- 2. 4. Managing network shares -

- INDEX -

2. 4. 1. Users Rights

2. 4. 2. Permissions

2. 4. 3. Exercises

- 2. 4. 1. Users Rights -

Users Rights

A right is an attribute of a user (or group) that allows him to perform a specific action to the whole system, not to a particular resource.

Users rights authorize users to perform specific actions, such as logging on to a system interactively or backing up files and directories.

User rights are different from permissions because they apply to user accounts, whereas permissions are attached to objects.

Keep in mind that changes made to user rights can have a far-reaching effect.

Because of this, only experienced administrators should make changes to the user rights policy.

Microsoft defines user rights in two types of categories: Logon Rights and Privileges.

These are defined as follows:

1.Logon Right:

A user right that is assigned to a user and that specifies the ways in which a user can log onto a system.

An example of a logon right is the right to log on to a system remotely.

2. Privilege:

A user right that is assigned to a user who has already been logged into the system and that specifies allowable actions on the system.

An example of a privilege is the right to shut down a system, making backups, changing the system date and time, etc.

User rights define capabilities at the local level.

Although they can apply to individual user accounts, user rights are best administered on a group account basis.

This ensures that a user logging on as a member of a group automatically inherits the rights associated with that group.

By assigning rights to groups rather than individual users, user account administration can be simplified.

When users in a group all require the same user rights, they can be assigned the set of rights once to the group, rather than repeatedly assigning the same set to each individual user account.

User rights that are assigned to a group are applied to all members of the group while they remain members.

If a user is a member of multiple groups, the user's rights are cumulative, which means that the user has more than one set of rights and privileges.

The only time that rights assigned to one group might conflict with those assigned to another is in the case of certain logon rights.

For example a member of multiple groups who is given the "Deny Access to This Computer from the Network" logon right would not be able to log on despite the logon rights granted to the user by other groups.

In general, however, user rights assigned to one group do not conflict with the rights assigned to another group.

To remove rights from a user, the administrator simply removes the user from the group.

In this case, the user no longer has the rights assigned to that group.

Some of the privileges can override permissions set on an object.

For example, a user logged on to a domain account as a member of the Backup Operators group has the right to perform backup operations for all domain servers.

However, this requires the ability to read all files on those servers, even files on which their owners have set permissions that explicitly deny access to all other users, including members of the Backup Operators group.

A user privilege, in this case, the right to perform a backup, takes precedence over all file and directory permissions.

The privileges, which can override permissions set on an object, are the following:

- Take Ownership of Files or Other Objects.
- Manage Auditing and Security Log.
- Back Up Files and Directories.
- Restore Files and Directories.
- Debug Programs.
- Bypass Traverse Checking.

Assigning Users Rights

User rights policies can be administered as follows:

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 -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies.
6. Select User Rights Assignment. Note: All policies are either defined or not defined. That is, they are either configured for use or not configured for use. A policy that is not defined in the current container could be inherited from another container.
7. To configure user rights assignment, double-click a user right or right-click on it and select Security. This opens a Security Policy Setting dialog box. For a site, domain, or organizational unit, individual user rights can be configured by completing the following steps:
8. Open the Security Policy Setting dialog box for the user right to be modified.

9. Select Define these policy settings to define the policy.
10. To apply the right to a user or group, click Add.
11. In the Add user or group dialog box, click Browse. This opens the Select Users Or Groups dialog box. The right can now be applied to users and groups.

- 2. 4. 2. Permissions -

Permissions

Permissions are a key component of the Windows Server security architecture that you can use to manage the process of authorizing users, groups, and computers to access objects on a network.

Permissions enable the owner of each secured object, such as a file, Active Directory object, or registry key, to control who can perform an operation or a set of operations on the object or object property.

Because access to an object is at the owner's discretion, the type of access control that is used in Windows Server is called discretionary access control.

An owner of an object always has the ability to read and change permissions on the object.

Permissions are applied to secured objects, such as files and folders, Active Directory objects, services, or registry objects.

Permissions can be granted to a user, group, or computer.

You can assign permissions on objects to the following:

- Groups, users, and special identities in the domain.
- Groups and users in the domain and any trusted domains.
- Local groups and users on the computer where the object resides.

Granting and Denying Permissions

A permission is authorization to perform an operation on a specific object, such as a file.

Permissions can be granted by owners and by anyone with the permission to grant permissions, which normally includes administrators on the system.

If you own an object, you can grant any user or security group any permission on that object, including the permission to take ownership.

When permission to perform an operation is not explicitly granted, it is implicitly denied.

For example, if Alice allows the Marketing group, and only the Marketing group, permission to read her file, users who are not members of the Marketing group are implicitly denied access.

Permissions can also be explicitly denied.

For example, Alice might not want Bob to be able to read her file, even though he is a member of the Marketing group.

She can exclude Bob by explicitly denying him permission to read the file.

This is normally how explicit denies are used — to exclude a subset (such as Bob) from a larger group (such as Marketing) that has been given permission to perform an operation.

Note that use of explicit denials, while possible, increases the complexity of the authorization policy and can create unexpected errors.

For example, you might want to allow domain administrators to perform an action but deny domain users.

If you attempt to implement this by explicitly denying domain users, you also deny any domain administrators who are also domain users.

Though it is sometimes necessary, you can and should avoid the use of explicit denies in most cases.

