins the domain.

- When the computer boots, this password is used to authenticate the computer to the domain. This password is used to establish a secure channel between the computer and the domain controller.
- The password is saved on the local computer and in Active Directory. By default, the password is changed automatically every 30 days.
- If the two passwords become unsynchronized, the computer will not be able to connect to the domain, and you will see an error indicating that the computer failed to authenticate. This problem will also occur if you have rebuilt the computer, or if you are replacing the computer with another one using the same computer account name.
- When computer logon fails, reset the computer account. To reset the account, use one of the following methods:
    - Run the **netdom reset** command followed by the computer account name and the domain.
    - In Active Directory Users and Computers, right-click the computer account and select **Reset Account**.

- Create a script in Visual Basic.

After resetting the computer account, you must rejoin the computer to the domain.

2.6. What is a Group?

A *group* is used to collect user accounts, computer accounts, and other group accounts into manageable units. Working with groups instead of individual user accounts helps simplify network maintenance and administration. For instance, through groups the users receive all the user rights assigned to the group and all the permissions assigned to the group on any shared resources.

Like user accounts, there are both local and domain groups.

- Local groups exist only on the local computer, and control access to local resources.
- Domain groups exist in Active Directory, and can be used to control access to domain and local resources. In an Enterprise environment, you will work mainly with domain groups.

Active Directory groups have a group *scope*. The scope defines the potential group membership and the resource access that can be controlled through the group. The following table lists the different security group scopes and their membership and use.

Group scope	Membership	Resource Access
Global	Global groups can contain members within the same domain. These include: • Global groups in the same domain (in native mode only). • Users and computers within the same domain. Use global groups to group users and computers within	Global groups can be assigned permissions to resources anywhere in the forest. Create global groups to organize users (e.g., Sales or Development).

	the domain who have similar access needs.	
Domain Local	Domain local groups can contain members from any domain in the forest. These include: • Domain local groups in the same domain (in native mode only). • Global groups within the forest. • Universal groups within the forest (in native mode only). • Users and computers within the forest.	Domain local groups can be assigned permissions within a domain. Create domain local groups representative of the domain controller resources to which you want to control access, and then assign permissions on the resource to the group.
Universal	Universal groups can contain members from any domain in the forest. These include: • Universal groups within the forest. • Global groups within the forest. • Users and computers within the forest.	Universal groups can be assigned permissions to resources anywhere in the forest. Universal group membership should be relatively stable. For this reason, you should only add global or universal groups to universal groups. Avoid adding user accounts directly to universal groups.

In addition to the group scope, there are two types of groups:

Group Type	Description
Security	A *security* group is one that can be used to manage rights and permissions. • Group members get the permissions that are granted to the group. • A security group represents an object with a security identifier (SID), which through the *member* attribute, collects other objects, such as users, computers, contacts, and other groups.
Distribution	A *distribution* group is used to maintain a list of users and is typically used for sending e-mails to all group members. Distribution groups cannot be used for assigning permissions.

Be aware of the following when managing groups:

- The basic best practices for user and group security are:
  - Create groups based on user access needs.
  - Assign user accounts to the appropriate groups.
  - Assign permissions to each group based on the resource needs of the users in the group and the security needs of your network.
- After creating a group, you may need to convert the group's scope and/or type.
  - Converting a security group to a distribution group removes permissions assigned to the group. This could prevent or allow unwanted access.
  - You cannot directly convert a group from global to domain local or domain local to global. Instead, convert the group to a universal group and apply the changes, then convert the group to the desired scope.
  - If a global group is nested in another global group, the nested global group cannot be converted to a universal group because a universal group cannot be a member of a global group.
- To add or remove members of a group, use one of the following methods:

- On the group object, edit the **Members** tab and add the group members. Use this method to efficiently add multiple members to the same group.
- On the user account, edit the **Members Of** tab and select the group to which you want to add the user. The **Member Of** tab displays all of groups to which the object is a member. Use this method to efficiently add a single user to multiple groups.

Because a group can be a member of another group, a group object also has a **Member Of** tab. Adding objects to the **Member Of** tab for a group makes the group a member of another group (it does not add members to the group).

