9.2 - Setting Up Users, Groups, and Policies

3 - Setting Up Users, Groups, and Policies.

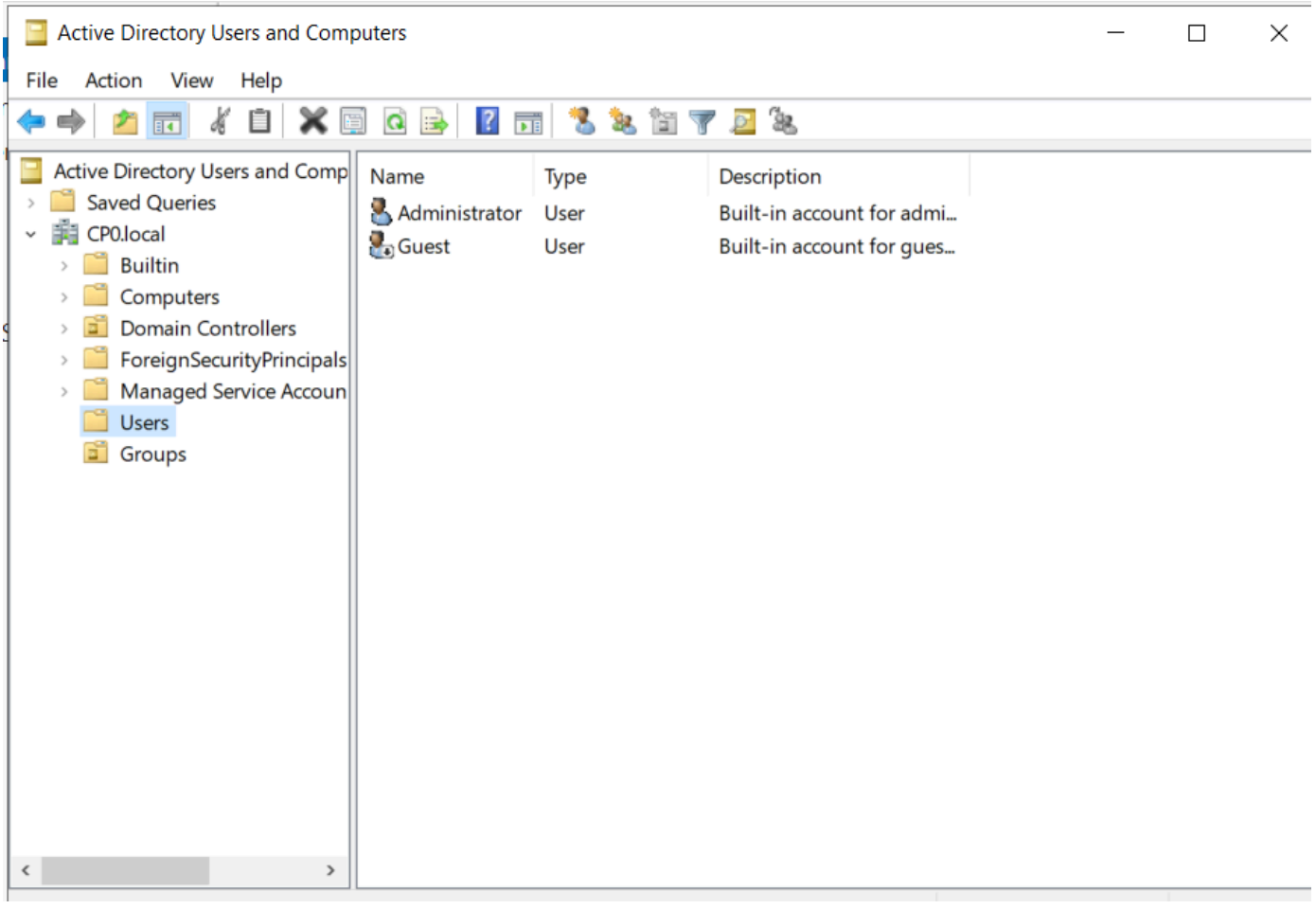
Here, we are going to use the DC. Which is the Windows Server.

Server Manager > Tools > Active Directory Users and Computers.

It stores all users and computers. OUs (Organizational Units for the Active Directory).

To make it more organized, we are going to separate the users from the groups. For that purpose, we are going to create a new organizational unit to move the groups to that "folder"(which is actually an OU). So, open the local domain, right click it > New > Organizational Unit > We are going to name it "Groups".

Now, go to the "Users" OU ("folder"), and move all the groups to the new OU. We should have left only the Administrator, and Guest account left.



We are going to create a new Administrator account.

Lets just copy the Built-in Administrator.

Right-click it > Copy.

That is a shortcut to copy all the privileges of the Administrator account.

To check Admin privileges, right-click admin built-in account > Member Of > And you should be able to see the Groups the account is associated.

This is going to be the Domain Administrator:

Name: Usopp

Last: Sogeking

User Logon Name: USogeking@ONEPIECE.local

(Pre - Windows 2000): ONEPIECE/USogeking

Password : Password12345!

Select the "Password never expires" box (which is not a good idea in a real live environment).

Now, we are going to do another big no-no, which is create a Service Account that is a Domain Administrator.

Services account are used to run a service.