Each permission that an object's owner grants to a particular user or group is stored as an ACE (Access Control Entry) in a Discretionary Access Control List (DACL) that is part of the object's security descriptor.

Permissions and Security Descriptors

Every container and object on the network has a set of access control information attached to it that is called a security descriptor.

This information controls the type of access that is allowed to users and groups.

The security descriptor is automatically created along with the container or object that is created.

For example, each file has a security descriptor.

An object's security descriptor contains its permissions.

Permissions are associated with, or assigned to, specific users and groups.

For example, for a file Temp.dat, the Administrator group might be assigned Read, Write, and Delete permissions, while the Operator group might be assigned Read and Write permissions only.

Each assignment of permissions to a user or group is called a permission entry, which is a type of ACE (Access Control Entry).

The entire set of permission entries in a security descriptor is known as a permission set or ACL (Access Control List).

Therefore, for the file named Temp.dat, the permission set includes two permission entries, one for the Administrator group and one for the Operator group.

Ownership

Every object has an owner, whether in an NTFS volume or in Active Directory.

The owner controls how permissions are set on the object and to whom permissions are granted.

By default, in Windows Server, the owner is the creator of the object.

If the creator of an object is a member of the Administrators group, the Administrators group is the owner.

The owner can always change permissions on an object, even when denied all access to the object.

Ownership can be taken by the following:

- Any user with the "Take ownership of files or other objects" user right, which can be granted to any user. By default, the Administrators group is given the "Take ownership of files or other objects" user right. An administrator who wants to repair or change permissions on a file must begin by taking ownership of the file.
- Anyone or any group who has the "Take ownership" permission on the object in question.
- A user who has the "Restore files and directories" user right.

Ownership can be transferred in the following ways:

- The current owner can grant the “Take ownership” permission to another user, allowing that user to take ownership at any time. The user must actually take ownership to complete the transfer.
- An administrator can take ownership.
- A user who has the “Restore files and directories” user right can assign ownership to any user or group.

Explicit vs. Inherited Permissions

There are two types of permissions, explicit permissions and inherited permissions:

- Explicit permissions are those that are set by default when the object is created or by user action.
- Inherited permissions are those that are propagated to a child object from a parent object. Inherited permissions ease the task of managing permissions and ensure consistency of permissions among all objects in a given container.

By default, objects that are created in a container inherit the permissions from that container when the objects are created.

For example, when you create a folder called MyFolder, all subfolders and files that are created in MyFolder automatically inherit the permissions from MyFolder.

Therefore, MyFolder has explicit permissions, while all subfolders and files in it have inherited permissions.

Notes:

- Inherited Deny permissions do not prevent access to an object if the object has an explicit Allow permission entry.
- Explicit permissions take precedence over inherited permissions, even inherited Deny permissions.

So the Discretionary Access Control List (DACL) of every folder is formed by 2 lists:

- Inherited Discretionary Access Control List (DACL): permissions that the current folder inherits from its parent folder.
- Explicit Discretionary Access Control List (DACL): permissions that you manually set up in the current folder.

Permissions on a Shared Folder

Access on a shared folder is determined through two sets of permission entries: the permissions that are set on the share (called share permissions) and the permissions that are set on the folder (called NTFS file and folder permissions).

Share permissions are often used for managing computers with FAT32 file systems or for managing other computers that do not use the NTFS file system.

Share permissions and NTFS permissions are independent in the sense that neither changes the other.

The final access permissions on a shared folder are determined by taking into consideration both the share permission and the NTFS permission entries.

The more restrictive permissions are then applied.

Experienced administrators prefer to always set share permissions to Full Control for Everyone and to rely entirely on NTFS permissions to restrict access.

You should know the following information:

- NTFS permissions affect access both locally and remotely. NTFS permissions apply regardless of protocol. Share permissions, by contrast, apply only to network shares. Share permissions do not restrict access to any local user, or to any terminal server user, of the computer on which you have set share permissions. Therefore, share permissions do not provide privacy between users on a computer that is used by several users, nor on a terminal server that is accessed by several users.
- By default, Everyone does not include Anonymous Users; therefore, permissions that are applied to Everyone do not affect Anonymous Users.
- A user who places a file on a share is the creator of that copy of the file and therefore has the ability to read and change the permissions on the file independent of the permissions that are inherited.
- When possible, you should attempt to grant permissions to groups instead of to specific user accounts.

- Exercises -

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

"2. 4. Managing network shares - 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: Sharing a folder accessible to all the users of the company

On the Domain Controller (Windows Server), it is usual to place the folders that we are going to share located in a disk partition where we store user data, for example, in the partition D: \ ("DATA") of the server.

Maybe your Windows Server only has one partition (C:\), so for doing these exercises you can use that "C:\" partition to place all the shared folders.

In order to have the server's hard drive well organized, we can save all the shared folders to a folder called:

C:\XXX-Company\Shared\

being **XXX** your first name.

We will prepare the folder structure of the server to house all the shared folders that we will use in the future in "our company".

Thus, we will use a particular folder structure that may work well in these exercises, but on a server of a real company we may need a different folder structure.

Therefore, we will have to study the situation in each case, so that the folder structure can meet our current requirements and be scalable in the future.

