# Practical No: 6

Configure FSLogix container

Agenda:

Section 4:

1. Create Groups in Dc and assign Roles in Fileshare
2. Mount FS in VM and Config NTFS permission
3. Configure Fslogix container and config NTFS
4. Reference: - https://www.youtube.com/watch?v=6Zpq9XnFRLA&list=PL-7q6zBuziYE9ZMWhigjU6VXlOv1mLnpL&index=6
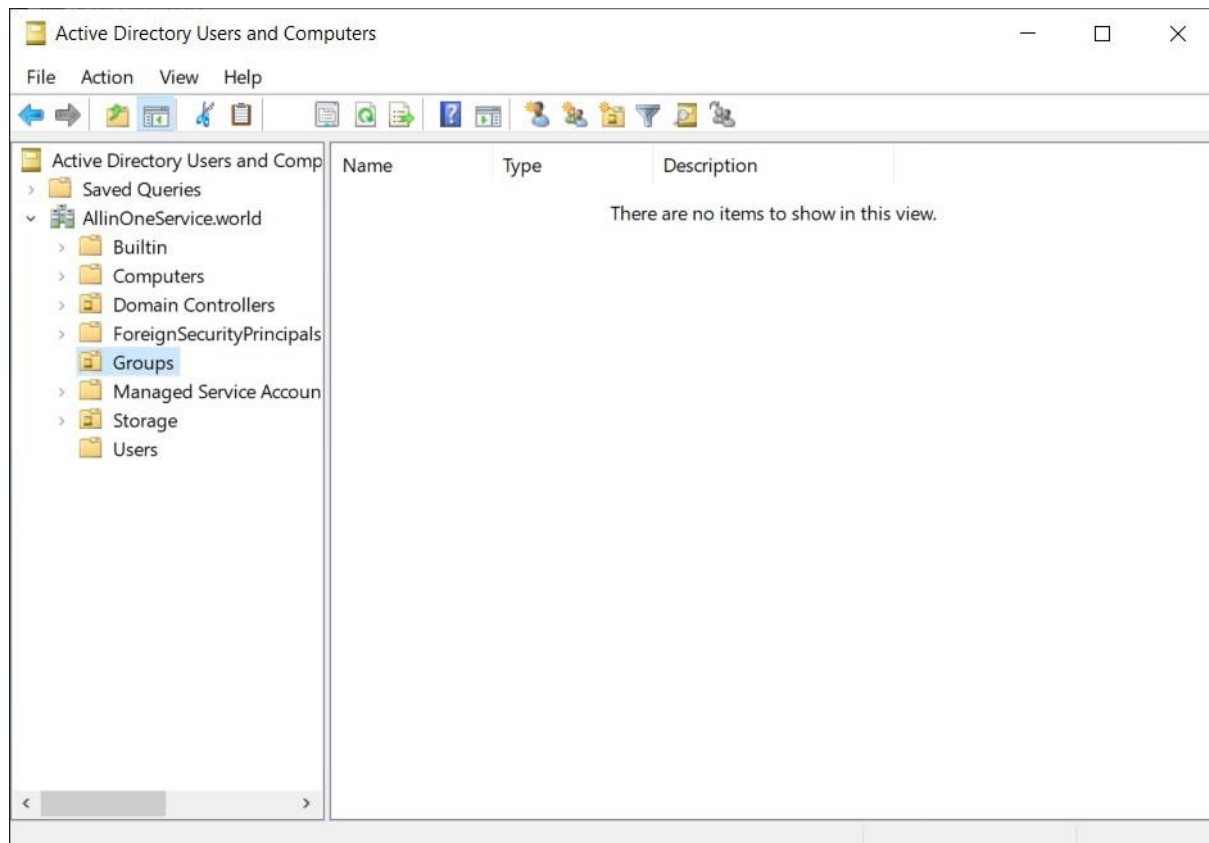
1. Create Groups in Dc and assign Roles in Fileshare:

