- 2. 3. Users and Groups Management -

- INDEX -

- 2. 3. 1. Managing Users -

Local users and domain users

A local user is one whose username and encrypted password are stored on the computer itself.

When you log in as a local user, the computer checks its own list of users and its own password file to see if you are allowed to log into the computer.

The computer itself then applies all the permissions (e.g., “can use the CD-ROM”, “can install programs”) and restrictions (e.g., “cannot install programs”) that are assigned to you for that computer.

A domain user is one whose username and password are stored on a domain controller rather than the computer the user is logging into.

When you log in as a domain user, the computer asks the domain controller what privileges are assigned to you.

When the computer receives an appropriate response from the domain controller, it logs you in with the proper permissions and restrictions.

Domain users evolved in response to the challenges administrators face when managing large numbers of computers, peripherals (e.g., printers, network storage), services, and users.

When a network has a large population of users on various computers, it is difficult to maintain information for every user on each individual computer.

The task of managing so many users is simplified by allowing each computer to validate access through a central source to see if each user can log in and use computing resources.

With one centralized source of user info, network administrators have only a small set of computers on which to maintain user information.

Domain users are managed in a domain controller using the "Active Directory Users and Computers" program.

User profiles

The system creates a user profile the first time that a user logs on to a computer.

At subsequent logons, the system loads the user's profile, and then other system components configure the user's environment according to the information in the profile.

A user profile consists of the 2 following elements:

1. A registry hive.

The registry hive is the file NTuser.dat.

The hive is loaded by the system at user logon, and it is mapped to the HKEY_CURRENT_USER registry key.

The user's registry hive maintains the user's registry-based preferences and configuration.

2. A set of profile folders stored in the file system.

User-profile files are stored in the "Users" directory, on a folder per-user basis.

The user-profile folder is a container for applications and other system components to populate with sub-folders, and per-user data such as documents and configuration files.

Windows Explorer uses the user-profile folders extensively for such items as the user's Desktop, Start menu and Documents folder.

User profiles provide the following advantages:

- When the user logs on to a computer, the system uses the same settings that were in use when the user last logged off.
- When sharing a computer with other users, each user receives their customized desktop after logging on.
- Settings in the user profile are unique to each user. The settings cannot be accessed by other users. Changes made to one user's profile do not affect other users or other users' profiles.

There are 4 types of User Profiles:

1. Local User Profiles

A local user profile is created the first time that a user logs on to a computer.

The profile is stored on the computer's local hard disk.

Changes made to the local user profile are specific to the user and to the computer on which the changes are made.

2. Roaming User Profiles

A roaming user profile is a copy of the local profile that is copied to, and stored on, a server share.

This profile is downloaded to any computer that a user logs onto on a network.

Changes made to a roaming user profile are synchronized with the server copy of the profile when the user logs off.

The advantage of roaming user profiles is that users do not need to create a profile on each computer they use on a network.

3. Mandatory User Profiles

A mandatory user profile is a type of profile that administrators can use to specify settings for users.

Only system administrators can make changes to mandatory user profiles.

Changes made by users to desktop settings are lost when the user logs off.

4. Temporary User Profiles

A temporary profile is issued each time that an error condition prevents the user's profile from loading.

Temporary profiles are deleted at the end of each session, and changes made by the user to desktop settings and files are lost when the user logs off.

- 2. 3. 2. Managing Groups -

Understanding groups

A group is a collection of user and computer accounts, contacts, and other groups that you can manage 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.

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).

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.

Group types

There are two types of groups in Active Directory Domain Services: distribution groups and security groups.

You can use distribution groups to create e-mail distribution lists.

You can use distribution groups only with e-mail applications (such as Microsoft Exchange Server) 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).

You can use security groups to assign permissions to shared resources.

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 AD DS 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.

They also 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.

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 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 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.

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.

Domain local groups

Members of domain local groups can include other groups and accounts from Windows Server 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:

- Accounts from any domain.
- Global groups from any domain.
- Universal groups from any domain.
- Domain local groups, but only from the same domain as the parent domain local group.
- 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.