1. Login to your Windows Server with the "Administrator" user.

2. On your server, open “File Explorer” and create the following folder -> C:\XXX-Company\Shared\
3. Right click on C:\XXX-Company\Shared\ -> Properties -> “Security” tab.
4. Notice that the “Users” group (that contains the “Domain Users”, i.e., all the users of the Domain) is included here with “Read” permissions (among others). This means that any Domain user could access the content of this folder. To avoid that, you are going to follow the next steps.
5. In the “Security” tab of the C:\XXX-Company\Shared\ folder -> Click on the “Edit” button -> Select the “Users” group -> Click on the “Remove” button in order to try to delete the “Users” group from the list. You should not be allowed to do this because this folder has inherited the permissions of the root folder (C:\), and the “Users” group with read permissions is included by default.
6. To allow you to delete the “Users” group-> Right click on C:\XXX-Company\Shared\ -> Properties -> “Security” tab -> Click on the “Advanced options” button -> “Disable inheritance” button -> To the question “What would you like to do with the current inherited permissions?” -> Answer: “Convert inherited permissions into explicit permissions on this object” -> “OK” -> “OK”.
7. Now you should be able to delete the “Users” group with the “Remove” button -> Right click on C:\XXX-Company\Shared\ -> Properties -> “Security” tab -> Click on the “Edit” button -> Select the “Users” group -> Click on the “Remove” button -> “OK” -> “OK”.
8. Right click on C:\XXX-Company\Shared\ -> Properties -> “Security” tab -> Click on the “Edit” button -> “Add” button -> Add the “Domain admins” group -> Give “Full control” permissions in the “Allow” column.
9. Right click on C:\XXX-Company\Shared\ -> Properties -> “Security” tab -> Click on the “Advanced options” button -> “Permissions” tab -> Check the option “Replace all child object permission entries with inheritable permission entries from this object” -> Answer “Yes” to the question “This will replace defined permissions explicitly in all descendants” -> “OK” -> “OK”. This way all the objects (files and folders) that you create below the “C:\XXX-Company\Shared\” folder will inherit the permissions of this folder, not the root folder (C:\).
10. Create the following folder -> C:\XXX-Company\Shared\Public
11. Check that the C:\XXX-Company\Shared\Public folder has the same NTFS permissions (“Security” tab) than its parent folder C:\XXX-Company\Shared\
12. The C:\XXX-Company\Shared\Public folder will be used to share common and public information between all the workers of the company. That is, all the users of the company must have access to this folder. So you are going to give the proper permissions.
13. Right click on C:\XXX-Company\Shared\Public -> Properties -> “Sharing” tab -> Click on the “Advanced Sharing” button -> Check “Share this folder” -> In “Share name:” write “Public-**XXX-Company**” being **XXX** your name ->

“Permissions” button -> Check “Full Control” on the “Allow” column for the “Everyone” group -> “OK” -> “OK” -> “Close”.

14. Open your Windows 10 client.
15. Login into Windows 10 (into your domain) with one of the users of your company that you have created before in “Active Directory Users and Computers”.
16. Open “File Explorer” and in the address bar write \\Name-of-your-server -> “OK”. The “Name-of-your-server” should be something like “WS-1DAM-**XY**”, being **XY** the last 2 digits of your real computer’s IP.
17. You will see a list of all the shared (and visible) folders of your domain controller (server).
18. The “Public-**XXX-Company**” (being **XXX** your name) shared folder that you have shared before should appear here.
19. Try to access to the “Public-**XXX-Company**” (being **XXX** your name) shared folder: you should not have access, because the user of your company has “shared permissions” to access this folder, but that user does not have “NTFS permissions” to access this folder.
20. Logout from the Windows 10 client.
21. Login to your Windows Server with the “Administrator” user.
22. File Explorer -> Right click on C:\XXX-Company\Shared\Public -> Properties -> “Security” tab -> Click on the “Edit” button -> “Add” button -> Add the “**XXX** Company Local Group” group (being “**XXX**” your name) -> Give “Full control” permissions in the “Allow” column.
23. This way, all the users of your company should have permissions to access to the C:\XXX-Company\Shared\Public folder.
24. Open your Windows 10 client.
25. Login into Windows 10 (into your domain) with one of the users of your company that you have created before in “Active Directory Users and Computers”.
26. Open “File Explorer” and in the address bar write \\Name-of-your-server -> “OK”. The “Name-of-your-server” should be something like “WS-1DAM-**XY**”, being **XY** the last 2 digits of your real computer’s IP.
27. You will see a list of all the shared (and visible) folders of your domain controller (server).
28. The “Public-**XXX-Company**” (being **XXX** your name) shared folder that you have shared before should appear here.
29. Try to access to the “Public-**XXX-Company**” (being **XXX** your name) shared folder: now you should have access, because the user of your company has “shared permissions” to access this folder, and that user also has “NTFS permissions” to access this folder.
30. Try to create a new document and a new folder inside the “Public-**XXX-Company**” (being **XXX** your name) shared folder: you should be able to do this.
31. Remember that everything that you do inside the “Public-**XXX-Company**” (being **XXX** your name) shared folder while using it in Windows 10, in reality

you are doing it to the "C:\XXX-Company\Shared\Public" folder of your Windows Server.

32. Logout from the Windows 10 client.
33. Login into Windows 10 (into your domain) with another user of your company and repeat the latest actions in order to check if every user of the company has permissions in the "Public-**XXX-Company**" (being **XXX** your name) shared folder.

Exercise 2: Sharing a folder accessible to the users of one department

In the previous exercise you have shared a folder ("Public") in the Domain Controller with all the users of the company.

