Users, groups and local policies
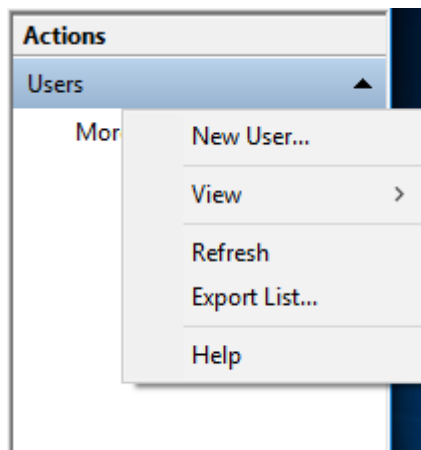
1.

We need to go to Computer management, then Users and new user.

Click on new user

We need to select User must change password at next logon then click on create.

2.

2.1

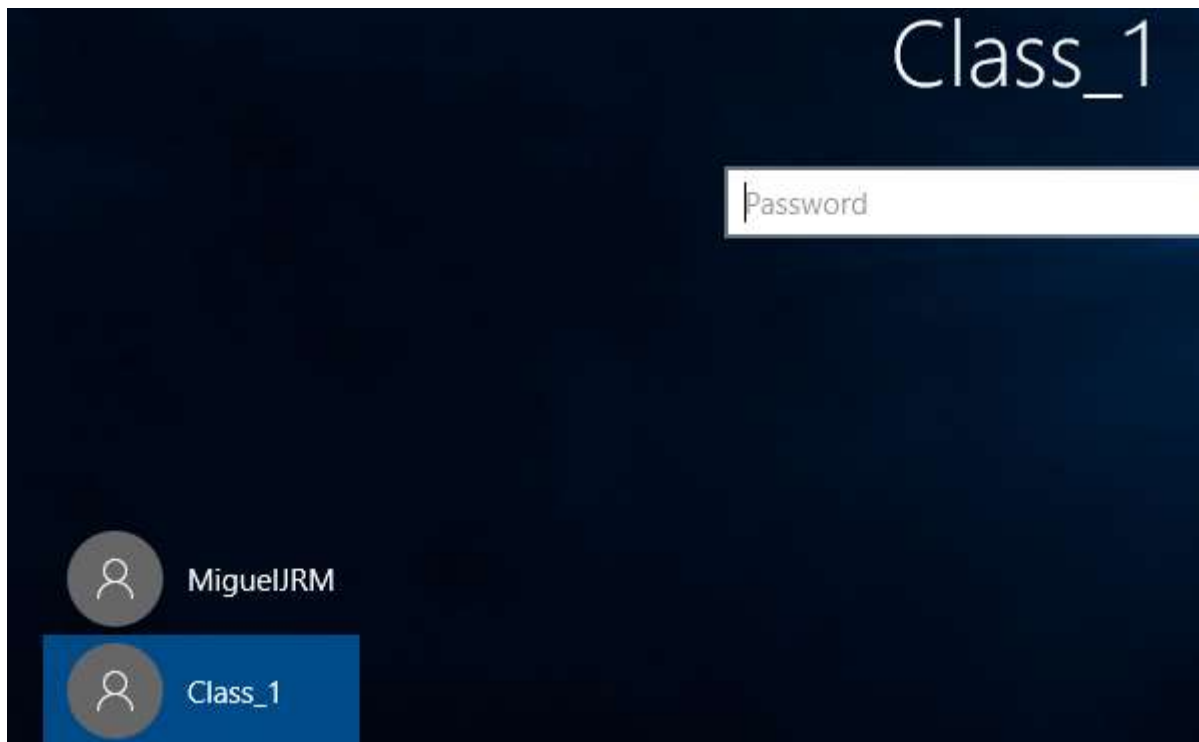This PC > Local Disk (C:) > Users >

Name

MiguelJRM

Public

The folder doesn't exist yet, until we login with the user.

2.2

2.3

Class_1
MiguelJRM
Public

2.4

Not Attached
Windows10Miguel_1.vdi 30.00 GB   2.00 MB

Search By Name ▼

Choose
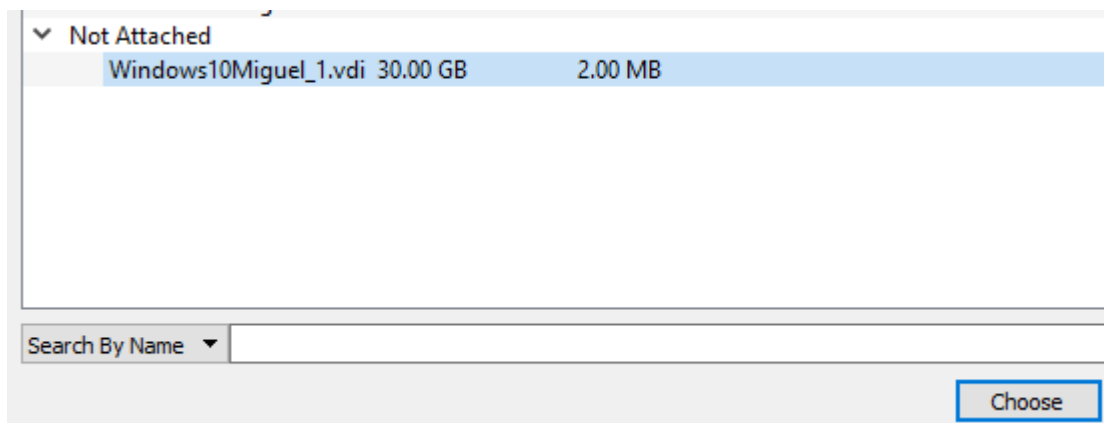
Adding the new hard drive.