Global groups

Members of global groups can include accounts from the same domain as the parent global group and global groups from the same domain as the parent global group.

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: it is 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.

Universal groups

Members of universal groups can have the following as their members:

- Accounts from any domain within the forest in which this Universal Group resides.
- Global groups from any domain within the forest in which this Universal Group resides.
- Universal groups from any domain within the forest in which this Universal Group resides.

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 that have 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.

Managing users and groups

A practical way to work with users and groups is the following:

1. Create the user.
2. Include that user in a global group.
3. Include that global group in a domain local group.

4. Assign permissions to that domain local group.

- 2. 3. 3. Managing Organizational Units -

Understanding Organizational Units

A particularly useful type of directory object that is contained within domains is the organizational unit (OU).

OUs are Active Directory containers into which you can place users, groups, computers, and other OUs.

An OU cannot contain objects from other domains.

An OU is the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority.

Using OUs, you can create containers within a domain that represent the hierarchical, logical structures in your organization.

You can then manage the configuration and use of accounts and resources based on your organizational model.

OUs can contain other OUs.

You can extend a hierarchy of OUs as necessary to model your organization's hierarchy within a domain.

Using OUs helps you minimize the number of domains that are required for your network.

You can use OUs to create an administrative model that you can scale to any size.

A user can have administrative authority for all OUs in a domain or for a single OU.

An administrator of an OU does not have to have administrative authority for any other OUs in the domain.

- 2. 3. 4. Exercises -

You are going to create a new Google Document inside the "2. Windows Server" folder of your Google Drive, named:

"2. 3. Users and Groups Management - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit.

Exercise 1: Changing the Password Policy

1. Although in a real company the password policy of the domain controller should follow the restrictions that come by default in Windows Server when installing the operating system, in our exercises we will modify the password policy so that it does not have to meet the complexity requirements that defines Windows Server and thus make it easier to create users and assign them simpler passwords.
2. Login to your Windows Server with the “Administrator” user.
3. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
4. On the left tree -> select your domain -> Users -> right click -> New -> User.
5. Try to create a user with the password “balmis”: Windows Server should not allow you to use this password.
6. Go to: Start button -> Windows Administrative Tools -> Group Policy Management.
7. Open the tree on the left: Group Policy Management -> Forest: (“your domain”) -> Domains -> “your domain” -> Default Domain Policy -> right click -> “Edit”.
8. You will get the “Group Policy Management Editor”.
9. Open the tree on the left: Default Domain Policy -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Accounts Policies -> Password Policy.
10. Change the password policies that you want.
11. After you have changed the password policies, go to the Windows search box, write “CMD” and in the CMD console write “gpupdate /force” and press “ENTER”.
12. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.

13. On the left tree -> select your domain -> Users -> right click -> New -> User.
14. Try to create a user with the password “balmis”: Windows Server should allow you to use this password.

Exercise 2: Create an Organizational Unit (OU)

1. Login to your Windows Server with the “Administrator” user.
2. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
3. On the left tree -> select your domain -> right click -> New -> Organizational Unit.
4. Name: “**XXX**-Company”, being **XXX** your first name.
5. OK.

Exercise 3: Managing an Organizational Unit (OU)

1. Let’s suppose that your company has 4 departments: IT (Information Technology), Sales, Marketing and HR (Human Resources).
2. Login to your Windows Server with the “Administrator” user.
3. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
4. On the left tree, select the Organizational Unit that you have created in the previous exercise.
5. Below that Organizational Unit, create 4 new Organizational Units: “IT”, “Sales”, “Marketing” and “HR”.

Exercise 4: Creating Users

1. Login to your Windows Server with the “Administrator” user.
2. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
3. On the left tree, select your company Organizational Unit.
4. You are going to create 8 new users. Each new user will have the following fields:
    - First name: a random first name.

    - Last name: a random last name.
    - User logon name: “firstname.lastname”.
    - “Next”.
    - Password: “Balmis2”.
    - Uncheck “User must change password at next logon”.
    - Check “Password never expires”.
5. After creating those 8 users, move them (2 per Organizational Unit) to the 4 Organizational Units: “IT”, “Sales”, “Marketing” and “HR”.