In this exercise you are going to share a folder but with a more limited access: only the users of the "Marketing" department are going to be allowed to access to this folder.

1. Login to your Windows Server with the "Administrator" user.
2. On your server, open "File Explorer" and create the following folder -> C:\XXX-Company\Shared\Marketing
3. Right click on C:\XXX-Company\Shared\Marketing -> Properties -> "Sharing" tab -> Click on the "Advanced Sharing" button -> Check "Share this folder" -> In "Share name:" write "Marketing-**XXX-Company**" being **XXX** your name -> "Permissions" button -> Check "Full Control" on the "Allow" column for the "Everyone" group -> "OK" -> "OK" -> "Close". Remember that you always have to do this when you want to share a folder in order to avoid problems with the shared resources permissions.
4. File Explorer -> Right click on C:\XXX-Company\Shared\Marketing -> Properties -> "Security" tab -> Click on the "Edit" button -> "Add" button -> Add the "Marketing Local Group" group -> Give "Full control" permissions in the "Allow" column.
5. Open your Windows 10 client.
6. Login into Windows 10 (into your domain) with one of the users of the "Marketing" department that you have created before in "Active Directory Users and Computers".
7. Open "File Explorer" and in the address bar write \\Name-of-your-server -> "OK". The "Name-of-your-server" should be something like "WS-1DAM-**XY**", being **XY** the last 2 digits of your real computer's IP.
8. You will see a list of all the shared (and visible) folders of your domain controller (server).

9. The "Marketing-**XXX-Company**" (being **XXX** your name) shared folder that you have shared before should appear here.
10. Try to access to the "Marketing-**XXX-Company**" (being **XXX** your name) shared folder: you should have access, because the user of the "Marketing" department has "shared permissions" to access this folder, and that user has "NTFS permissions" to access this folder.
11. Try to create a new document and a new folder inside the "Marketing-**XXX-Company**" (being **XXX** your name) shared folder: you should be able to do this.
12. Logout from the Windows 10 client.
13. Login into Windows 10 (into your domain) with one of the users of the "IT" department (NOT the "Marketing" department) that you have created before in "Active Directory Users and Computers".
14. Open "File Explorer" and in the address bar write \\Name-of-your-server -> "OK". The "Name-of-your-server" should be something like "WS-1DAM-**XY**", being **XY** the last 2 digits of your real computer's IP.
15. You will see a list of all the shared (and visible) folders of your domain controller (server).
16. The "Marketing-**XXX-Company**" (being **XXX** your name) shared folder that you have shared before should appear here.
17. Try to access to the "Marketing-**XXX-Company**" (being **XXX** your name) shared folder: you should not have access, because the user of the "IT" department has "shared permissions" to access this folder, but that user does not have "NTFS permissions" to access this folder.
18. Repeat the steps of the creation of the "C:\XXX-Company\Shared\Marketing" shared folder with the proper shared and NTFS permissions, with the other departments: Sales and HR.

Exercise 3: Sharing a hidden folder accessible to the users of one department

In this exercise you are going to share a folder but with limited access: only the users of the "IT" department are going to be allowed to access this folder.

Besides, this is going to be a "hidden" shared folder: that means that this folder is not going to be shown in the "shared resources" of your server when you access it from a client.

1. Login to your Windows Server with the "Administrator" user.

2. On your server, open "File Explorer" and select the following folder that it should already exists -> C:\XXX-Company\Shared\IT
3. Right click on C:\XXX-Company\Shared\IT -> Properties -> "Sharing" tab -> Click on the "Advanced Sharing" button -> Check "Share this folder" -> In the "Name of the shared resource" write "IT-**XXX-Company**$" (being **XXX** your name) note that the $ is the item that hides this shared folder -> "Permissions" button -> Check "Full Control" on the "Allow" column for the "Everyone" group -> "OK" -> "OK" -> "Close".
4. File Explorer -> Right click on C:\XXX-Company\Shared\IT -> Properties -> "Security" tab -> Click on the "Edit" button -> "Add" button -> Add the "IT Local Group" group -> Give "Full control" permissions in the "Allow" column.
5. Open your Windows 10 client.
6. Login into Windows 10 (into your domain) with one of the users of the "IT" department that you have created before in "Active Directory Users and Computers".
7. Open "File Explorer" and in the address bar write \\Name-of-your-server -> "OK". The "Name-of-your-server" should be something like "WS-1DAM-**XY**", being **XY** the last 2 digits of your real computer's IP.
8. You will see a list of all the shared (and visible) folders of your domain controller (server).
9. The "IT-**XXX-Company**" (being **XXX** your name) shared hidden folder that you have shared before should NOT appear here, because it is a hidden shared folder.
10. In order to access to the "IT-**XXX-Company**" (being **XXX** your name) shared hidden folder, open "File Explorer" and in the address bar you have to write the following (remember to write the dollar sign $) -> \\Name-of-your-server\"IT-**XXX-Company**$" (being **XXX** your name) -> "OK". This way, writing the complete path, we "unhide" the hidden shared folder.
11. Try to access to the "IT-**XXX-Company**" (being **XXX** your name) shared hidden folder: you should have access, because the user of the "IT" department has "shared permissions" to access this folder, and that user has "NTFS permissions" to access this folder.
12. Try to create a new document and a new folder inside the "IT-**XXX-Company**" (being **XXX** your name) shared hidden folder: you should be able to do this.
13. Logout from the Windows 10 client.
14. Login into Windows 10 (into your domain) with one of the users of the "Marketing" department (NOT the "IT" department) that you have created before in "Active Directory Users and Computers".
15. Open "File Explorer" and in the address bar write \\Name-of-your-server\"IT-**XXX-Company**$" (being **XXX** your name) -> "OK".
16. Try to access to the "IT-**XXX-Company**" (being **XXX** your name) shared hidden folder: you should not have access, because the user of the "Marketing" department has "shared permissions" to access this folder, but that user does not have "NTFS permissions" to access this folder.