- When you delete a group, all information about the group (including any permissions assigned to the group) is deleted. User accounts, however, are not deleted. They are simply no longer associated with the group. If you delete the group, use one of the following strategies to recover it:
  - Re-create the group, add all the original group members, and reassign any permissions granted to the group.
  - Restore the group from a recent backup.

2.7. Default Local Groups

A local group is created and available only a local, single computer. Windows creates default local groups automatically during installation. These groups have default rights, permissions, and group memberships. You can rename these groups, but cannot delete them. Some default groups are listed in the following table:

Group	Description
Administrators	Members of the Administrators group have complete and unrestricted access to the computer, including every system right. The group contains the Administrator user account (by default) and any account designated as a *computer administrator*.
Backup Operators	Members of the Backup Operators group can back up and restore files (regardless of permissions), log on locally, and shut down the system. However, members cannot change security settings.
Users	Members of the Users group: • Can use the computer but cannot perform system administration tasks and might not be able to run legacy applications. • Cannot share directories or install printers if the driver is not yet installed. • Cannot view or modify system files. You should know the following about the Users group: • Any user created with Local Users and Groups is automatically a member of this group. • User accounts designated as *limited use* accounts are members of this group.

Power Users	Members of the Power Users group have no more user rights or permissions than a standard user account, by default. For legacy applications requiring the same Power User rights and permissions that were present in previous versions of Windows, administrators can apply a security template that enables the Power Users group to assume the same rights and permissions present in previous versions of Windows.
Guests	Members of the Guests group have limited rights (similar to members of the Users group), such as shutting down the system. Members of the Guests group have a temporary profile created at log on, that is then deleted when the member logs off.

***Note**: Additional groups, such as Network Configuration Operators and Replicator, also exist. Additionally, many features or applications may create default groups. In most cases, you should not modify the membership or privileges of these groups without understanding how they are used.*

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

2.8. Default Domain Groups

A *domain group* is a resource group to which permissions to access resources can be assigned on a domain-wide scale. Active Directory includes several default groups that are created automatically. These groups have default members, rights, and permissions. The following table lists some of the default groups that are created in the Builtin folder:

Builtin Group	Description
Administrators	Full control over the computer, including every available right in the system (the only built-in account that automatically has all rights), including the Take ownership of files or other objects right.
Server Operators	Log on locally, backup and restore files and directories, change the system time, and force a local or remote shutdown. Can also create and delete shared resources, format the hard disk, and start and stop some services. Abilities extend to domain controllers.
Backup Operators	Back up, copy, and restore files on the computer (regardless of permissions). Log on to and shut down the computer. Cannot change security settings.
Account Operators	Create, delete, and modify domain user accounts and groups. Cannot modify the Administrators group or any Operators groups.
Guests	The domain Guest account is a member of this group. The group does not have any default rights.
Network Configuration Operators	Change TCP/IP settings including changes on domain controllers.
Print Operators	Create, share, manage, and delete printers on domain controllers. Manage Active Directory printer objects. Log on locally, add or remove device drivers, and shut down domain controllers.

Users	Perform common tasks such as running applications, using local and remote printers, and locking workstations. By default, all domain members are members of this group.

Additional domain groups are also created in the Users folder in Active Directory. The following table describes some of these groups:

User Group	Description
Domain Admins	Full control over the domain. This group is a member of the Administrators group on all computers when they are joined to the domain. This means that members of the Domain Admins group can perform all tasks on any computer in the domain (including domain controllers).
Domain Computers	Contains all computers that are a member of the domain. When you join a computer to the domain, it becomes a member of this group.
Domain Controllers	Contains all domain controllers. When a computer is made a domain controller, it is added to this group.
Domain Guests	Contains all domain guests. It does not have any default rights.
Domain Users	Contains all domain users. This group can be used to give access to all users in a domain.
Enterprise Admins	Full control over all domains in the forest. This group is a member of the Administrators group on all computers in the forest, allowing them to perform any task on any computer in the forest.
Schema Admins	Full control over the Active Directory schema. By default, the Administrator account is a member of this group.
Read-only Domain Controllers	Contains all members who have administrative access to the Read-Only Domain Controllers in the domain.
DHCP Administrators	Contains all members who have administrative access to the DHCP service.

