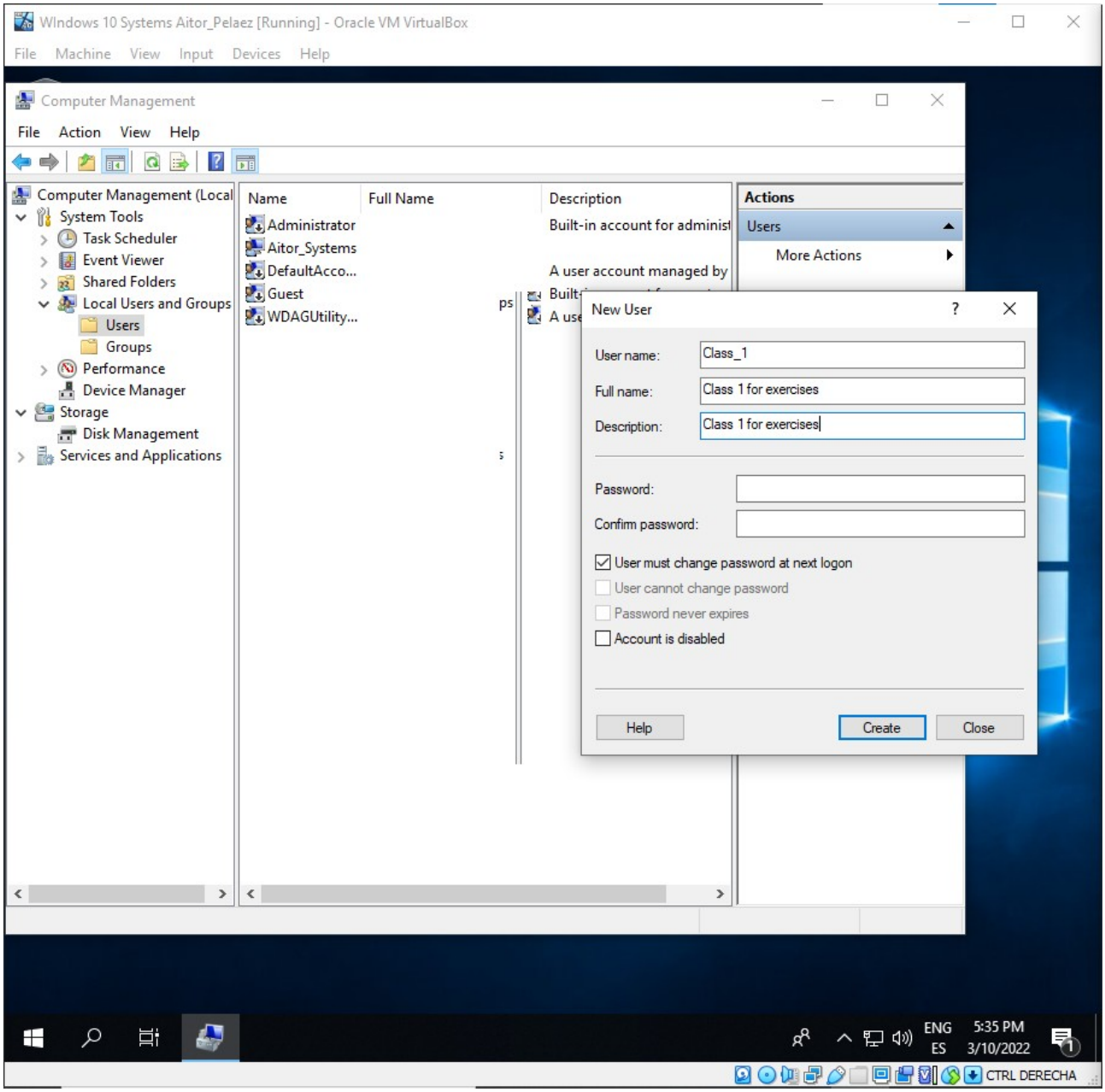
Aitor Pelaez

Users, groups and local policies

1. Add a new standard user named “Class_1” including the description and full name.

The user must change the password at next logon.



2. Complete the following parts about the user “Class_1” from the previous exercise.

• Verify if the profile folder exists.

Aitor Pelaez

• Log in as “Class_1”.

• Verify if the profile folder now exists.

• Add a second hard drive to the virtual machine and create a folder called

“My Documents” in F:\

• Move “Class_1” Documents folder to the directory you have just created.

• Open “Documents” shortcut and create a new folder. Check if this folder has

actually been created in “F:\My Documents”.

3. How do you configure a user to log in without a password and automatically when

turning the computer on?

4. How do you configure a specific user so that the password never expires? How can

you configure this policy for everyone?

Local security policies -> Maximum password age = 0. This way, the password for every user will never expire.

5. When can you use a locked account?

After the lockout duration or the logon failed attempts are reset. The administrator is also able to unlock an account from computer management. The checkbox will be automatically enabled.

6. Imagine you define an “Account lockout threshold” of 3 and “Account lockout

duration” of 5. What would be the valid values of “Reset account lockout counter

after”? What if “Account lockout threshold” value were 0?