Exercise 4: Sharing a hidden folder accessible to one user

In this exercise you are going to share a folder but with a more limited access yet: only one user of the domain is going to be allowed to access to this folder.

Besides, this is going to be a "hidden" shared folder: that means that this folder is not going to be shown in the "shared resources" of your server when you access it from a client. Hiding a folder with only access of a unique user is a common practice.

1. Login to your Windows Server with the "Administrator" user.
2. On your server, open "File Explorer" and create the following folder -> C:\XXX-Company\Shared\Users
3. Create the following folder -> C:\XXX-Company\Shared\Users\Name-LastName being "Name-LastName" the "Name" and the "Last Name" of a user of the "Sales" department.
4. Right click on C:\XXX-Company\Shared\Users\Name-LastName -> Properties -> "Sharing" tab -> Click on the "Advanced options" button -> Check "Advanced sharing" -> In the "Name of the shared resource" write "Name-LastName$" (the $ is the item that hides this shared folder; being "Name-LastName" the "Name" and the "Last Name" of a user of the "Sales" department) -> "Permissions" button -> Check "Full Control" on the "Allow" column for the "Everyone" group -> "OK" -> "OK" -> "Close".
5. File Explorer -> Right click on C:\XXX-Company\Shared\Users\Name-LastName -> Properties -> "Security" tab -> Click on the "Edit" button -> "Add" button -> Add the "Name-LastName" user of the "Sales" department -> Give "Full control" permissions in the "Allow" column.
6. Open your Windows 10 client.
7. Login into Windows 10 (into your domain) with the "Name-LastName" user of the "Sales" department that you have created before in "Active Directory Users and Computers".
8. Open "File Explorer" and in the address bar write \\Name-of-your-server -> "OK". The "Name-of-your-server" should be something like "WS-1DAM-**XY**", being **XY** the last 2 digits of your real computer's IP.
9. You will see a list of all the shared (and visible) folders of your domain controller (server).
10. The "Name-LastName" folder that you have shared before should NOT appear here, because it is a hidden shared folder.

11. In order to access to the “Name-LastName” hidden shared folder, open “File Explorer” and in the address bar you have to write the following (remember to write the dollar sign $) -> \\Name-of-your-server\Name-LastName$ ->”OK”. This way, writing the complete path, we “unhide” the hidden shared folder.
12. Try to access the “Name-LastName” hidden folder: you should have access, because the “Name-LastName” user of the “Sales” department has “shared permissions” to access this folder, and that user has “NTFS permissions” to access this folder.
13. Try to create a new document and a new folder inside the “Name-LastName” folder: you should be able to do this.
14. Logout from the Windows 10 client.
15. Login into Windows 10 (into your domain) with one of the users of the “Marketing” department (NOT the “Name-LastName” user of the “Sales” department) that you have created before in “Active Directory Users and Computers”.
16. Open “File Explorer” and in the address bar write \\Name-of-your-server\Name-LastName$ -> “OK”.
17. Try to access the “Name-LastName” folder: you should not have access, because the user of the “Marketing” department has “shared permissions” to access this folder, but that user does not have “NTFS permissions” to access this folder.
18. Login to your Windows Server with the “Administrator” user.
19. On your server, open “File Explorer” and delete the following folder -> C:\XXX-Company\Shared\Users\Name-LastName being “Name-LastName” the “Name” and the “Last Name” of a user of the “Sales” department.

Exercise 5: "Shared Folders" application

In this exercise we are going to check the "Shared Folders" application in your Windows Server.

With the "Shared Folders" application you can see all the shared folders that are created in your Windows Server in order to control and to manage them properly.

1. Login to your Windows Server with the “Administrator” user.
2. Click on the "Start" button on the lower left corner -> "Windows Administrative Tools" -> "Computer Management".
3. On the "Computer Management" application, on the left column, click on "Shared Folder" -> "Shares".

4. On the right column, you can see all the shared folders of your Windows Server.
5. If you select any of the shared folders of this right column and right click on "Properties", you can see 3 tabs:
    1. General: here you can see the share name, folder path, description and user limit.
    2. Share Permissions: here you can see and modify the shared permissions of the shared folder.
    3. Security: here you can see and modify the NTFS permissions of the shared folder.

Exercise 6: Local Profile

In this exercise we are going to review local profiles, that are the only ones that we have worked with until now.

1. Open your Windows 10 client.
2. Login into Windows 10 (into your domain) with one of the users of the "IT" department that you have created before in "Active Directory Users and Computers".
3. Go to the Windows 10 desktop and create some new shortcuts to programs like: Notepad, Calculator, etc.
4. Check the content of the folder -> C:\Users\%UserName%\Desktop (%UserName% is a Windows variable that contains the user logon name, like "name.lastname").
5. In that folder you should see the new shortcuts that you have just created.
6. Logout from the Windows 10 client.
7. Go to a different PC (with Windows 10) of one of your partners and add this Windows 10 client to your Domain.
8. Login into your partner's PC with Windows 10 (into your domain) with the same user of the "IT" department of your Domain.
9. Check that the shortcuts that you have created before in your PC are not in your partner's PC Desktop.
10. Check that the shortcuts that you have created before in your PC are not in your partner's PC in the folder -> C:\Users\%UserName%\Desktop
11. Logout from the Windows 10 client of your partner.