Volume
(C:)
MiguelJRMVolume (F:)
System Reserved

2.5

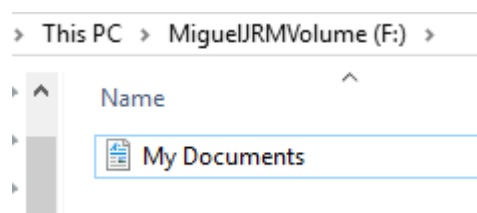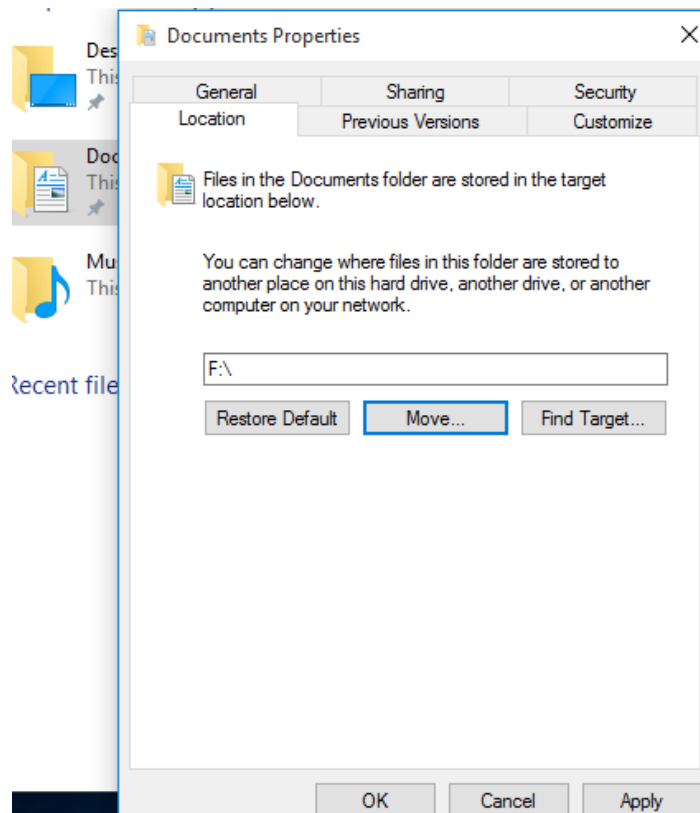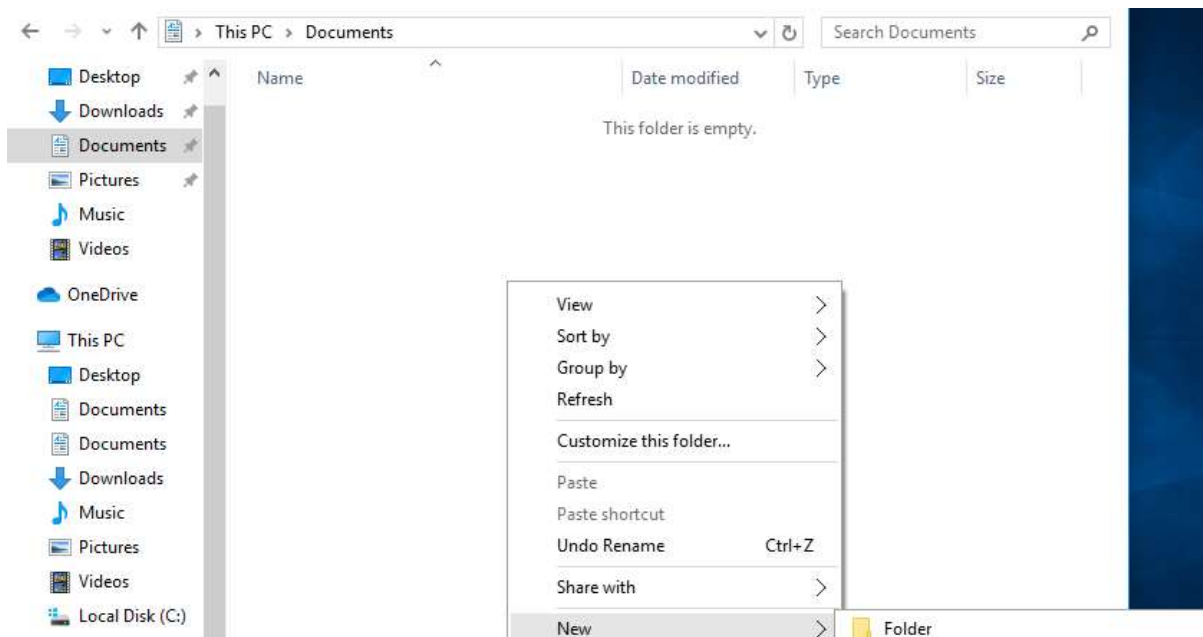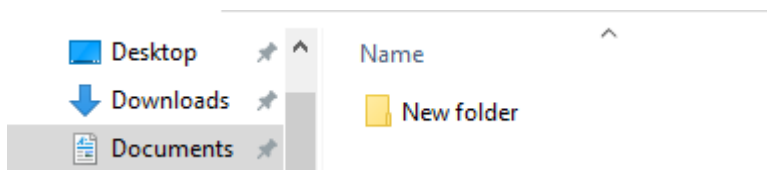Now rigth click on documents folder, properties and set the location to the new hard drive

Documents Properties   ✕

General	Sharing	Security
Location	Previous Versions	Customize

Files in the Documents folder are stored in the target location below.

You can change where files in this folder are stored to another place on this hard drive, another drive, or another computer on your network.

F:\

Restore Default   Move...   Find Target...