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

Aitor Pelaez

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

7. Configure the system according to the following criteria:

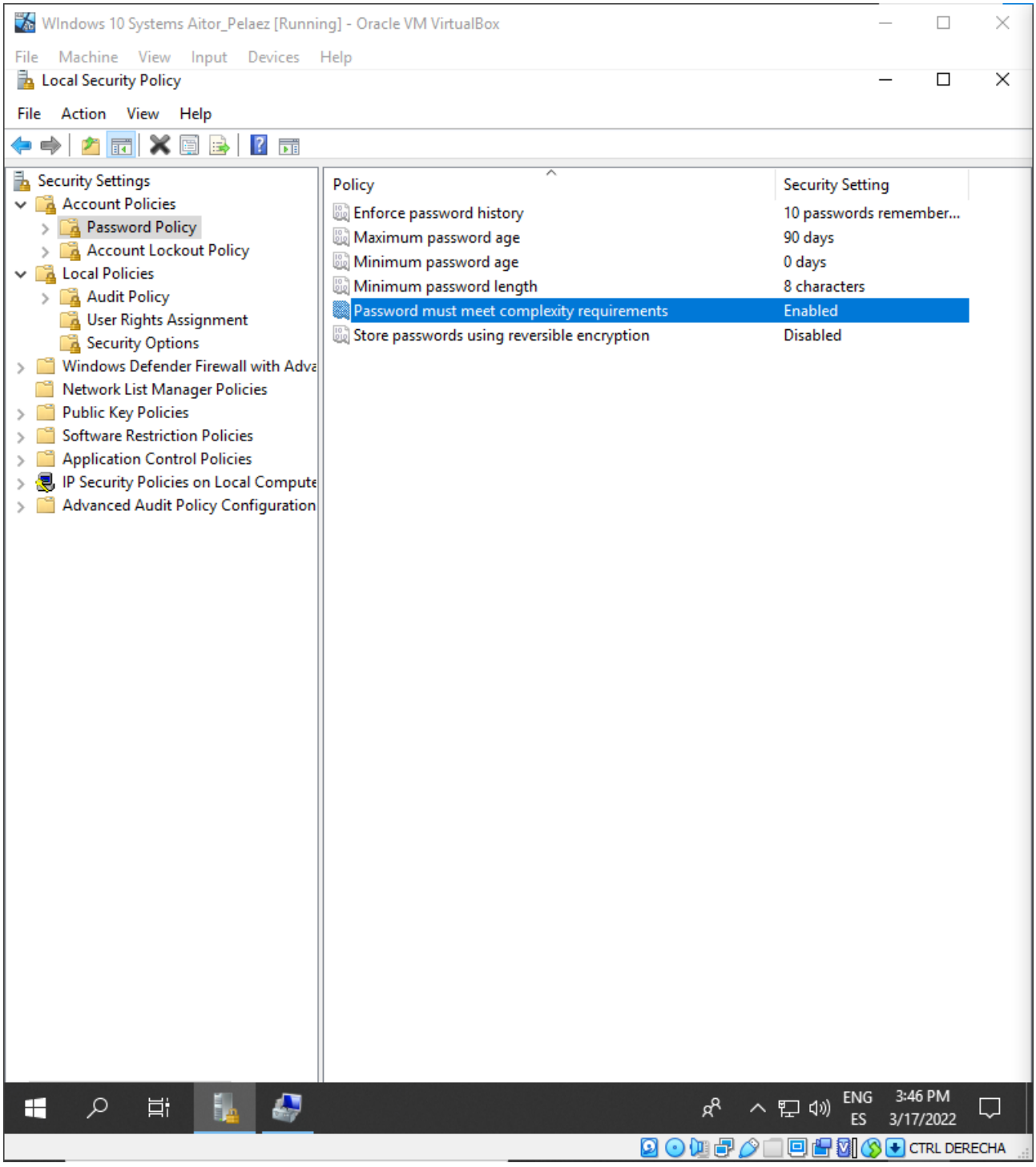
• All the passwords must have at least 8 characters.

• All the passwords must contain uppercase, lowercase, numbers and nonalphanumeric characters.

• The system stores the last 10 passwords for each user.

• All the passwords expire after 3 months.

Aitor Pelaez



8. Configure the user “Class_1” to be locked after 3 invalid logon attempts. If the user is locked out, it will be able to type the password again in 5 minutes. Complete the following steps:

• Lock the user.

• Unlock the user as administrator and check if the user is able to log in.

• Lock the user again.

Aitor Pelaez

• Wait for 5 minutes.