Exercise 7: Roaming Profile – Profile path

In this exercise we are going to create a Roaming Profile and work with the Profile Path.

1. Login to your Windows Server with the "Administrator" user.
2. On your server, open "File Explorer" and create the following folder -> C:\XXX-Company\Shared\Users\Profiles
3. In this folder you are going to store all the Roaming Profiles of the users of the company. Now you are going to share this folder and to change its shared resource permissions.
4. Right click on C:\XXX-Company\Shared\Users\Profiles -> Properties -> "Sharing" tab -> Click on the "Advanced Sharing" button -> Check "Share this folder" -> In the "Name of the shared resource" write: "Profiles-**XXX-Company**$" (being **XXX** your name), note that the $ is the item that hides this shared folder -> "Permissions" button -> Check "Full Control" on the "Allow" column for the "Everyone" group -> "OK" -> "OK" -> "Close".
5. Now you are going to change the NTFS permissions of this folder.
6. File Explorer -> Right click on C:\XXX-Company\Shared\Users\Profiles -> Properties -> "Security" tab -> Click on the "Edit" button -> "Add" button -> Add the "Users" group -> Give "Full Control" permissions in the "Allow" column.
7. Open "Active Directory Users and Computers".
8. Select a user of the "HR" department -> Right click -> Properties -> "Profile" tab.
9. In "User Profile" -> "Profile path" write the following: \\\\Name-of-your-server\Profiles-**XXX-Company**$\%UserName% (being **XXX** your name).
10. Click "OK".
11. Again, select the same user of the "HR" department -> Right click -> Properties -> "Profile" tab. The environment variable %UserName% should be now the "User logon name" of that user.
12. Login into Windows 10 (into your domain) with the user of the "HR" department.
13. Go to the Windows 10 desktop and create some new shortcuts to programs like: Notepad, Calculator, etc.
14. Logout from the Windows 10 client.
15. Login to your Windows Server with the "Administrator" user.
16. In File Explorer, try to open the folder -> C:\XXX-Company\Shared\Users\Profiles\%UserName% being %UserName% the same user of the "HR" department. You should not be

able to access this folder, because the "Administrator" user does not have NTFS permissions to read this folder.

17. Login into Windows 10 (into your domain) with the user of the "HR" department.
18. Open "File Explorer" and in the address bar you have to write the following (remember to write the dollar sign $) -> \\Name-of-your-server\Profiles-**XXX-Company**$\%UserName% ->"OK", being **XXX** your name and being %UserName% the same user of the "HR" department.
19. Open the folder "Desktop".
20. Check that there you have the new shortcuts (o programs like: Notepad, Calculator, etc.) that you have created before in Windows 10 with the "HR" user.
21. Logout from the Windows 10 client.
22. Go to a different PC (with Windows 10) of one of your partners and add this Windows 10 client to your Domain (if you haven' done it yet).
23. Login into your partner's PC with Windows 10 (into your domain) with the same user of the "HR" department of your Domain.
24. Check that the shortcuts that you have created before in your PC are also in your partner's PC Desktop.
25. Create new shortcuts in your partner's PC Desktop.
26. Logout from your partner's PC with Windows 10.
27. Login into Windows 10 (into your domain) with the user of the "HR" department.
28. Check that the new shortcuts that you have created before in your partner's PC are also in your PC Desktop.

Exercise 8: Roaming Profile – Home folder

In this exercise we are going to create a Home folder for a Roaming Profile.

We already have a server running Windows Server with the File Server function installed, so we are going to save the working files of the users (when they are using the files) directly in a folder of the server's hard drive, not in the local hard drive of each PC.

This way, we will always have the working files of the users in the server, so we can backup those files in a centralized way, and we will have those files under control.

Another advantage is that the users will have their files available from any PC in which they open a session in the domain.

However, we must be careful not to exceed the capacity of the server's hard drive , because we will be saving the files of a lot of users.

In this exercise, we are going to create the "Home folder" of the same "HR" user of your domain that you have worked with in the previous exercise.

1. Login to your Windows Server with the "Administrator" user.
2. On your server, open "File Explorer" and create the following folder -> C:\XXX-Company\Shared\Home Folders\
3. In this folder you are going to store all the Home Folders of the users of the company. Now you are going to share this folder and to change its shared resource permissions.
4. Right click on C:\XXX-Company\Shared\Home Folders\ -> Properties -> "Sharing" tab -> Click on the "Advanced Sharing" button -> Check "Share this folder" -> In the "Name of the shared resource" write "Home-Folders-**XXX-Company**$" (being **XXX** your name), note that the $ is the item that hides this shared folder -> "Permissions" button -> Check "Full Control" on the "Allow" column for the "Everyone" group -> "OK" -> "OK" -> "Close".
5. Open "Active Directory Users and Computers".
6. Select the user of the "HR" department of the previous exercise -> Right click -> Properties -> "Profile" tab.
7. In "Home folder" -> "Connect:" choose the "X:" letter, and write: \\Name-of-your-server\Home-Folders-**XXX-Company**$\%UserName% (being **XXX** your name).
8. Click "OK".
9. When you open again the "Properties" of this "HR" department user, in the "Profile" tab, check that the %UserName% variable has been changed to the real "User logon name" of that user.
10. Also, if you open "File Explorer" and check the following folder C:\XXX-Company\Shared\Home Folders\ you will see that the following folder has been created C:\XXX-Company\Shared\Home Folders\%UserName%\ , being %UserName% the real "User logon name" of that user.
11. Login into Windows 10 (into your domain) with the user of the "HR" department.
12. Open File Explorer and check that in "This PC", there is a "X:" drive letter with a label like: %UserName% in \\Name-of-your-server\Home-Folders-**XXX-Company**$\%UserName% (being **XXX** your name).