OK   Cancel   Apply

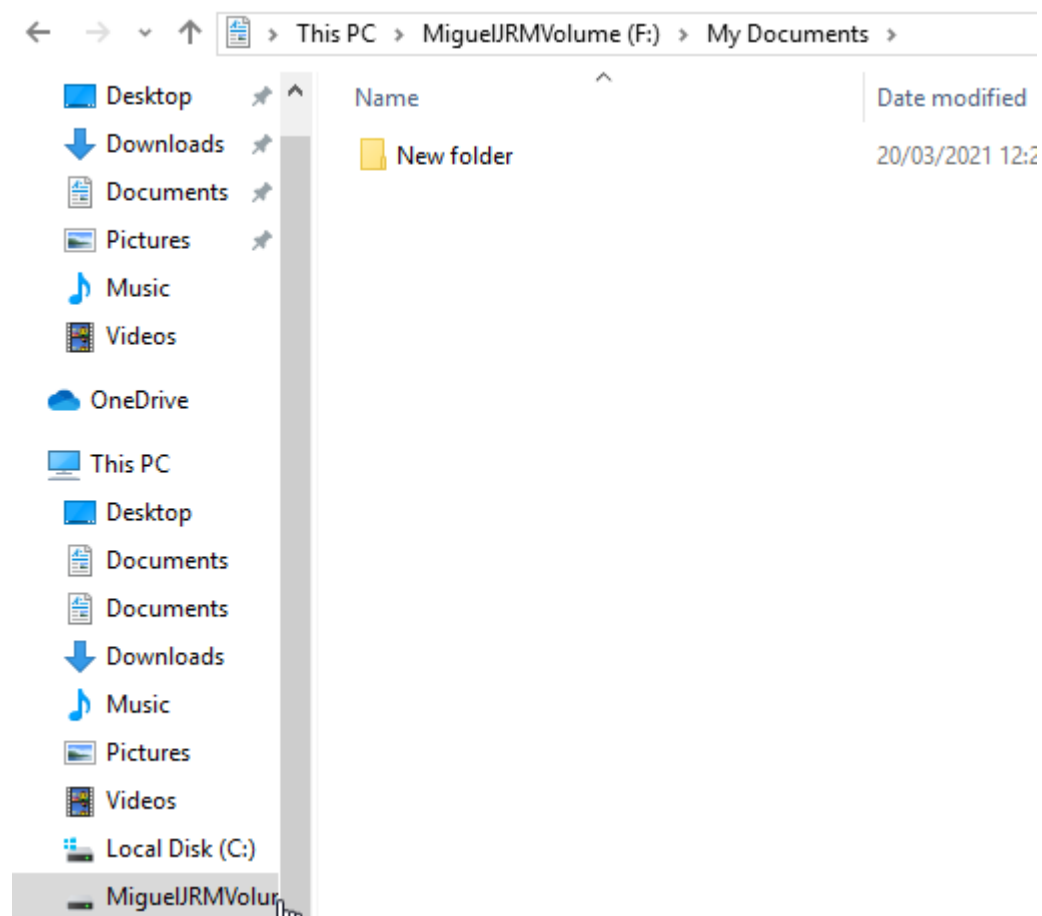> This PC > MiguelJRMVolume (F:) >

Name

📄 My Documents

2.6

We create the folder inside the Documents shorcut

Checking that the folder has been created

3.

We need to set up some configurations in order to achieve this

First in the Local Security Policy we need to set up this config.

Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled

Then we have to change the password from the user, using the same method as the first exercice
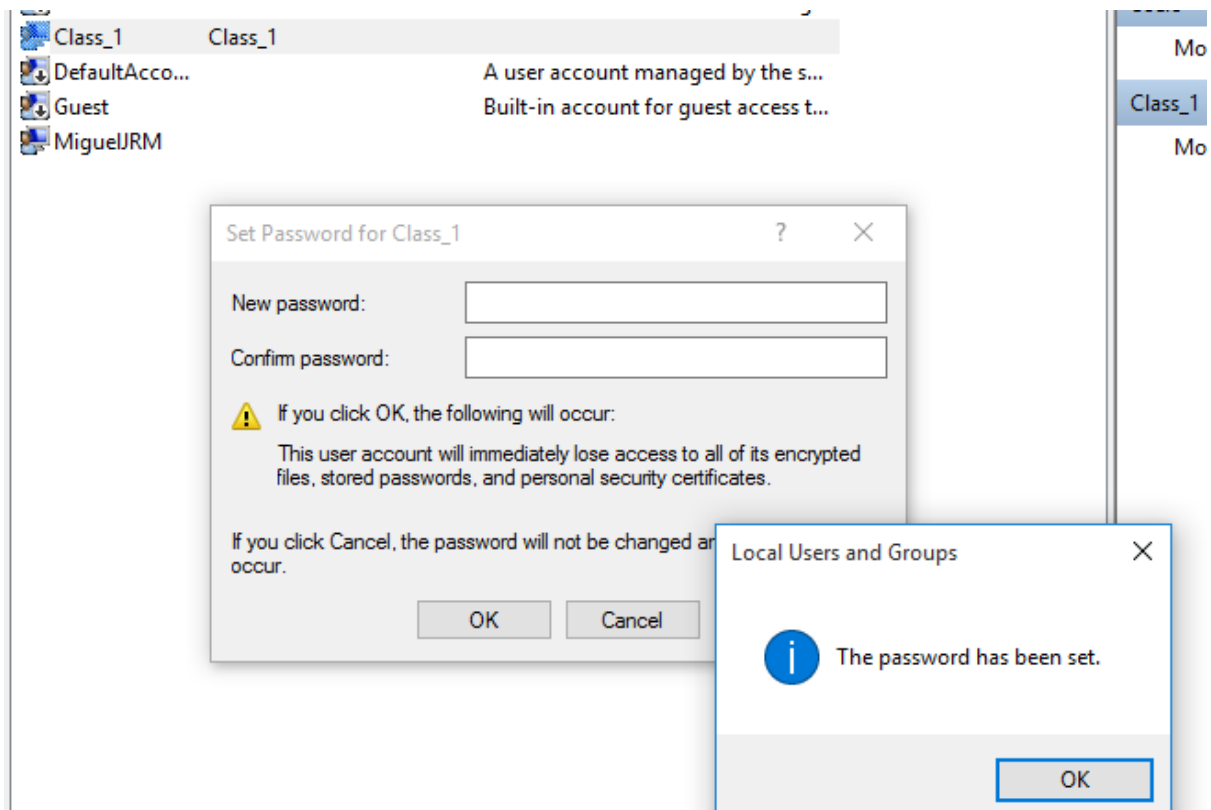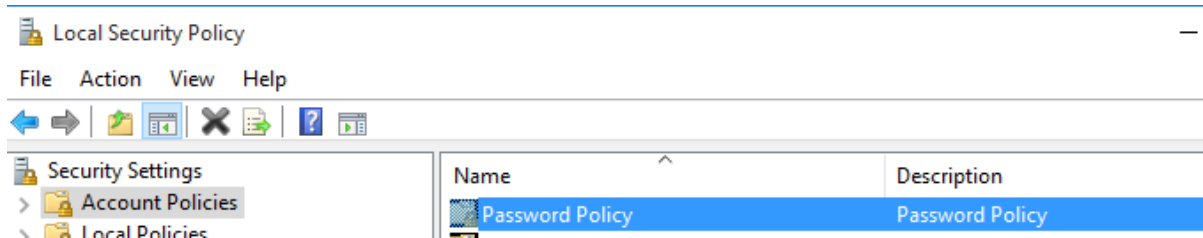
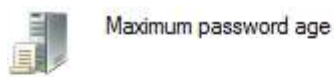We run the netplwiz tool in order to enable the automatic logon
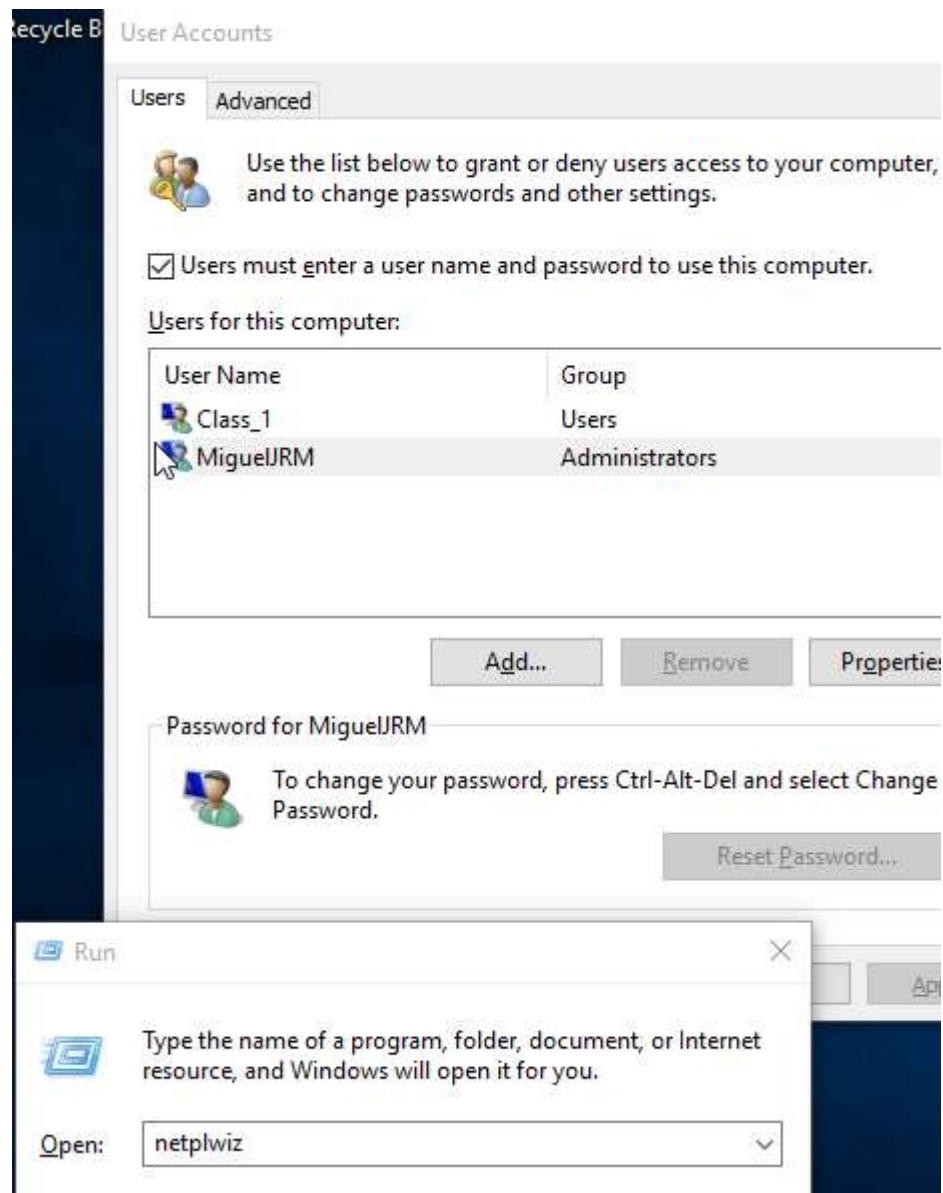
4.