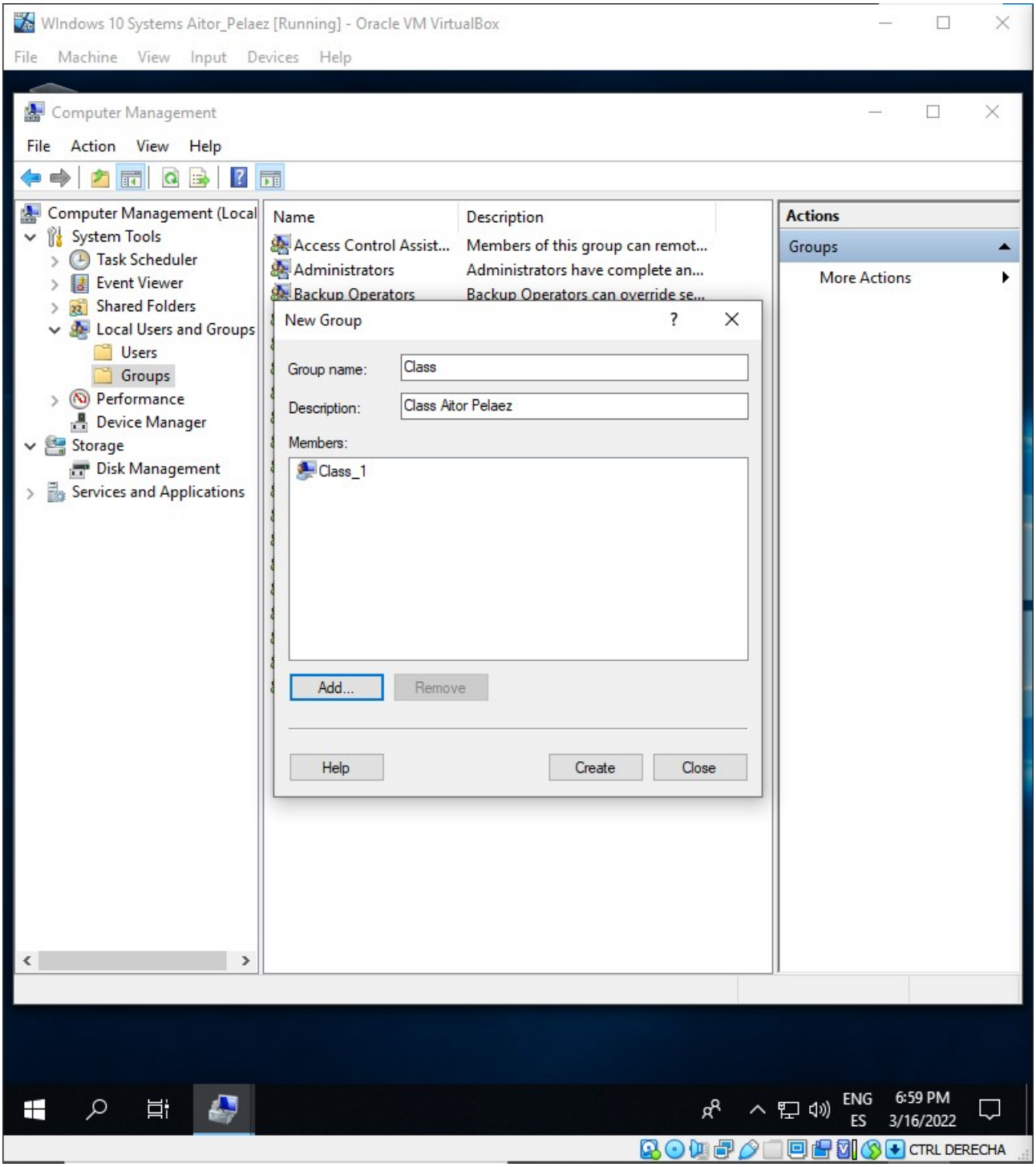
• Type the right password and check if the user is able to log in.

9. Add a new group name “Class” and complete the following:

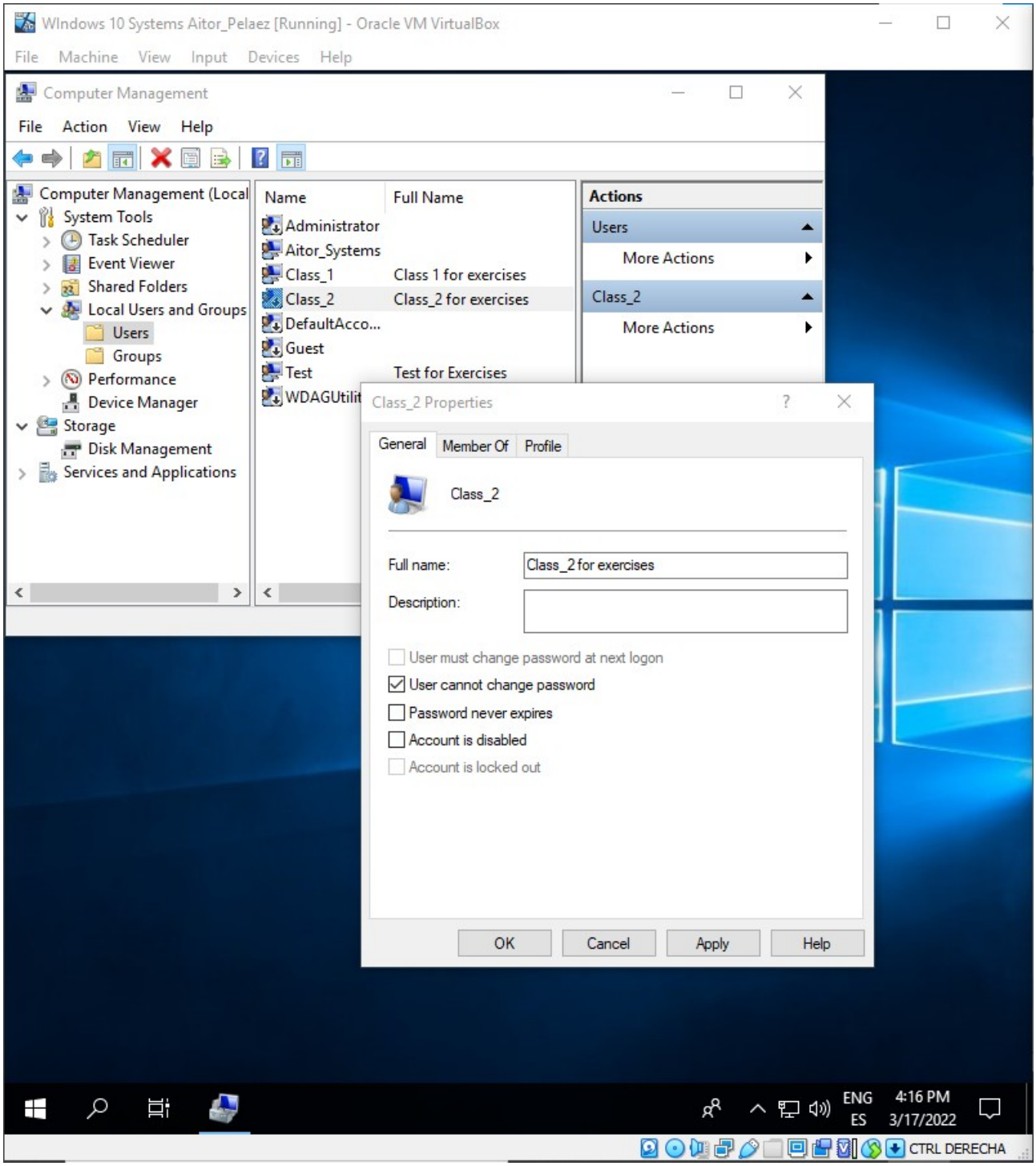
• Add the user “Class_1” to the group “Class”.