13. Try to create a new document and a new folder inside: you should be able to do this. Remember that the “X:” drive letter is not part of the PC’s hard drive (Windows 10 client), but part of your server’s hard drive.
14. This “X:” drive letter is the place where the “HR” department user (or other users of the domain) should store his working files, not in “My documents” (Windows 10 client), so you should teach the users of your company to do this.
15. Go to File Explorer -> “This PC” -> “X:” -> Right click -> “Create shortcut” -> To the question “Windows can’t create a shortcut here. Do you want the shortcut to be placed on the desktop instead?” -> Answer: “Yes”.
16. Rename that shortcut in the desktop like “Work Documents”.
17. You have to teach the users of your company to go to their desktops, open that “Work Documents” shortcut (that will go to the “X:” drive, that is the user’s Home Folder in the server), and save the working files there.
18. Login to your Windows Server with the “Administrator” user.
19. In File Explorer, open the folder -> C:\XXX-Company\Shared\Home Folders\%UserName%\ , and check that the new document and the new folder created from the Windows 10 client are there.

Exercise 9: Roaming Profile – Logon script

We are going to create a “.BAT” file to execute a script during the logon process.

1. Login to your Windows Server with the “Administrator” user.
2. On your server, go to “File Explorer” and open the following folder: C:\ -> WINDOWS -> SYSVOL -> SYSVOL -> **"Name-Of-Your-Domain"** -> SCRIPTS .
3. Go to “View” menu -> Check “File name extensions” -> “OK”.
4. Create a new file named “logon-script-**XXX-Company**.bat”, being **XXX-Company** your name.
5. Edit the “logon-script-**XXX-Company**.bat” with Notepad and write the following text inside: C:\Windows\System32\calc.exe
6. Open “Active Directory Users and Computers”, and select the “HR” department user of the previous exercise.
7. Open the user “Properties” -> “Profile” tab -> “Logon script” and write: \\\\Name-of-your-server\NETLOGON\logon-script-**XXX-Company** . Another option is to write: logon-script-**XXX-Company**.bat .
8. It is important that you do not write the “.bat” at the end of the previous line.

9. Login into Windows 10 (into your domain) with the user of the "HR" department.
10. After login, the Calculator should be started automatically because of the logon script.

Exercise 10: Mandatory Profile

In this exercise you are going to create the Roaming Profile – Profile path, of a user of the "Sales" department.

Later, you are going to transform the Roaming Profile of that user into a Mandatory Profile.

1. Login to your Windows Server with the "Administrator" user.
2. Open "Active Directory Users and Computers".
3. Select a user of the "Sales" department -> Right click -> Properties -> "Profile" tab.
4. In "User Profile" -> "Profile path" write the following: \\Name-of-your-server\Profiles-**XXX-Company**$\%UserName% (being **XXX** your name).
5. Click "OK".
6. Login into Windows 10 (into your domain) with the user of the "Sales" department.
7. Go to the Windows 10 desktop and create some new shortcuts to programs like: Notepad, Calculator, etc.
8. Logout from the Windows 10 client.
9. Login to your Windows Server with the "Administrator" user.
10. In File Explorer, try to open the folder -> C:\XXX-Company\Shared\Users\Profiles\%UserName% being %UserName% the same user of the "Sales" department. You should not be able to access to this folder, because the "Administrator" user does not have NTFS permissions to read this folder. To access to this folder with the "Administrator" user, follow the next steps.
11. In File Explorer, right click on the folder > C:\XXX-Company\Shared\Users\Profiles\%UserName% -> Properties -> "Security" tab -> "Advanced" button -> "Permissions" tab -> "Continue" button -> "Change" link -> Add the "Administrator" user -> Check "Replace owners on subcontainers and objects".