- Go to Created VM
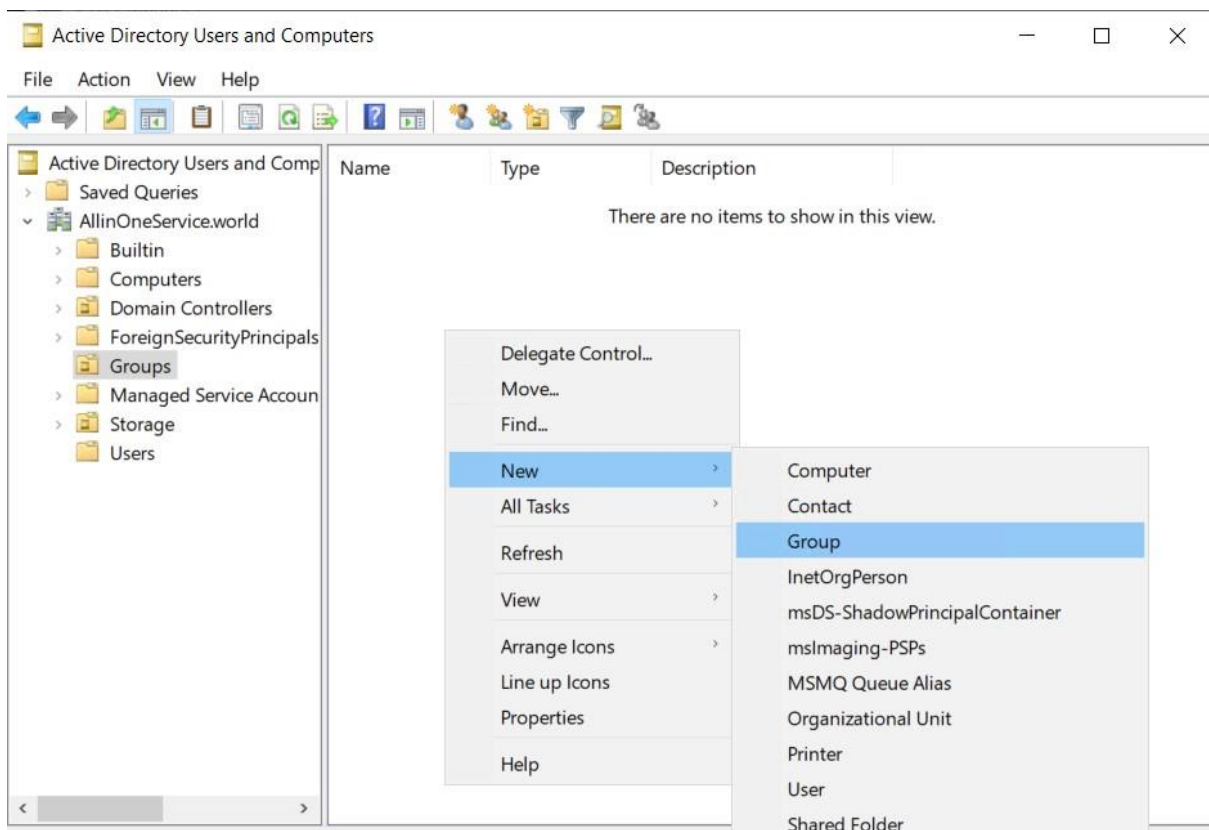- In server Manager→ Click to Tools→ Active Directory users and Computers
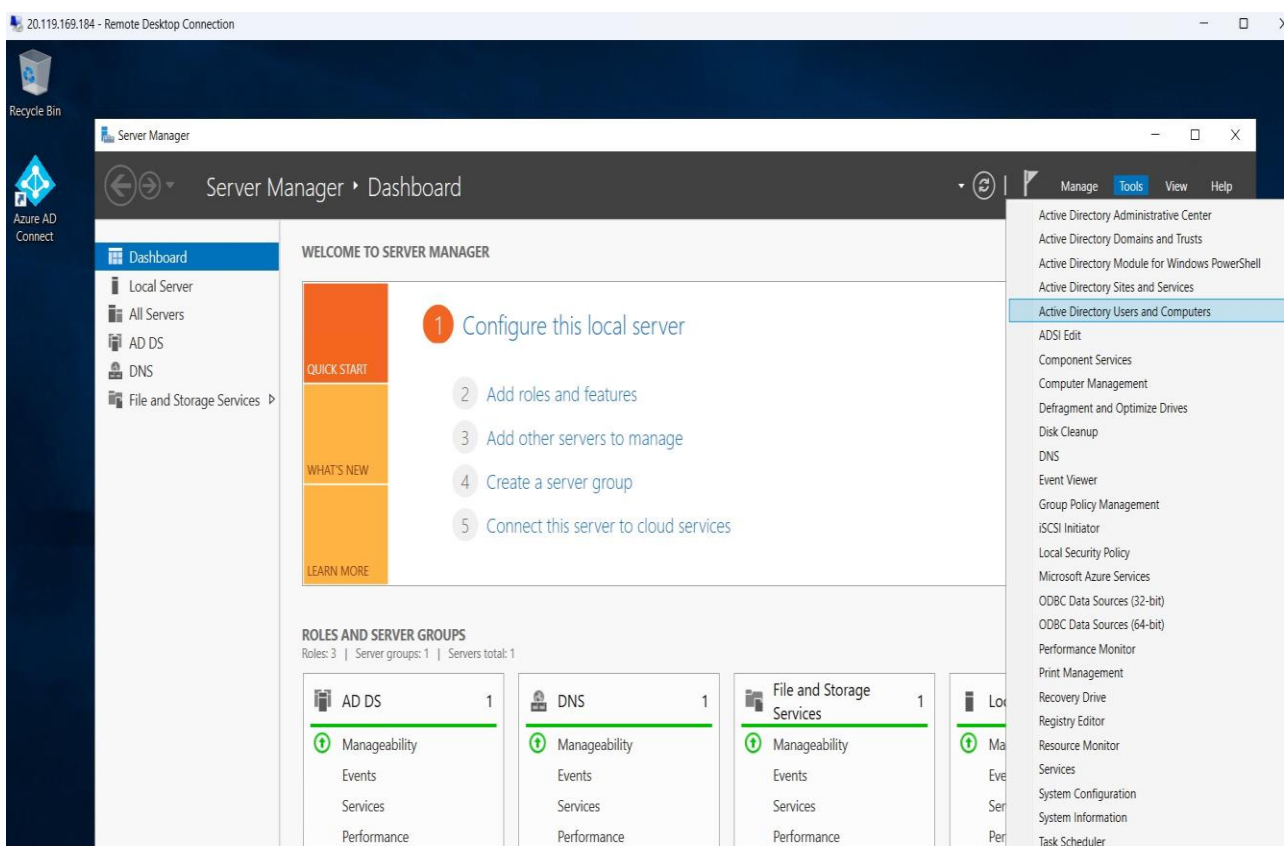