Copy the built-in Admin again.

name : SQL ; last: : Service

User Logon Name : SQLService@ONEPIECE.local

Password: MYpassword123#

Select the "Password never expires" box (which is not a good idea in a real live environment).

Then, we are going to right-click the new account > properties > in the Description field we are going to put the password for the account, which is another big no-no.

Next, we are going to create 2 regular users. Regular meaning low level users.

Right-click "Users" OU > New > Users.

Here, we are going to create the user accounts in the Active Directory. So far, the accounts created were in the local computer, but now they are going to be created in the Active Directory. Meaning, all computer joined to the domain are going to be available for those users to login. Just like in a University where you can login to many different computers with one single credential.

User 1 : Luffy Monkey, LMonkey@ONEPIECE.local, Password1 .

Select the "Password never expires" box (which is not a good idea in a real live environment).

User 2 : Zoro Roronoa, ZRoronoa@ONEPIECE.local, Password2 .

Select the "Password never expires" box (which is not a good idea in a real live environment).

Next thing, we are going to create a file share.

Server Manager > File and Storage Service (on the left Menu Bar) > Shares > TASKS > New Share > Select "SMB Share - Quick" > Next > Share name: hackme > Accept Default for all the rest > Create.

Next, We are going to finish setting up Service Account.

Run CMD as Admin > Then, run "#setspn -a GoingMerry-DC/SQLService.ONEPIECE.local:60111 ONEPIECE\SQLService"

So, Domain Controller PC name (GoingMerry-DC), and then Domain name (ONEPIECE.local).

To make sure the system took the command and in fact updated object, we can run:

" #setspn -T ONEPIECE.local -Q */* "

```
C:\Users\Administrator>setspn -a GoingMerry-DC/SQLService.ONEPIECE.local ONEPIECE\SQLService
Checking domain DC=ONEPIECE,DC=local

Registering ServicePrincipalNames for CN=SQL Service,CN=Users,DC=ONEPIECE,DC=local
        GoingMerry-DC/SQLService.ONEPIECE.local
Updated object

C:\Users\Administrator>setspn -T ONEPIECE.local -Q */*
Checking domain DC=ONEPIECE,DC=local
CN=GOINGMERRY-DC,OU=Domain Controllers,DC=ONEPIECE,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/GoingMerry-DC.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/ForestDnsZones.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/DomainDnsZones.ONEPIECE.local
        DNS/GoingMerry-DC.ONEPIECE.local
        GC/GoingMerry-DC.ONEPIECE.local/ONEPIECE.local
        RestrictedKrbHost/GoingMerry-DC.ONEPIECE.local
        RestrictedKrbHost/GOINGMERRY-DC
        RPC/4b263b8a-6a51-45f6-b6ad-ef58442d540e._msdcs.ONEPIECE.local
        HOST/GOINGMERRY-DC/ONEPIECE
        HOST/GoingMerry-DC.ONEPIECE.local/ONEPIECE
        HOST/GOINGMERRY-DC
        HOST/GoingMerry-DC.ONEPIECE.local
        HOST/GoingMerry-DC.ONEPIECE.local/ONEPIECE.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/4b263b8a-6a51-45f6-b6ad-ef58442d540e/ONEPIECE.local
        ldap/GOINGMERRY-DC/ONEPIECE
        ldap/4b263b8a-6a51-45f6-b6ad-ef58442d540e._msdcs.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/ONEPIECE
        ldap/GOINGMERRY-DC
        ldap/GoingMerry-DC.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/ONEPIECE.local
CN=krbtgt,CN=Users,DC=ONEPIECE,DC=local
        kadmin/changepw
CN=SQL Service,CN=Users,DC=ONEPIECE,DC=local
        GoingMerry-DC/SQLService.ONEPIECE.local

Existing SPN found!

C:\Users\Administrator>
```

Now, we are going to set up Group Policy. For that we will need to open Group Policy Management. We can find it by searching it on the Windows search box.

Group Policy Management > Expand Forest > Expand Domains > Right-Click "ONEPIECE.local" > "Create GPO in this Domain, and ...." > We are going to name it "Disable Windows Defender" > Disable Windows Defender.

This will create a GPO (Group Policy Object?) for the whole domain. It is possible to create GPOs for specific users, groups, and/or computers. But, this wont be the case here.

The new Policy should pop up under the ONEPIECE.local > Right-Click it > Edit > Expand "Policies" under "Computer Configuration" > Expand "Administrative Templates" > "Windows Components" > Select "Microsoft Defender Antivirus" > Right-click or Double-Click "Turn Off Microsoft Defender Antivirus" > Edit > Enable > Apply > Save.

Go to Group Policy Management > Right-Click Policy just created > Select "Enforced".

What will happen is any time a user or computer joins the domain, it is going to get this policy. Or if the user or computer is already domain joined, then the policy is going to be enforced as soon as it updates and sink to the systems.

Lastly,

Go to windows search bar > Type "ncpa.cpl" > Right-Click Network > Double Click "Internet Protocol Version 4 ..." > We are going to use a static Ip address. Just set to the same one found on "#ipconfig" command in CMD (IP ADDRESS, Gateway, Subnet Mask) > Do not give an alternate DNS Server, and leave Preferred DNS Server to be 127.0.0.1 (localhost).