# Setting Up Users, Groups, and Policies

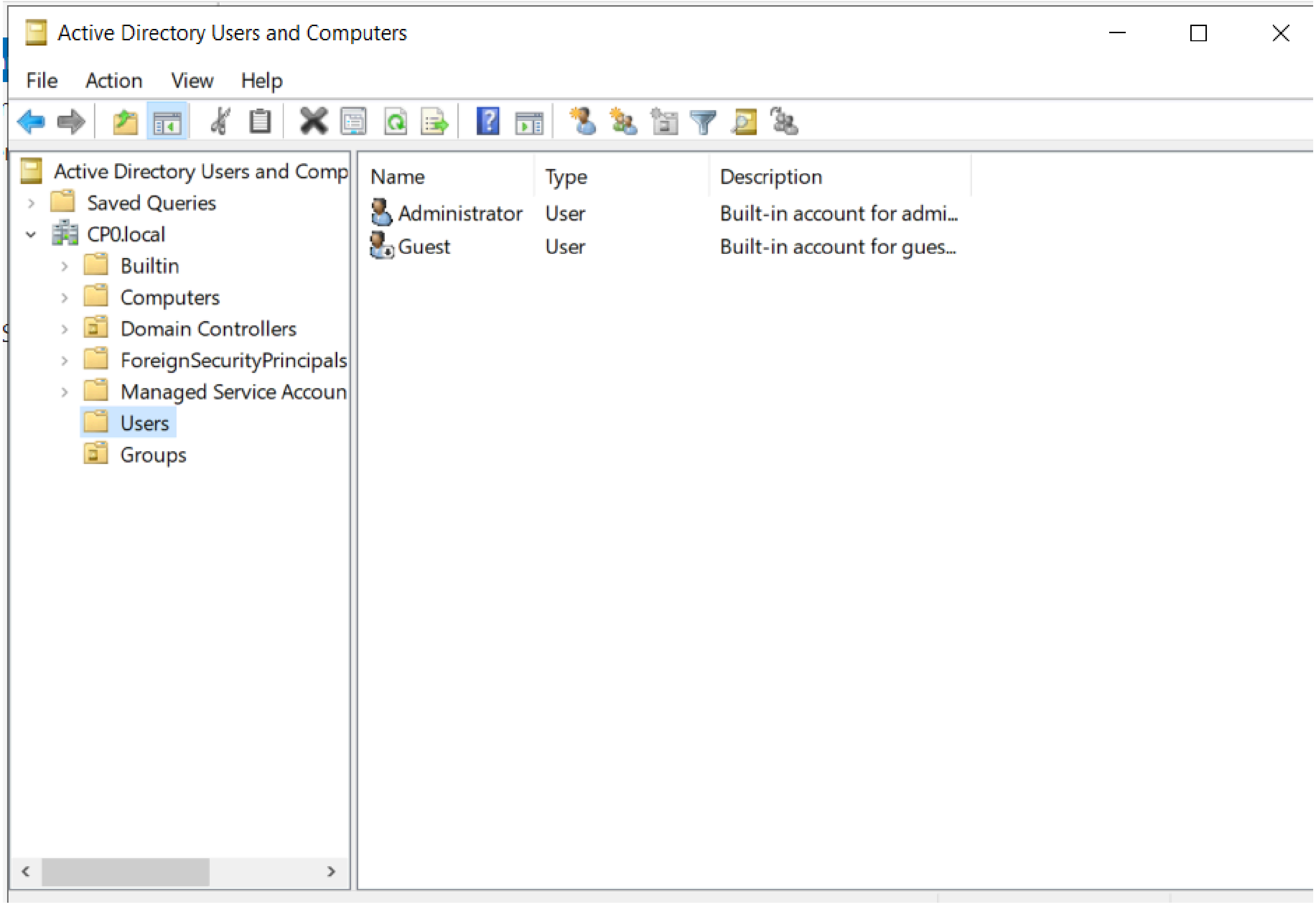
## 3 - Setting Up Users, Groups, and Policies.

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.

To make it more organized, we open the local, create new "Organizational Unit" called groups, go to the "Users" screen, and move all the groups to the new OU. We should have left only the Administrator, and Guest account left.



| Name | Type | Description |
|---|---|---|
| Administrator | User | Built-in account for admi... |
| Guest | User | Built-in account for gues... |

Lets create a new Administrator.

Lets just copy the Built-in.

Here, The User logon name is: kgunta@CP0.local

Last name: Gunta

First name: Kaku

Username: kgunta

Password: Password1234!

This will be the regular Administrator account.