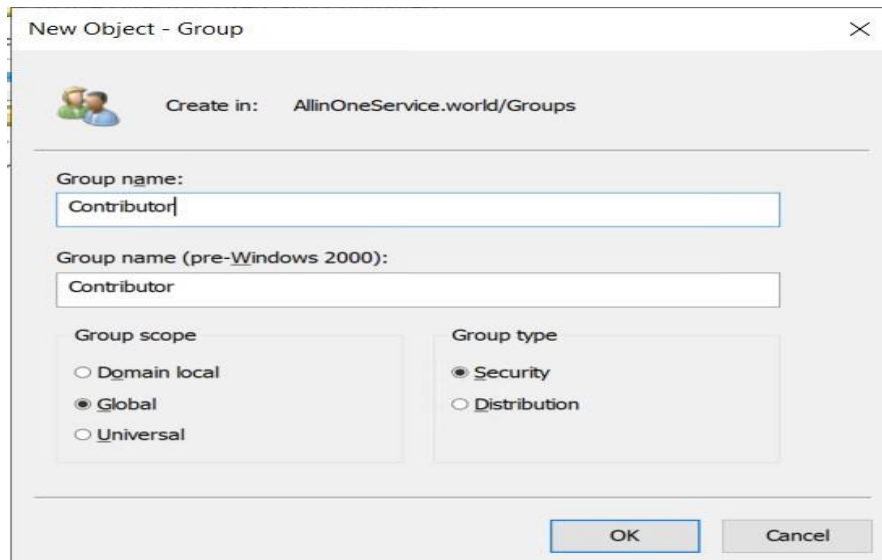
- Create a new group Floder

- Right click and create a new group

- Give name Contributor
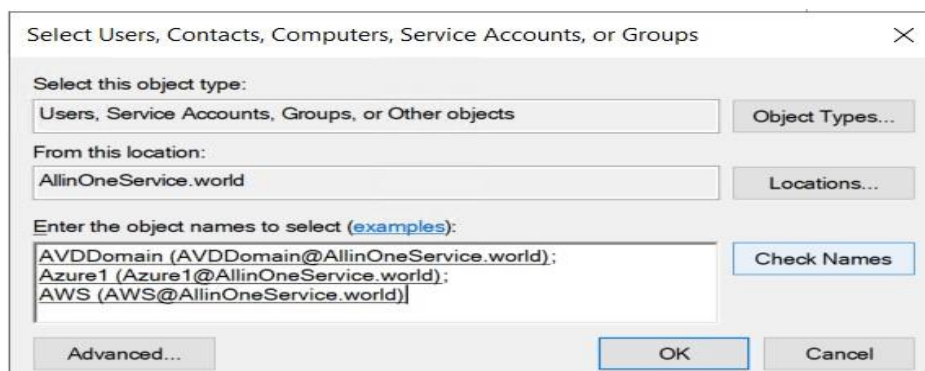
- Go to Members and Add created user