Cert Publishers	Contains all members which are permitted to publish certificates to the directory.

When working with domain networking resources, use domain groups for controlling access. However, to enable users to manage local systems, make domain user or group accounts members of the local groups.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

2.9. Group Strategy

To make permission assignments easier, assign permissions to a group, then add the accounts that need to use the group's resources. You can add user accounts, computers, and other groups to groups. Remember the following when assigning members to groups:

- Adding a user account to a group gives that account all the permissions and rights granted to the group (the user must log off and log back on before the change takes effect).
- The same user account can be included in multiple groups. (This multiple inclusion may lead to permissions conflicts, so be aware of the permissions assigned to each group.)
- *Nesting* is the technique of making a group a member of another group. Using hierarchies of nested groups may make administration simpler--as long as you remember what permissions you have assigned at each level.

The following table shows the three basic recommended approaches to managing users, groups, and permissions.

Strategy	Use	Description	Application
AGDLP	Used in mixed mode domains and in native mode domains (does not use universal groups, which are also not available in mixed mode).	**A**: Place user Accounts **G**: Into Global groups **DL**: Into Domain Local groups **P**: Assign Permissions to domain local groups	1. Identify the users in the domain who use the same resources and perform the same tasks. Group these accounts together in global groups. 2. Create new domain local groups if necessary, or use the built-in groups to control access to resources. 3. Combine all global groups that need access to the same resources into the

			domain local group that controls those resources. 4. Assign permissions to the resources to the domain local group.
AGUDLP	Used in native mode domains, when there is more than one domain, and you need to grant access to similar groups defined in multiple domains.	**A**: Place user Accounts **G**: Into Global groups **U**: Into Universal groups **DL**: Into Domain Local groups **P**: Assign Permissions to domain local groups	Universal groups should be used when you need to grant access to similar groups defined in multiple domains. It is best to add global groups to universal groups, instead of placing user accounts directly in universal groups.
ALP	Used on workstations and member servers.	**A**: Place user Accounts **L**: Into Local groups **P**: Assign Permissions to the local groups	ALP is best used in a workgroup environment, not in a domain.

To keep the number of groups to a minimum, you should *not* automatically use universal groups, even though they might be supported.

- Use universal groups only if both the users and the resources are located in *multiple* domains.
- You would *not* need universal groups in a single-domain design.
- You would *not* need universal groups if the resources you were controlling access to were located in a single domain.

2.10. Object Management Tool

If you have a small number of objects to create or modify, you can use the following tools:

Tool	Description
Active Directory Users and Computers	Use the Active Directory Users and Computers MMC snap-in to create, organize, and delete objects in Active Directory. Active Directory Users and Computers can be started from: • Server Manager • Administrative Tools (from the Control Panel or Start menu) • Running **dsa.msc**
ADSI Edit	Active Directory Service Interfaces Editor (ADSI Edit) acts as a low-level GUI editor for common administrative tasks such as adding, deleting, and moving objects. It runs within the Microsoft Management Console (MMC). You can use ADSI Edit to query, view, and edit attributes that are not exposed through other MMC snap-ins (such as Active Directory Users and Computers).
Command Prompt	Use the following command prompt tools to manage Active Directory objects, either from a command prompt or within a script. • **Dsadd** creates a new object in Active Directory. • **Dsquery** finds objects that match the search criteria (allows a search through the whole forest). The command returns a list of objects that match the search criteria. Use **Dsquery *** to search all object types. • **Dsget** retrieves property information about an object. Use the **-expand** switch to show nested group membership for users. • **Dsmod** modifies or changes the properties of an object.

	• **Dsmove** moves objects from one location to another and renames an object. • **Dsrm** removes (deletes) objects. Use the **-subtree** option to delete a container object and all objects below that object. • **Movetree** moves an OU and its objects (it does not move computer objects). • **Netdom** adds computer objects, joins a computer to a domain, and moves computer objects. Be aware of the following facts about using the **Ds** commands to work with Active Directory objects: • When using the command, follow the command with the type of object you want to edit (e.g. user, computer, or group). For example, to create a new user account, use the **Dsadd user** command, followed by the various parameters required to configure the object. • For all commands except for **Dsquery**, you must identify the object or objects you want to modify. For example, **Dsget** returns properties of a specific object, while **Dsquery** returns a list of objects that match the query parameters. • When moving objects, you should typically use Active Directory Users and Computers instead of **Dsmove**. Active Directory Users and Computers perform additional actions that **Dsmove** does not.