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

The User Logon Name is : SQLService@CP0.local

Password: MYpassword123#

A low level user - User Logon Name is : kfunks@CP0.local

Password: Password1

Another low level user - bzion@CP0.local

Password: Password2

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

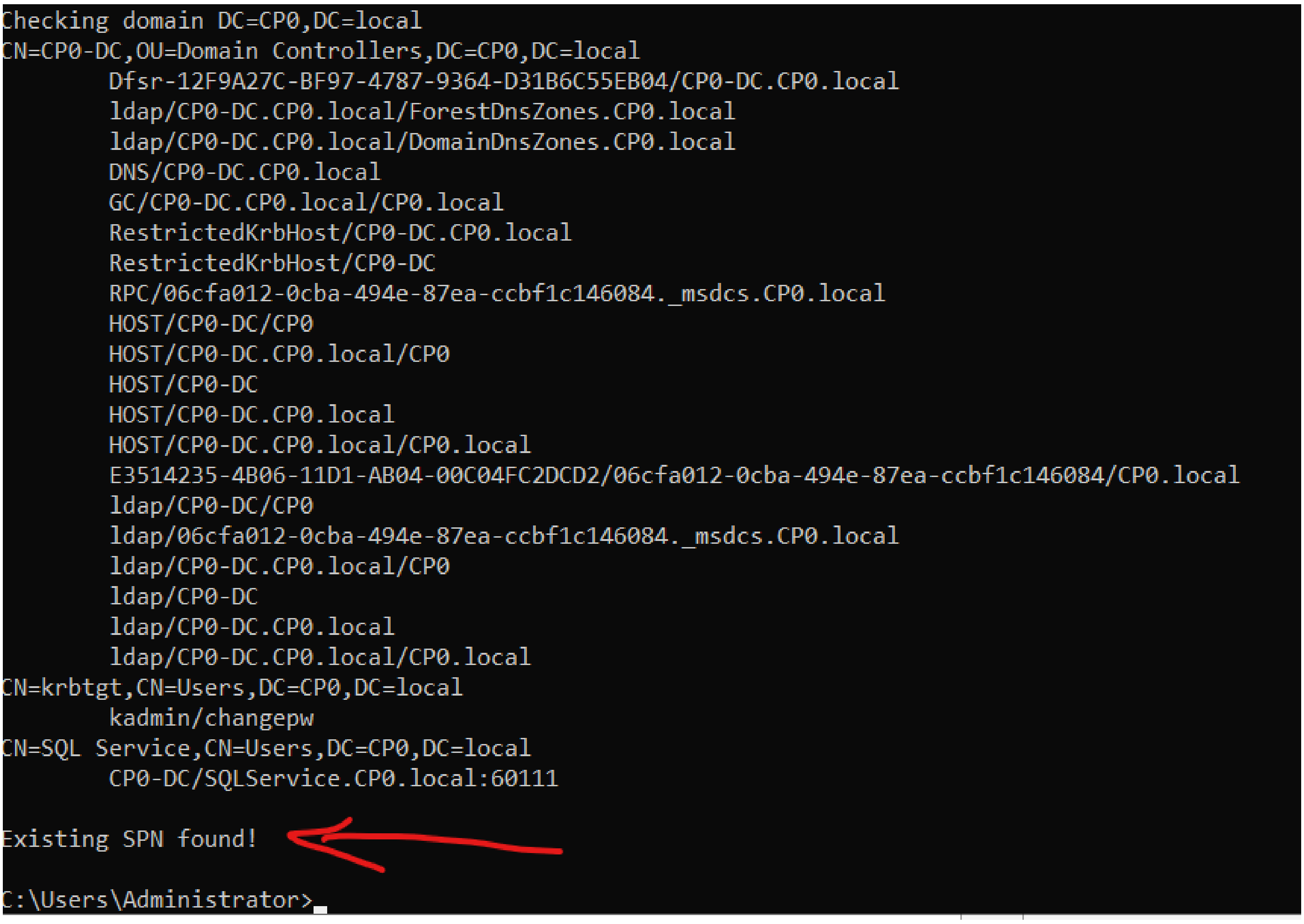
Server Manager > File and Storage Service, on the left Menu Bar > Shares > TASKS > New Share > Select "SMB Share - Quick" > Next > Share name: hackme > Accept Default for all the rest > Create.

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

Run CMD as Admin > Then, run "#setspn -a CP0-DC/SQLService.CP0.local:60111 CP0\SQLService"

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

```
"#setspn -T CP0.local -Q */* "
```



```
Checking domain DC=CP0,DC=local
CN=CP0-DC,OU=Domain Controllers,DC=CP0,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/CP0-DC.CP0.local
        ldap/CP0-DC.CP0.local/ForestDnsZones.CP0.local
        ldap/CP0-DC.CP0.local/DomainDnsZones.CP0.local
        DNS/CP0-DC.CP0.local
        GC/CP0-DC.CP0.local/CP0.local
        RestrictedKrbHost/CP0-DC.CP0.local
        RestrictedKrbHost/CP0-DC
        RPC/06cfa012-0cba-494e-87ea-ccbf1c146084._msdcs.CP0.local
        HOST/CP0-DC/CP0
        HOST/CP0-DC.CP0.local/CP0
        HOST/CP0-DC
        HOST/CP0-DC.CP0.local
        HOST/CP0-DC.CP0.local/CP0.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/06cfa012-0cba-494e-87ea-ccbf1c146084/CP0.local
        ldap/CP0-DC/CP0
        ldap/06cfa012-0cba-494e-87ea-ccbf1c146084._msdcs.CP0.local
        ldap/CP0-DC.CP0.local/CP0
        ldap/CP0-DC
        ldap/CP0-DC.CP0.local
        ldap/CP0-DC.CP0.local/CP0.local
CN=krbtgt,CN=Users,DC=CP0,DC=local
        kadmin/changepw
CN=SQL Service,CN=Users,DC=CP0,DC=local
        CP0-DC/SQLService.CP0.local:60111

Existing SPN found!

C:\Users\Administrator>_
```

Finally, we are going to set up Group Policy.

Group Policy Management > Expand Forest > Expand Domains > Right-Click CP0.local > "Create GPO in this Domain, and ...." > Disable Windows Defender.

The new Policy should pop up under the CP0.local > Right-Click it > Edit > Expand "Policies" under "Computer Configuration" > Expand "Administrative Templates" > "Windows Components" > Select "Microsoft Defender Antivirus" > Select "Turn Off Microsoft Defender Antivirus" > Enable > Apply > Save.

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

Finally,

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 > Do not give an alternate DNS Server, and leave Preferred DNS Server to be 127.0.0.1 (localhost).