12. In the prompt window saying “You do not have permissions to read...” answer “Yes” -> “OK” -> “OK”.
13. File Explorer -> Right click on C:\XXX-Company\Shared\Users\Profiles\%UserName% -> Properties -> “Security” tab -> “Advanced” button -> “Permissions” tab -> “Add” button -> “Select a principal” -> Add the same user of the “Sales” department -> Give “Full control” permissions in the “Allow” column -> “OK”.
14. Go to the “Security” tab -> “Advanced” button -> Check “Replace all child object permissions entries with inheritable permission entries from this object” -> “OK”.
15. Prompt “Do you wish to continue?” -> “Yes” -> “OK”.
16. This way now you should have access with the “Administrator” user to the folder C:\XXX-Company\Shared\Users\Profiles\%UserName%
17. Go to the “Security” tab -> “Advanced” button -> “Owner” -> “Change” button -> Select the the same user of the “Sales” department -> Check “Replace owner on subcontainers and folders” -> “OK” -> “OK”.
18. Open the folder C:\XXX-Company\Shared\Users\Profiles\%UserName%\Desktop
19. Check that there you have the new shortcuts (to programs like: Notepad, Calculator, etc.) that you have created in Windows 10 with the “Sales” user.
20. In the folder C:\XXX-Company\Shared\Users\Profiles\%UserName%\Desktop , create a new text document with the file name "From the Server.txt". Everything that you include in this "Desktop" folder of the server will be included in the Desktop of the mandatory profile that you are going to create in the following steps.
21. Now you are going to transform the Roaming Profile of that user into a Mandatory Profile.
22. In your Windows Server, go to “File Explorer” and open the folder -> C:\XXX-Company\Shared\Users\Profiles\%UserName%\
23. In “File Explorer” go to “This PC” -> Click “View” -> Click “Show/hide” -> Check “Hidden items”.
24. Inside the folder -> C:\XXX-Company\Shared\Users\Profiles\%UserName%\ -> Locate the hidden file “NTUSER.DAT” and change its name to “NTUSER.MAN”.
25. This way you have transformed the Roaming Profile of that user into a Mandatory Profile.
26. Login into Windows 10 (into your domain) with the user of the “Sales” department.
27. Go to the Windows 10 desktop and create some other new shortcuts.
28. Logout from the Windows 10 client.
29. Login into another Windows 10 (into your domain) from one of your partners, with the user of the “Sales” department.

30. Now check that the latest desktop shortcuts that you have created are not there, because now this user has a Mandatory Profile, so the changes that you make to this user Profile, are not stored on the server.
31. You should see the first shortcuts (to programs like: Notepad, Calculator, etc.) that you have created with the "Sales" user before changing his Profile to Mandatory.

Mandatory Profiles can be used to create Active Directory users that later are used in our company for particular cases, such as:

- Guest users, who are not really employees of the company.
- Temporary workers: persons that do the same job (and maybe use the same computer) change often.

In these cases (and others) it can be interesting to have Active Directory users with a Mandatory Profile, since this way we "force" the users to load the user profile that we want.

Besides, users can't make changes in this Mandatory Profile.

Exercise 11: Trust relationships

In this exercise you are going to create a new bi-directional trusted relationship with the domain (and tree-forest) of one of your partners.

1. Login to your Windows Server with the "Administrator" user.
2. You are going to create a new bi-directional trusted relationship with the domain of your partner.
3. Go to the TCP/IP settings of your Windows Server, and on "Alternate DNS server", write the IP of the Windows Server of your partner.
4. Open "Active Directory Domains and Trusts".
5. On the left panel -> Right click on your domain -> "Properties" -> "Trusts" tab -> "New trust..." button -> "Next -> Write the name of the domain of your partner -> "Next" -> "Trust type:" -> "External trust" -> "Direction of Trust" -> "Two-way" -> "Next" -> "Sides of Trust" -> "Both this domain and the specified domain" -> "Next" -> "User Name and Password": use the Administrator of your partner's domain -> "Next" -> "Outgoing Trust Authentication Level-Local Domain" -> "Domain-wide authentication" -> "Next" -> "Outgoing Trust Authentication

Level-Specified Domain” -> “Domain-wide authentication” -> “Next” -> “Trust Selections Complete” -> “Next” -> “Trust Creation Complete” -> “Next” -> “Confirm Outgoing Trust” -> “Yes, confirm the outgoing trust” -> “Next” -> “Confirm Incoming Trust” -> “Yes, confirm the incoming trust” -> “Next” -> “Finish” -> “OK” -> “OK”.

6. Now you are going to give permissions in one of your server’s shared folders (C:\XXX-Company\Shared\Marketing) to an Active Directory group (“Sales Global Group”) of your partner’s domain.
7. On your server, go to “File Explorer” -> Right click on C:\XXX-Company\Shared\Marketing -> Properties -> “Security” tab -> Click on the “Edit” button -> “Add” button -> “Locations…” button -> Select your partner’s domain -> “OK” -> “Advanced” button -> “Find now” button -> Here you will all the users and groups of your partner’s domain -> Select the “Sales Global Group” group of your partner’s domain -> “OK” -> “OK” -> Give “Full control” permissions in the “Allow” column -> “OK” -> “OK”.
8. Open your partner’s Windows 10 client.
9. Login into Windows 10 (into your partner’s domain) with one of the users of the “Sales” department (of your partner).
10. Open “File Explorer” and in the address bar write \\Name-of-your-server -> “OK”.
11. You will see a list of all the shared (and visible) folders of your domain controller (server).
12. The “Marketing” folder (of your domain) that you have shared before should appear here.
13. Try to access to the “Marketing” folder: you should have access, because the user of the “Sales” department of your partner’s domain has “shared permissions” to access this folder (“Everyone” has “Change” access), and that user has “NTFS permissions” to access this folder because he is a member of the “Sales Global Group” group of your partner’s domain.
14. Try to create a new document and a new folder inside the “Marketing” folder: you should be able to do this.
15. Logout from the Windows 10 client.
16. Login to your Windows Server with the “Administrator” user.
17. Open “File Explorer” and open the folder C:\XXX-Company\Shared\Marketing
18. Check that the new document and the new folder created by the “Sales” user of your partner’s domain is here.