In local security policies we have to go to Account policies and then to Password policy
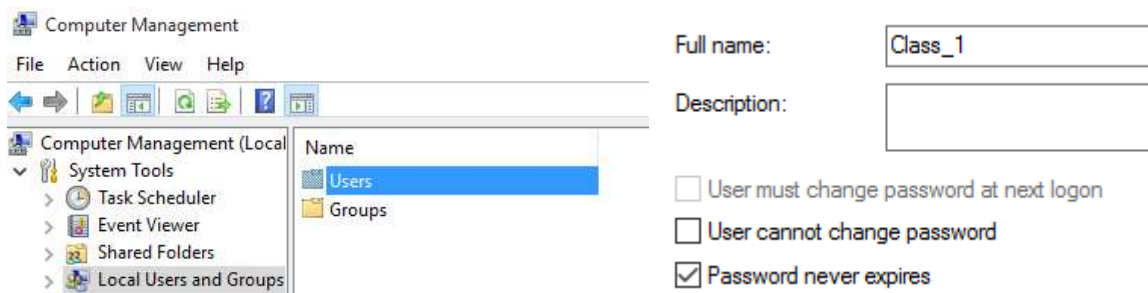

Finally set the Maximum password age to 0

If you want this set up but only for an specific user, yo have to go to Computer management>Local users and groups>users and then rigth click and go to properties for the user you want.

5.

After the lockout duration or the administrator unlock the user account via computer managment or using the command line as administrator.

6.

Reset account lockout counter after must be less or equal to "Account lockout duration".

If "Account lockout threshold" were 0, you would not be able to set the other policies, as you cannot lock a password.

7.

All this policies can be done in the same tab of the local security policies
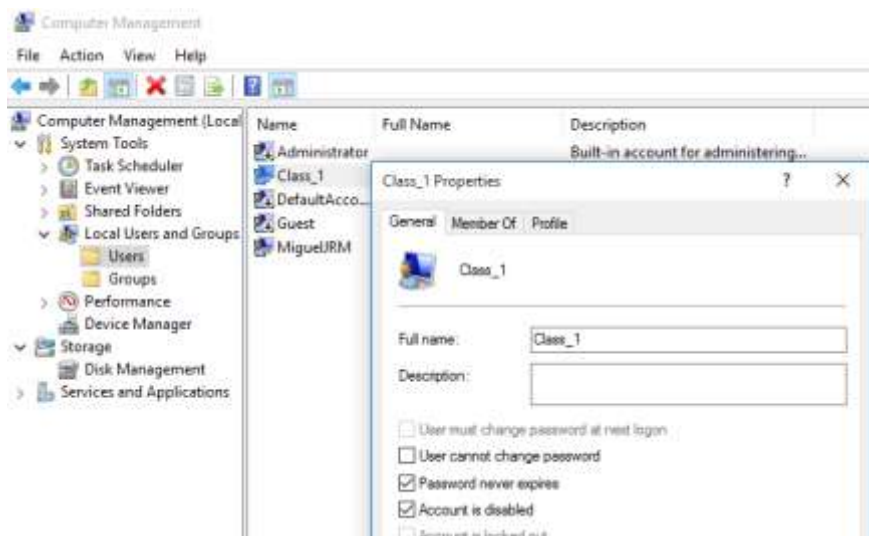
Go to account policies and then to password policy

8.

8.1

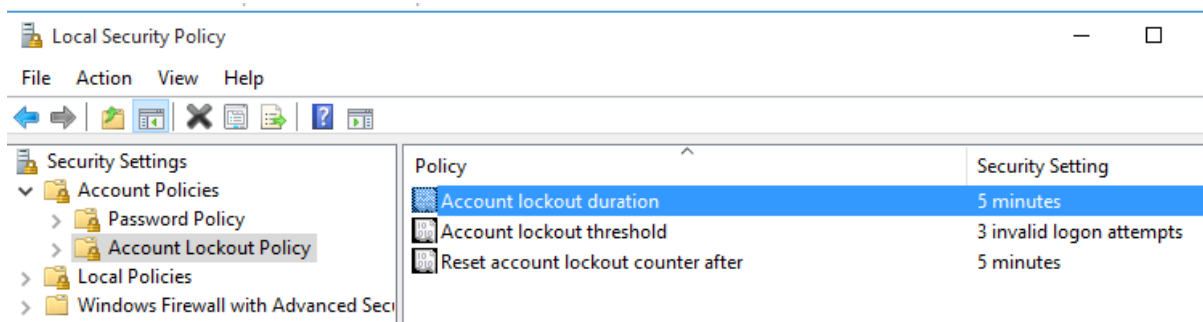We disable the account in Computer management

Or via cmd

8.2

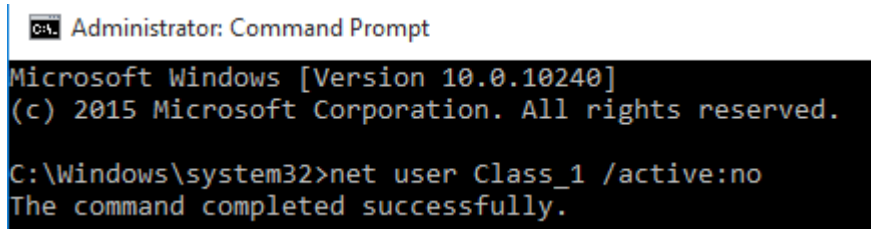Unlock the user with the administrator and the try to log in

8.3

Setting up the Account lockout threshold and the reset account lockout counter after