• Create a guest user called “Class_2”, initially disabled that cannot change the password. Then, add the user to “Class”.

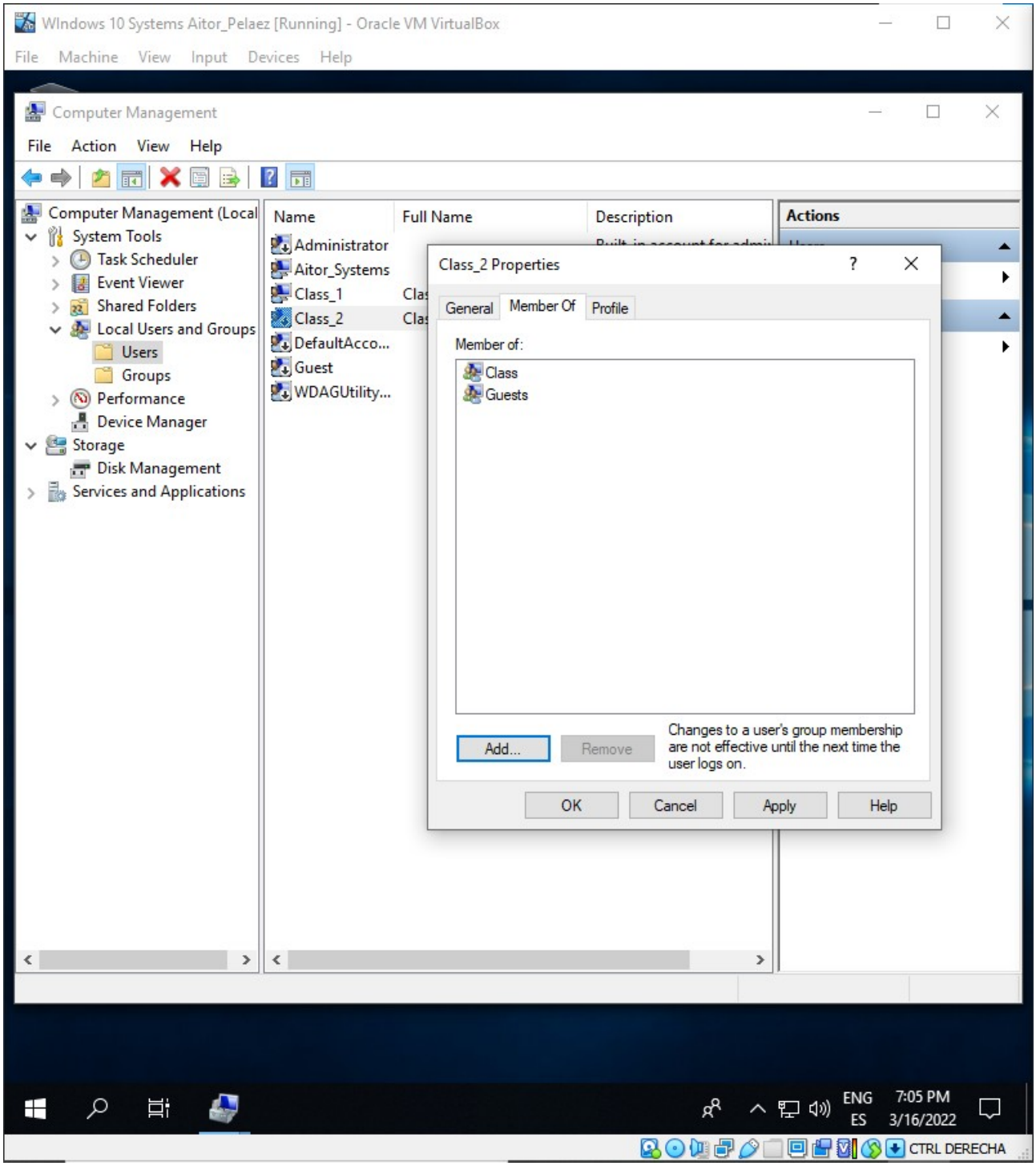
Aitor Pelaez



Aitor Pelaez