Note: you can “clone” users selecting a user in “Active Directory Users and Computers”, right click, and “Copy”.

Exercise 5: Creating Groups

NOTE: If 2 or more persons are using the same Domain Controller, the second person that will create the following groups is going to need to add a number **"2"** at the end of the groups names.

For example, if the first person has created before the “IT Global Group”, the second person will create the “IT Global Group **2**”.

1. Login to your Windows Server with the “Administrator” user.
2. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
3. On the left tree, select your company Organizational Unit.
4. You are going to create 4 new groups with “Group scope: Global” and “Group type: Security” with the following “Group names”:
    - “IT Global Group”.
    - “Sales Global Group”.
    - “Marketing Global Group”.
    - “HR Global Group”.
5. Move all those global groups to their correspondent Organizationals Units: “IT Global Group” to the “IT” OU, “Sales Global Group” to the “Sales” OU, “Marketing Global Group” to the “Marketing” OU, and “HR Global Group” to the “HR” OU.
6. Include each user of every OU into the correspondent Global Group of his/her department.
7. On the left tree, select your company Organizational Unit.
8. You are going to create 4 new groups with “Group scope: Domain local” and “Group type: Security” with the following “Group names”:
    - “IT Local Group”.
    - “Sales Local Group”.
    - “Marketing Local Group”.
    - “HR Local Group”.

9. Move all those local groups to their correspondent Organizationals Units: “IT Local Group” to the “IT” OU, “Sales Local Group” to the “Sales” OU, “Marketing Local Group” to the “Marketing” OU, and “HR Local Group” to the “HR” OU.
10. Include each Global Group into the correspondent Local Group of each department:
    - “IT Global Group” inside “IT Local Group”.
    - “Sales Global Group” inside “Sales Local Group”.
    - “Marketing Global Group” inside “Marketing Local Group”.
    - “HR Global Group” inside “HR Local Group”.
11. On the left tree, select your company Organizational Unit.
12. Create a new group (“Group scope: Domain local” and “Group type: Security”) named: “**XXX** Company Local Group”, being **XXX** your first name.
13. Include inside the local group “**XXX** Company Local Group” the following groups:
    - “IT Global Group”.
    - “Sales Global Group”.
    - “Marketing Global Group”.
    - “HR Global Group”.
14. That way, the local group “**XXX** Company Local Group” contains all the users of your Company, because every user is included in the global group of his/her department.

Exercise 6: Login to the Domain from a Client

1. Open your Windows 10 client (virtual machine).
2. Try to login to your Domain with one of the Domain users that you have created in the previous exercises.

Exercise 7: Managing the users passwords

1. Login to your Windows Server with the “Administrator” user.
2. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
3. On the left tree, select your company Organizational Unit.
4. Select the “Sales” OU.
5. Select a user from the “Sales” OU -> right click -> Properties -> “Account” tab -> Account options -> Uncheck “Password never expires” -> Check “User must change password at next logon” -> OK.
6. Open your Windows 10 client.

7. Try to login to your Domain with the “Sales” department user.
8. Before loading the Windows desktop, Windows 10 should ask you to change the “Sales” department user’s password: you must write the password twice: use “Balmis3” as the password. After changing the password, Windows should continue with the normal starting.
9. Logout from Windows 10 with the “Sales” department user.
10. Login to your Windows Server with the “Administrator” user.
11. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
12. Select the “Sales” department user -> right click -> Properties -> “Account” tab -> Account options -> Check “Password never expires” -> OK.
13. Select the “Sales” department user -> right click -> “Reset password…”.
14. Write twice “Balmis4” as the new password for the “Sales” department user.
15. Open your Windows 10 client.
16. Try to login to your Domain with the “Sales” department user with the previous password (“Balmis3”): Windows should not allow you to login.
17. Try to login to your Domain with the “Sales” department user with the current password (“Balmis4”). Windows should allow you to login.