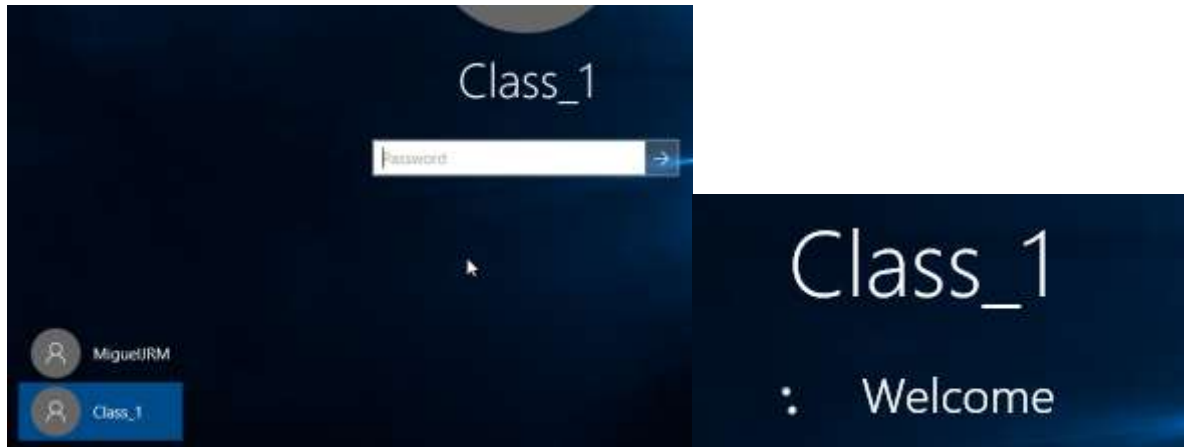This policies are inside the local security policy
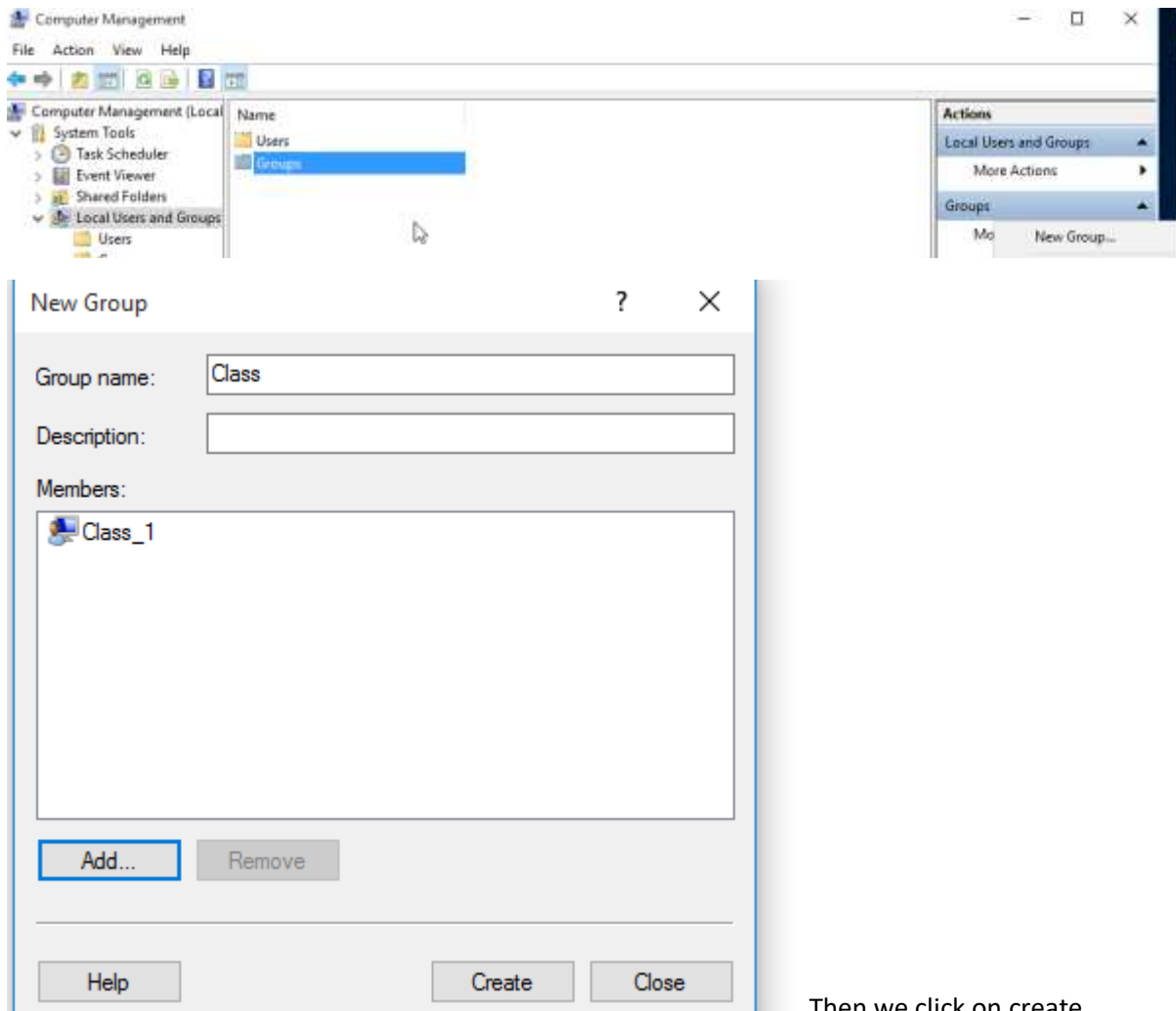

Then lock the user using cmd

8.5

After 5 minutes the user account is accessible

9.