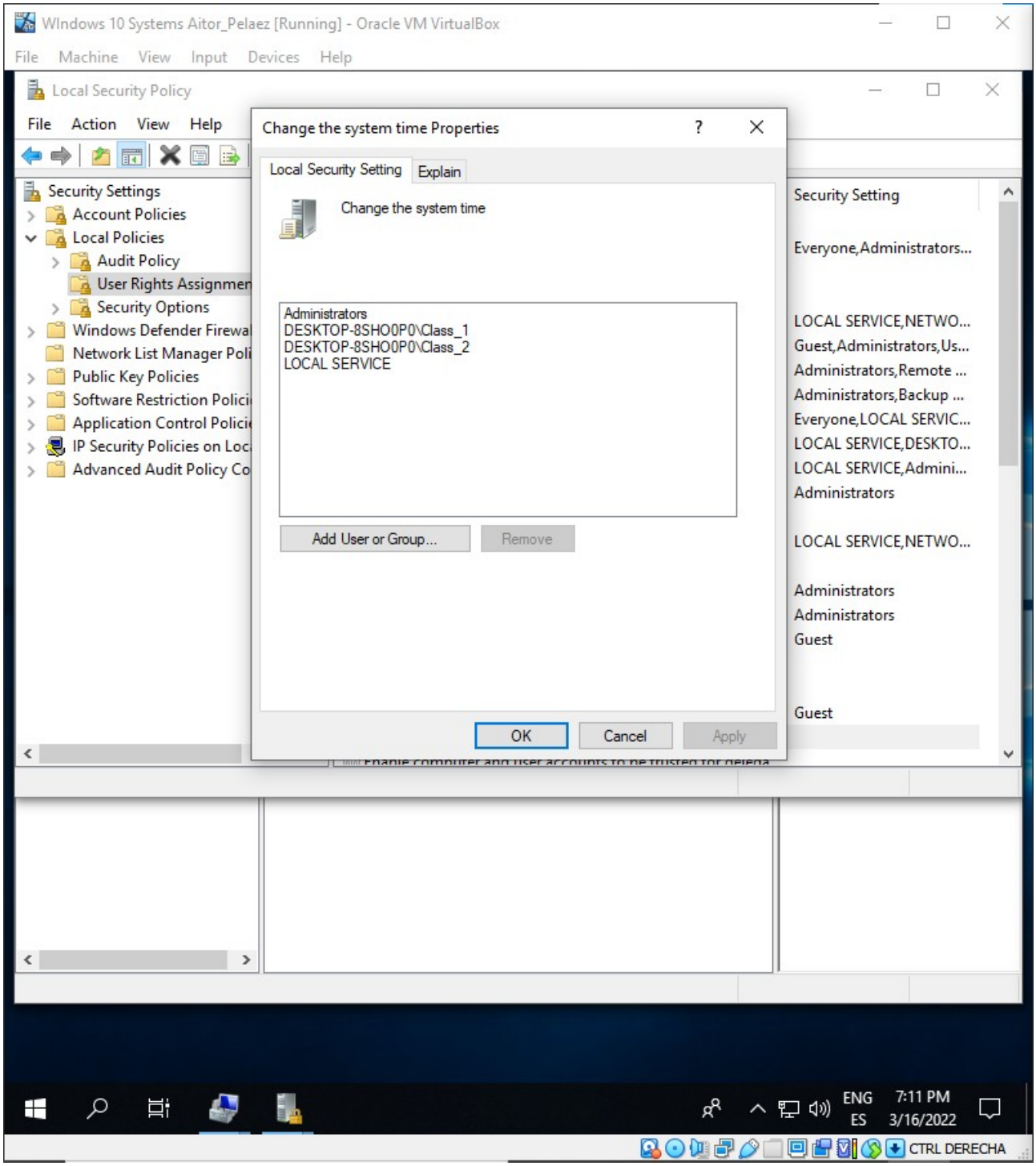


Aitor Pelaez



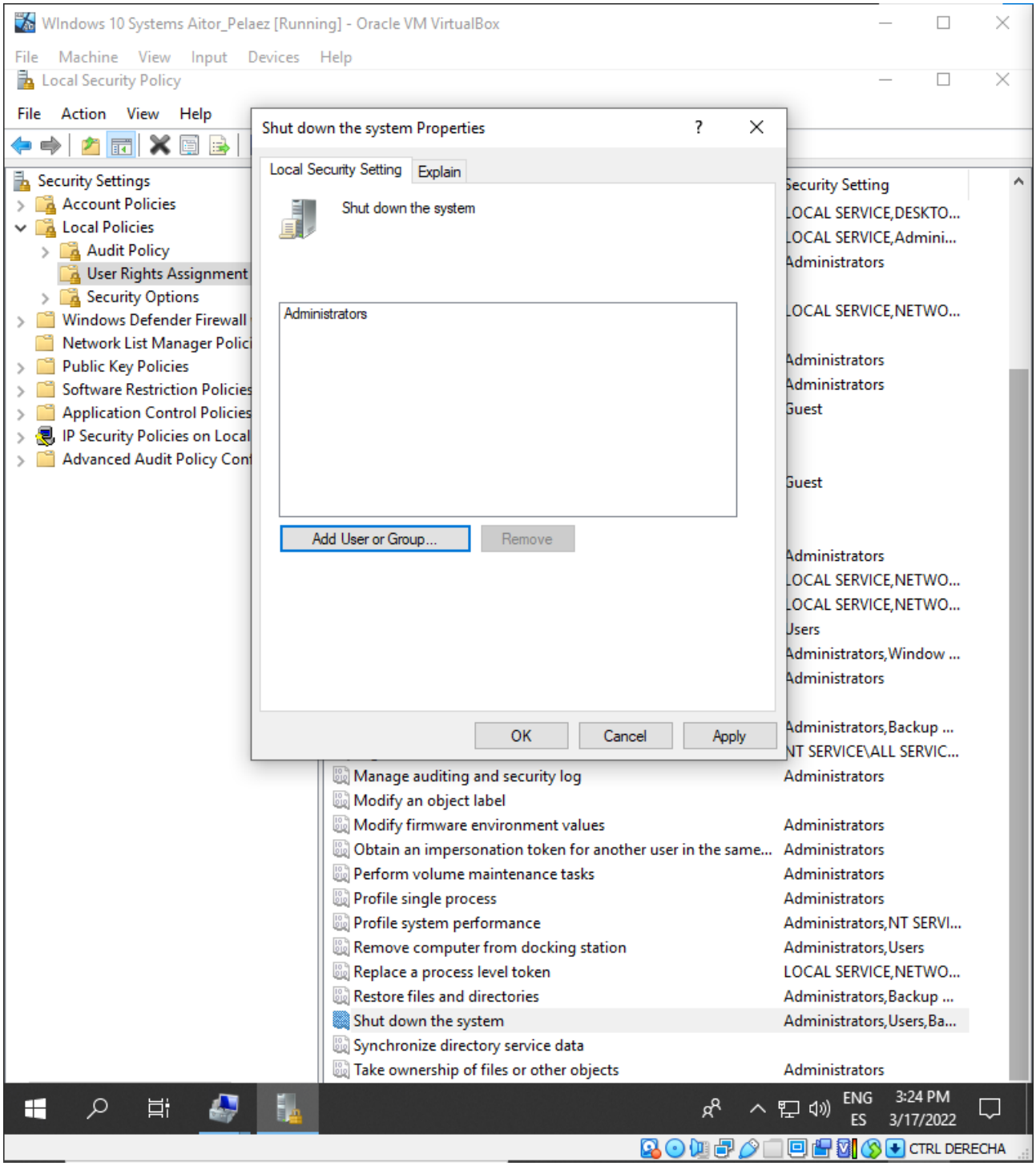
10. Modify the user rights so “Class_1” and “Class_2” will be able to “Change the system time”.