Exercise 8: Managing the users logon

1. Login to your Windows Server with the “Administrator” user.
2. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
3. On the left tree, select your company Organizational Unit.
4. Select the “Marketing” OU.
5. Select a user from the “Marketing” OU -> right click -> Properties -> “Account” tab -> “Logon Hours…” button -> Choose that this user only has the “Logon Permitted” (blue color) from 01:00 to 05:00 hours.
6. Open your Windows 10 client.
7. Try to login to your Domain with the “Marketing” department user.
8. Because the time is not probably between 01:00 to 05:00, Windows 10 should not allow you to login.
9. Login to your Windows Server with the “Administrator” user.
10. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
11. On the left tree, select your company Organizational Unit.
12. Select the “Marketing” OU.
13. Select a user from the “Marketing” OU -> right click -> Properties -> “Account” tab -> “Logon Hours…” button -> Choose that this user only has the “Logon Permitted” (blue color) from 00:00 to 24:00 hours. That is the original way.
14. Open your Windows 10 client.
15. Try to login to your Domain with the “Marketing” department user.

16. Now Windows 10 should allow you to login.
17. Login to your Windows Server with the “Administrator” user.
18. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
19. On the left tree, select your company Organizational Unit.
20. Select the “Marketing” OU.
21. Select a user from the “Marketing” OU -> right click -> Properties -> “Account” tab -> “Log On To…” button -> Select “The following computers” -> Add the Windows 10 client of one of your partners. NOTE: Before doing this, you should add your partner’s Windows 10 client to your Domain in order to do this part of the exercise.
22. Open your Windows 10 client.
23. Try to login to your Domain with the “Marketing” department user.
24. Windows 10 should not allow you to login, because your computer is not in the “Log On To…” list of the “Marketing” department user.
25. Open your partner’s Windows 10 client.
26. Try to login to your Domain with the “Marketing” department user.
27. Now Windows 10 should allow you to login, because this computer is in the “Log On To…” list of the “Marketing” department user.
28. Login to your Windows Server with the “Administrator” user.
29. Go to Start -> Windows Administrative Tools -> Active Directory Users and Computers.
30. On the left tree, select your company Organizational Unit.
31. Select the “Marketing” OU.
32. Select a user from the “Marketing” OU -> right click -> Properties -> “Account” tab -> “Log On To…” button -> Select “All computers”.
33. Open your Windows 10 client.
34. Try to login to your Domain with the “Marketing” department user.
35. Now Windows 10 should allow you to login.

Exercise 9: Setting the Proxy configuration in the Domain Controller

1. Login to your Windows Server with the “Administrator” user.
2. Go to: Start button -> Windows Administrative Tools -> Group Policy Management.
3. Open the tree on the left: Group Policy Management -> Forest: (“your domain”) -> Domains -> “your domain” -> Default Domain Policy -> right click -> “Edit”.
4. You will get the “Group Policy Management Editor”.
5. Open the tree on the left: Default Domain Policy -> User Configuration -> Preferences -> Control Panel Settings -> Internet Settings -> (on the right panel, right click) "New" -> Select "Internet Explorer 10" -> (right click) Properties -> "Connections" tab -> "LAN settings" button -> Proxy server -> Check "Use a proxy server for your LAN" -> Address: 192.168.0.100 -> Port: 8080

-> Check "Bypass proxy server for local addresses". If these fields are underlined with a red colour, you have to select those fields and press the F6 button in order to change those fields to a green colour. After changing the red colour to the green colour -> "OK" -> "OK".

6. After you have done this in your Domain Controller, open your Windows 10 client.
7. In your Windows 10 client, login to your Domain with a “HR” department user that has never logged into your Domain.
8. Open Google Chrome and check if you have an Internet connection.
9. To check if the user has got the Proxy settings from your Domain Controller, in your Windows 10 client, go to: Settings -> Network & Internet -> Proxy -> Manual proxy setup. Check that "Use a proxy server" is "On", and that in the "Address" and "Port" fields you have the correct information that you have set up before in your Domain Controller.