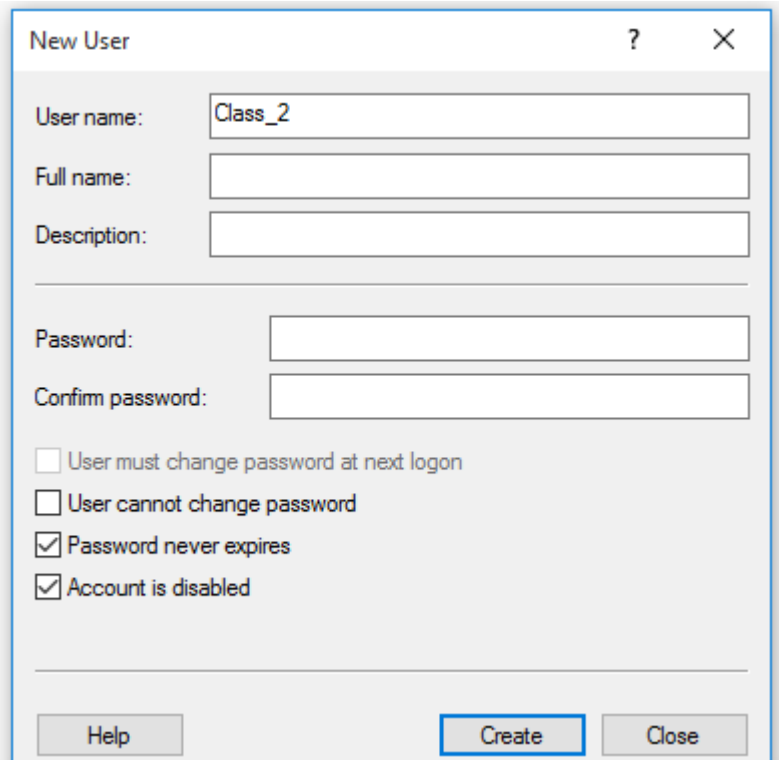We go to computer management and inside groups we click in more actions, then new group

 Then we click on create

Now we create the user Class_2 initially disabled

New User

User name: Class_2

Full name:

Description:

Password:

Confirm password:

☐ User must change password at next logon
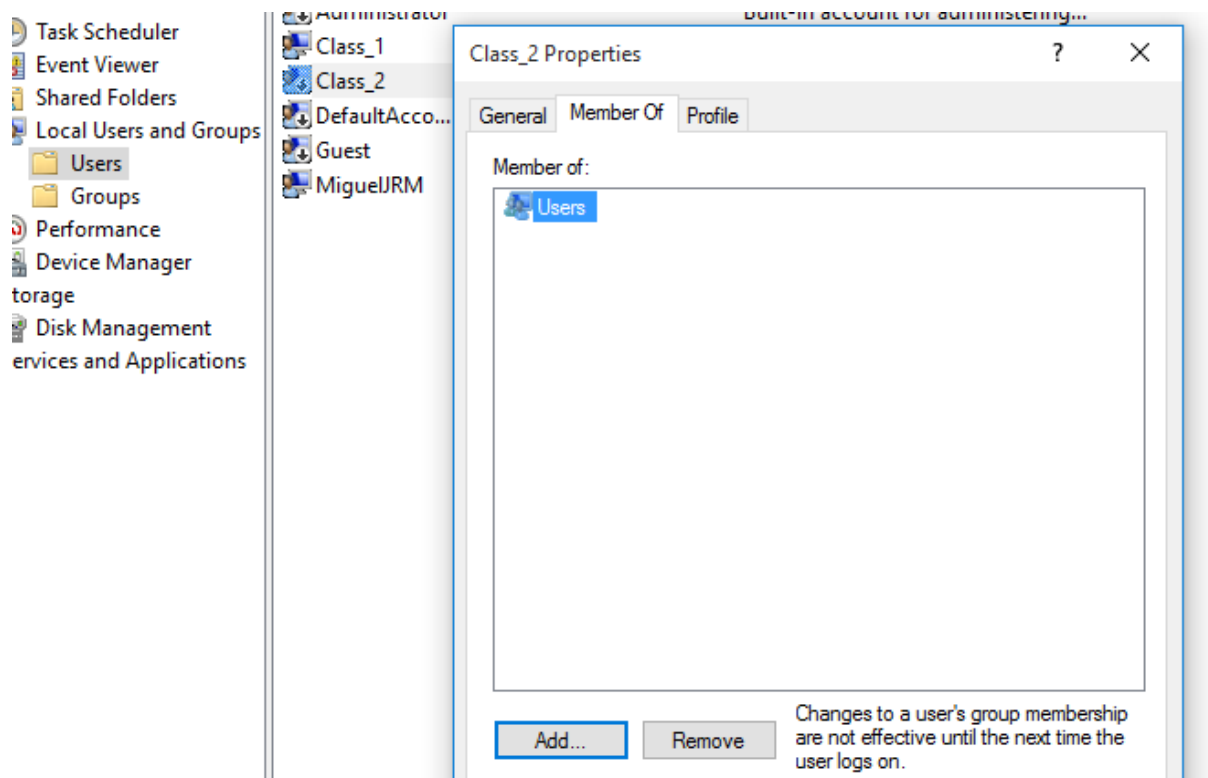☐ User cannot change password
☑ Password never expires
☑ Account is disabled

Help   Create   Close

First remove this user from Users group

Then we add the user to the Class group
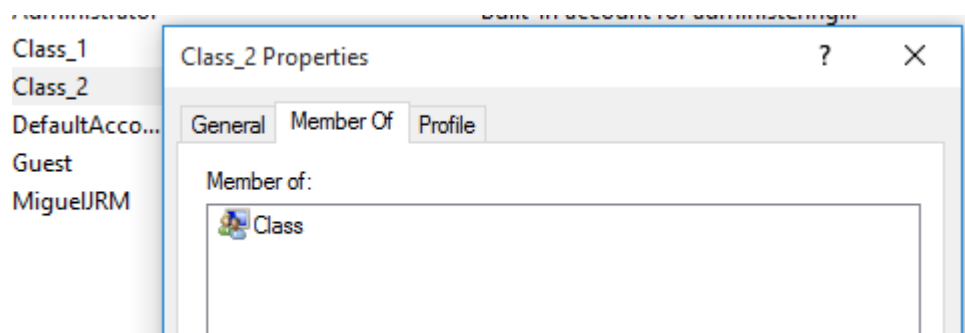
10.