Aitor Pelaez



11. Modify the user rights so that only the administrator users can “Shut down the system”

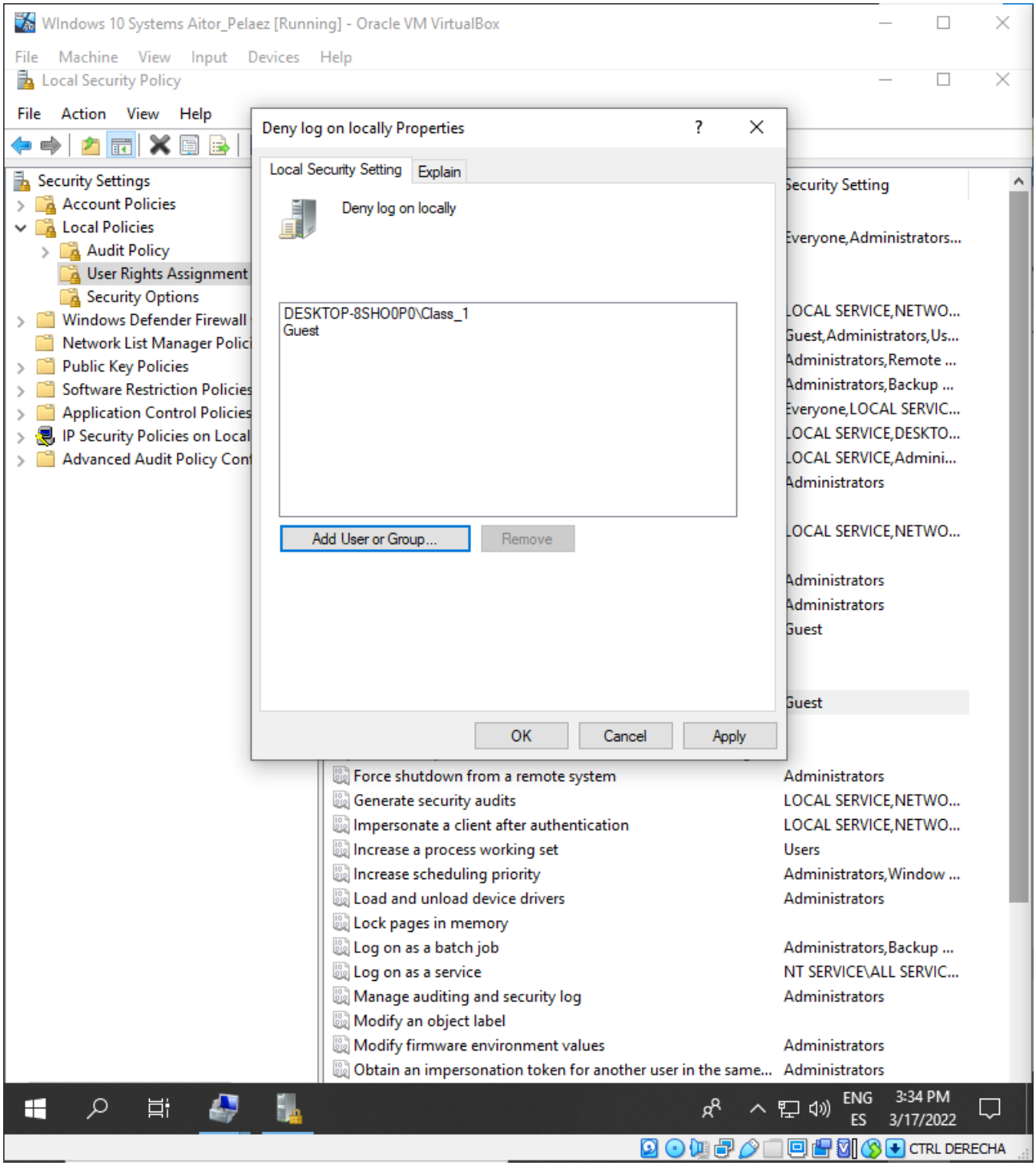
Aitor Pelaez



12. Suppose all the standard users are able to log in. How can we deny log on to the specific user “Class_1”?

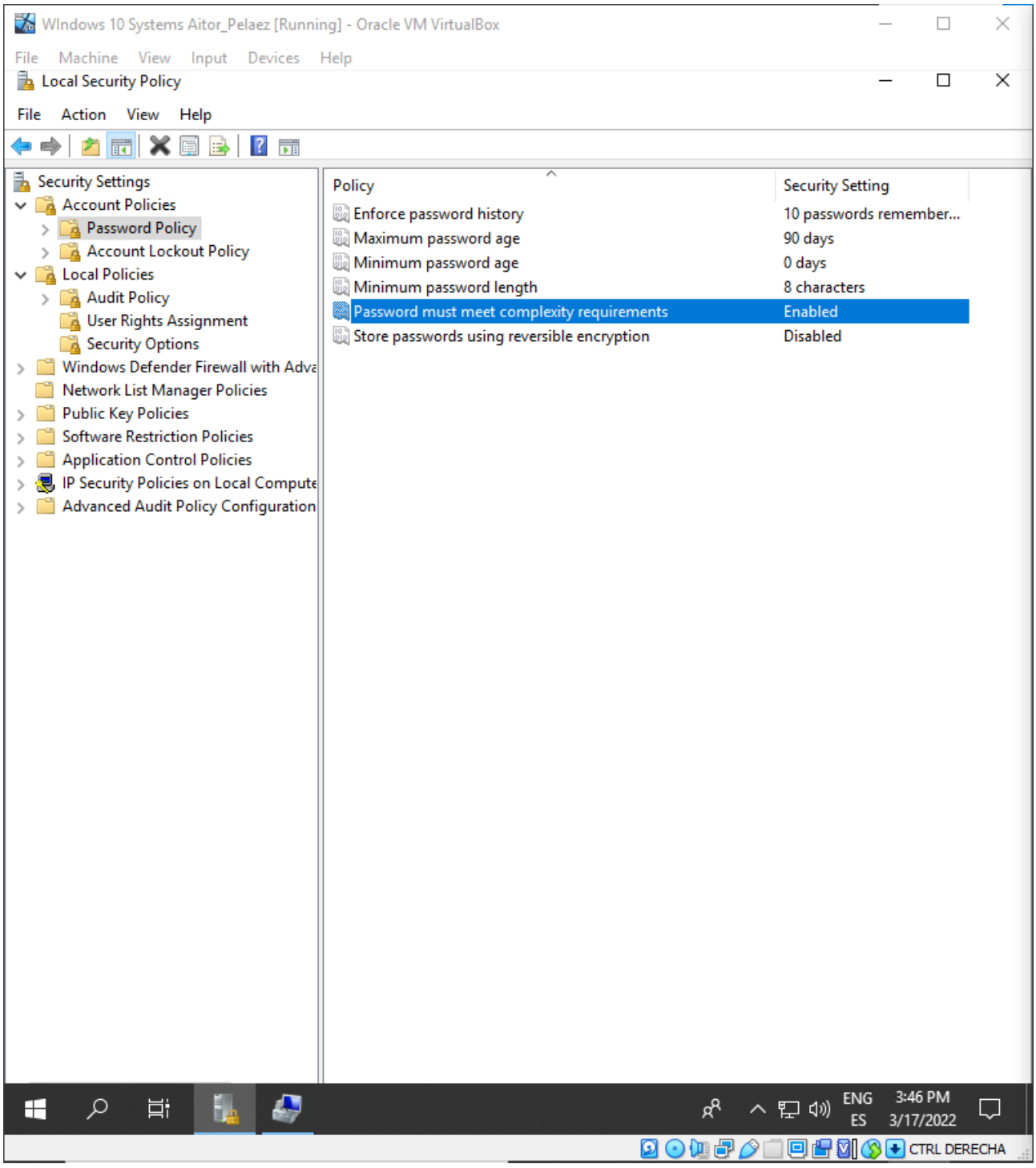
You can deny the log on by configuring it in the Local Security Policy and in the option “Deny log on locally”