2.11. Bulk Object Management

Use the following tools if you have a large number of objects to create or modify:

Tool	Description

Csvde	The **Csvde** command imports and exports Active Directory objects using a comma-separated list file.
	
	• **Csvde** can read existing information from Active Directory (export) or create new objects in Active Directory (import).
	• You cannot use **Csvde** to modify existing objects in Active Directory.
	• Common uses for **Csvde** include:
	  o Using **Csvde** to export objects from one Active Directory system (or an Exchange 5.5 database) and import them into a different Active Directory database.
	  o Using a database program to create a CSV file, modifying the file, and importing the objects into Active Directory.
	• **Csvde** switches include:
	  o **-i** to import objects
	  o **-e** to export objects
	  o **-f** to identify the filename
	
	Note: When you export user accounts with **Csvde**, passwords are not exported. You cannot import passwords for user accounts using **Csvde**.

Ldifde	The **Ldifde** command imports, exports, modify, and delete objects in Active Directory using LDAP Data Interchange Format (LDIF) files. • **Ldifde** files include a **changeType** parameter that identifies the action to take using the data in the file: o Add

	- Modify - Delete - Common uses for **Ldifde** include: - Using **Ldifde** to export a set of Active Directory objects, modifying various attributes, and then re-importing the file to change the attributes. - Exporting or importing data that exists on non-Active Directory LDAP directories. **Ldifde** switches include: **-i** to import objects **-e** to export objects **-f** to identify the filename **Note**: When you export user accounts with **Ldifde**, passwords are not exported. You can change passwords for existing user accounts using an **.ldif** file, but you cannot create new user accounts with a password. To export user accounts and import them with a password, use the following process: - Export the user accounts. The **unicodePwd** field will be blank. - Import the user accounts to create the accounts. The user accounts will be disabled, and the user will be forced to change the password at next logon. - Modify the **.ldif** file to change the operation to modify existing objects. Add a password for each user account and add entries to enable the account. - Run **Ldifde** using the file with the passwords to modify the existing user accounts.
PowerShell	Windows PowerShell is a command line environment designed for automating administration and maintenance for Windows Server 2008/2012/2016. PowerShell uses specialized commands, known as *cmdlets*, to create and manage Active Directory objects. Cmdlets can execute single commands or large scripts which, for example, can import a CSV file and use the information to create new Active Directory users.

	Be aware of the following: • Stringing together the actions of two or more cmdlets is known as *pipelining* (also called *piping*). Output from the first cmdlet is fed into the second cmdlet (and so on). • Using cmdlets scripts to create and manage accounts in Active Directory requires a thorough knowledge of programming.
Visual Basic scripts (VBscripts)	Visual Basic scripts (VBscripts) can also be used to create and manage objects within the Active Directory database. Using VBscripts to create and manage accounts in Active Directory requires a thorough knowledge of programming.
Ldp	The **Ldp** utility allows you to search for and view the properties of multiple Active Directory objects. It is a GUI-based, Windows Explorer-like utility with a scope pane on the left that is used for navigating through the Active Directory namespace, and a details pane on the right that is used for displaying results.
Active Directory Migration Tool (ADMT)	The Active Directory Migration Tool (ADMT) is a GUI-based utility that helps you restructure your Active Directory organization or migrate objects from one domain to another. • You can move objects to different domains within the same forest (intraforest), or to domains in other forests (interforest). • Use the SID history feature to enable migrated accounts to be able to continue to access resources in the original domain. For intraforest moves, SID history is enabled automatically. • Use a SID mapping file to map security objects in one domain with security objects in another domain. For example, you can translate group membership in one domain and have user's added to similar groups in the target domain. • Use the password migration DLL to migrate passwords between forests. Passwords remain protected

	throughout the migration process. Passwords are automatically migrated for intraforest move operations. • For interforest migration, the target forest must trust the source forest. Trusts already exist within a forest.