As the users are in the same group, we open the local security policy and go to user rights assignment and then adding the class group in the Chamge system time policy.

Object Types

Select the types of objects you want to find.

Object types:

- ☑ Other objects
- ☑ Built-in security principals
- ☑ Groups
- ☑ Users

Local Security Setting   Explain

Change the system time

Administrators
DESKTOP-PS5VH0V\Class
LOCAL SERVICE
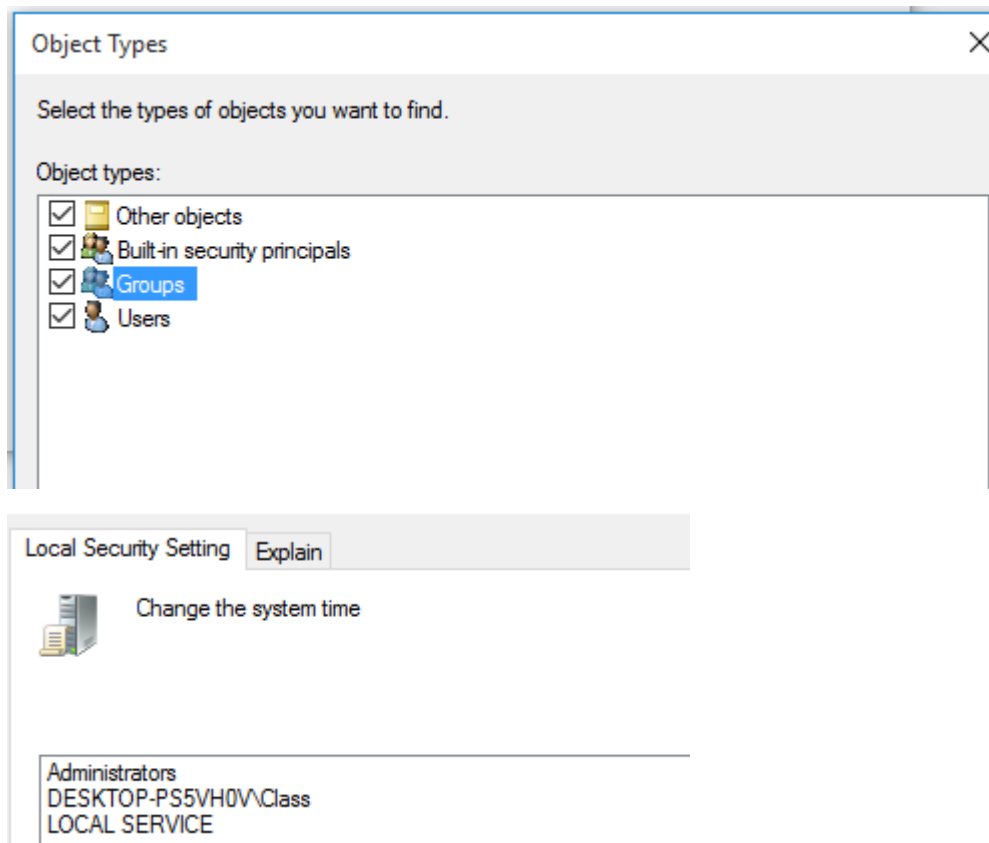
11.

In the same tab as the previous exercice, now we look for the Shut down the system policy and remove all users except the administrator

Shut down the system
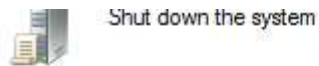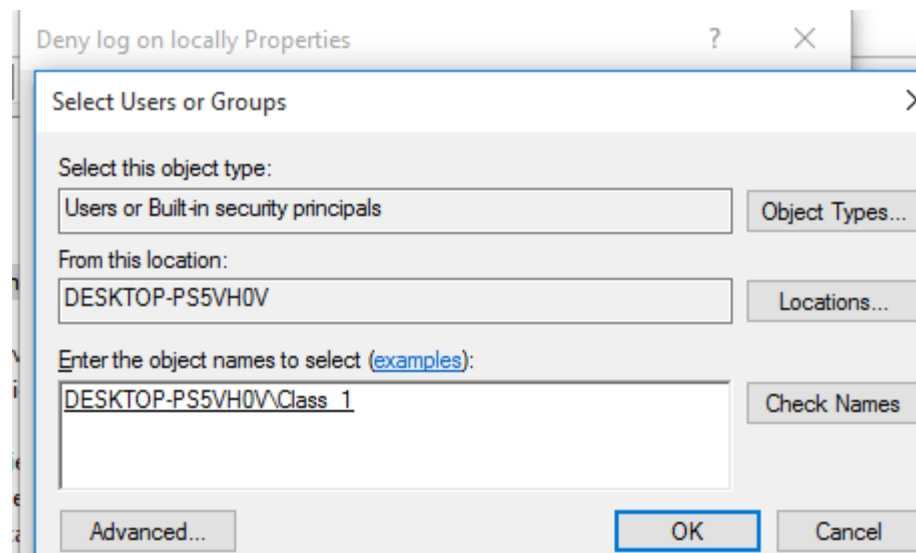
Administrators

12.

Allocated in the same tab as the previous exercice we look for Deny log on locally and we add Class_1 user.

Deny log on locally Properties   ?   ✕

Select Users or Groups   ✕

Select this object type:

| Users or Built-in security principals | Object Types... |

From this location:

| DESKTOP-PS5VH0V | Locations... |

Enter the object names to select (examples):

| DESKTOP-PS5VH0V\Class_1 | Check Names |

Advanced...   OK   Cancel

13.

First we check that the policies are the same as it supposed to be in the exercice 7

Enforce password history	10 passwords remember...
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled

Then, we create the user

Click on remove and ok

Now the user doesn't appear in the log in screen as it doesn't belong to any group that have the privileges to log on in the system