Aitor Pelaez

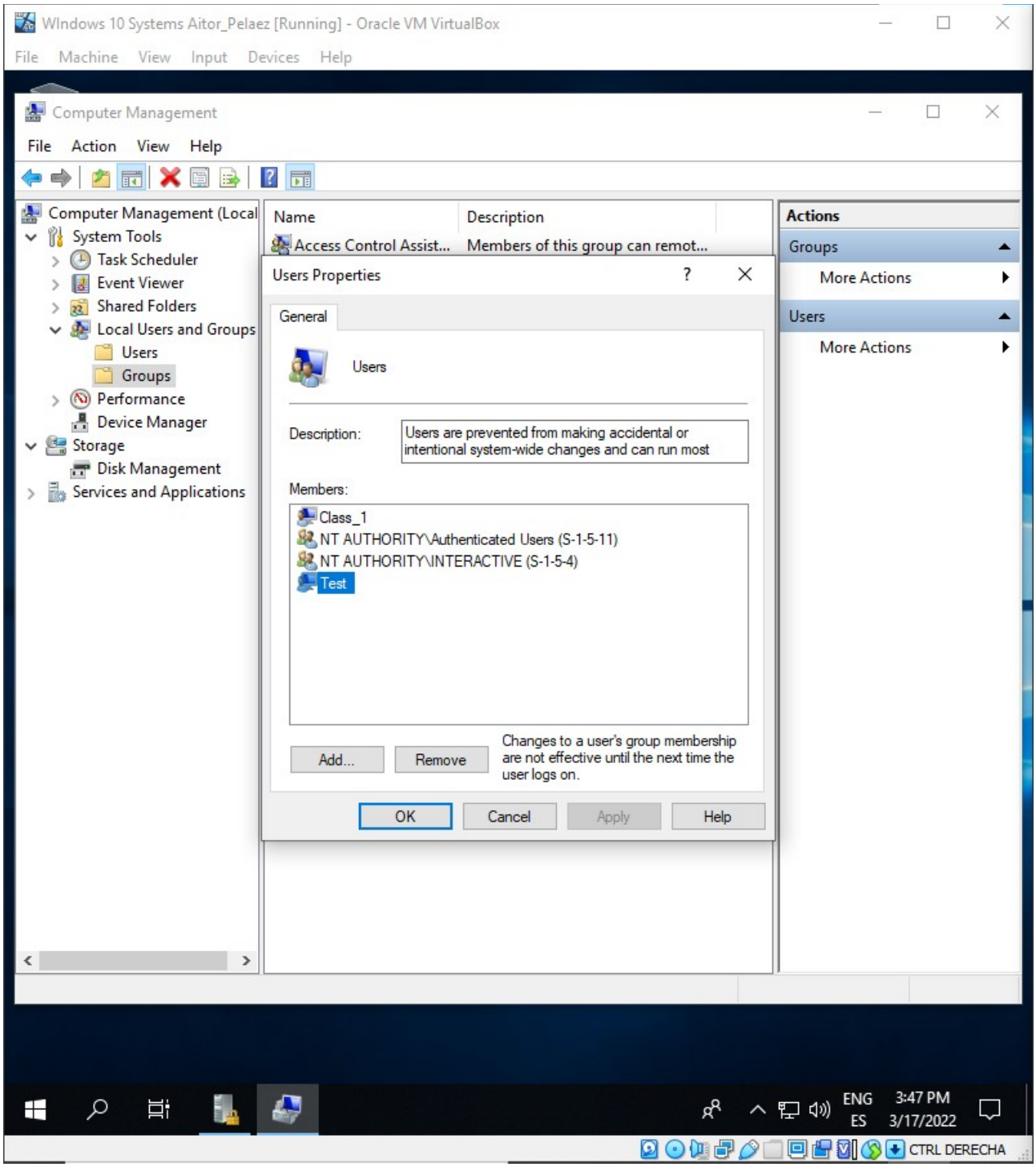


13. Overall, add a new user called “Test” according to the requirements in exercise 7. What if we deleted “Test” from the group “Users”? Try to log in and explain what happens.

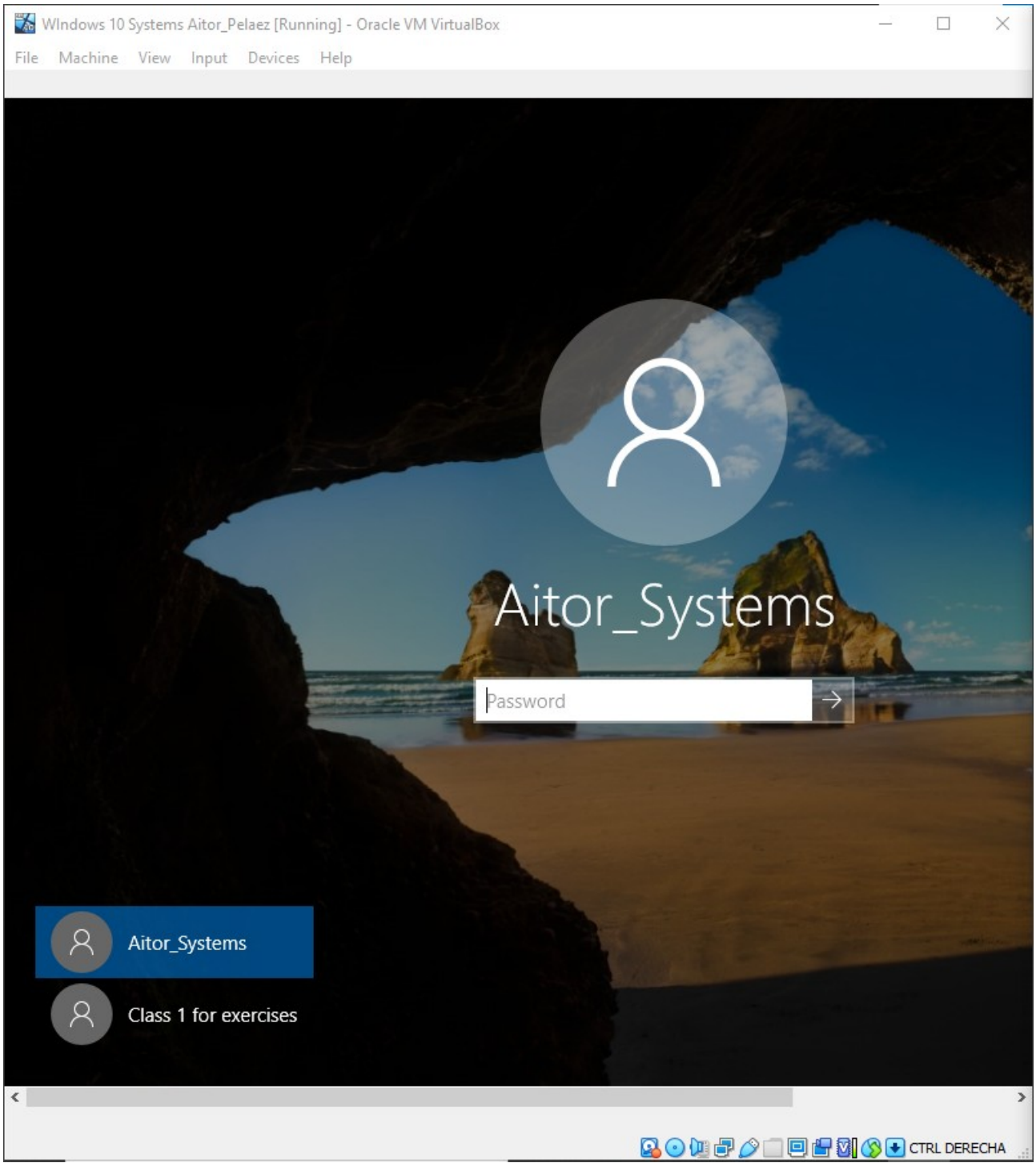
Aitor Pelaez



Aitor Pelaez



Aitor Pelaez



The user Test doesnt appear to log in with. Is beacause we erraised from the group users, so is not a user.