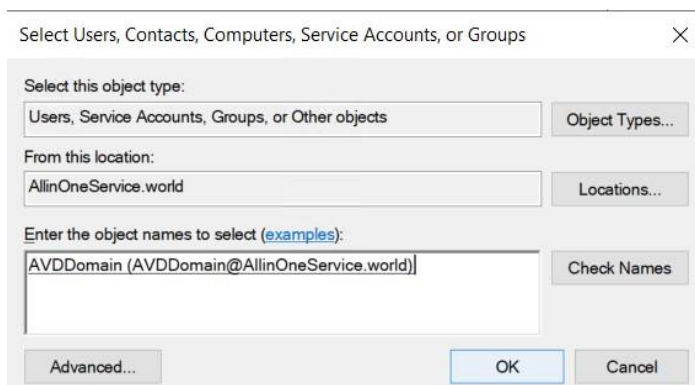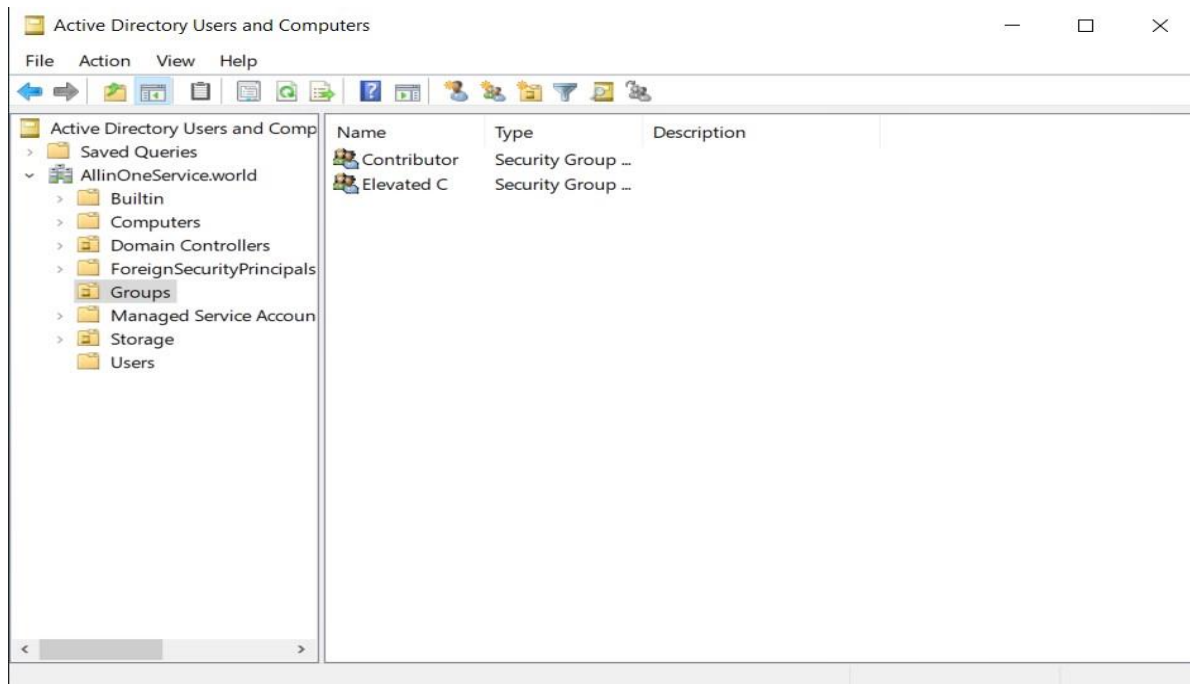- Now again Right click and create a new group
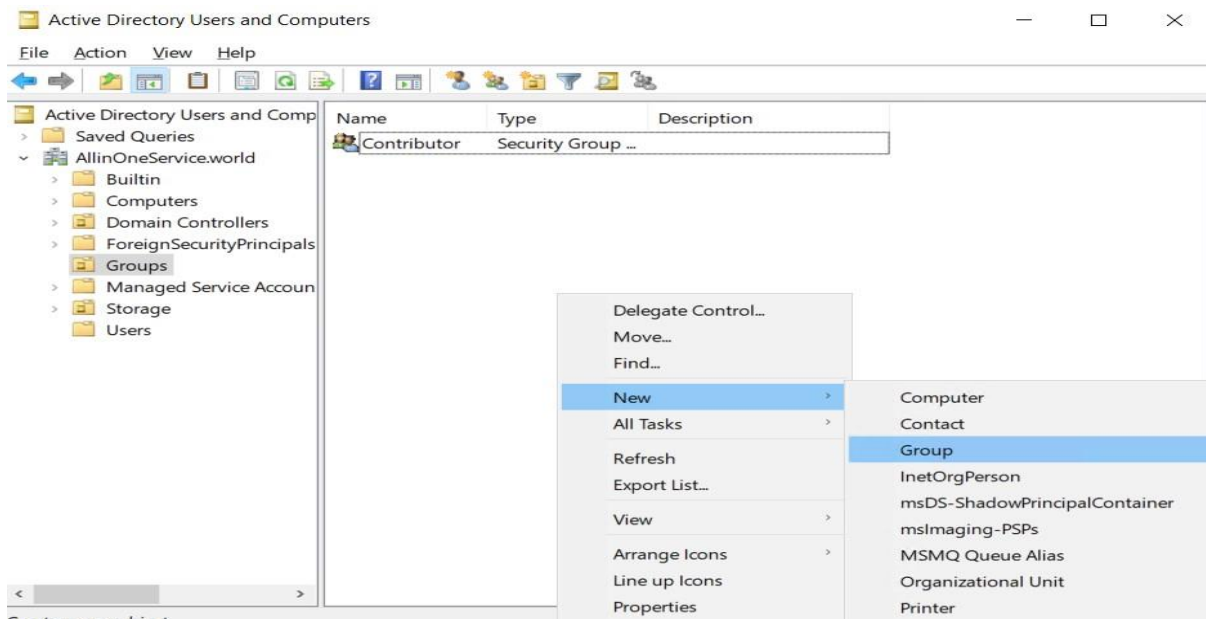
- Give name of Group Elevated C
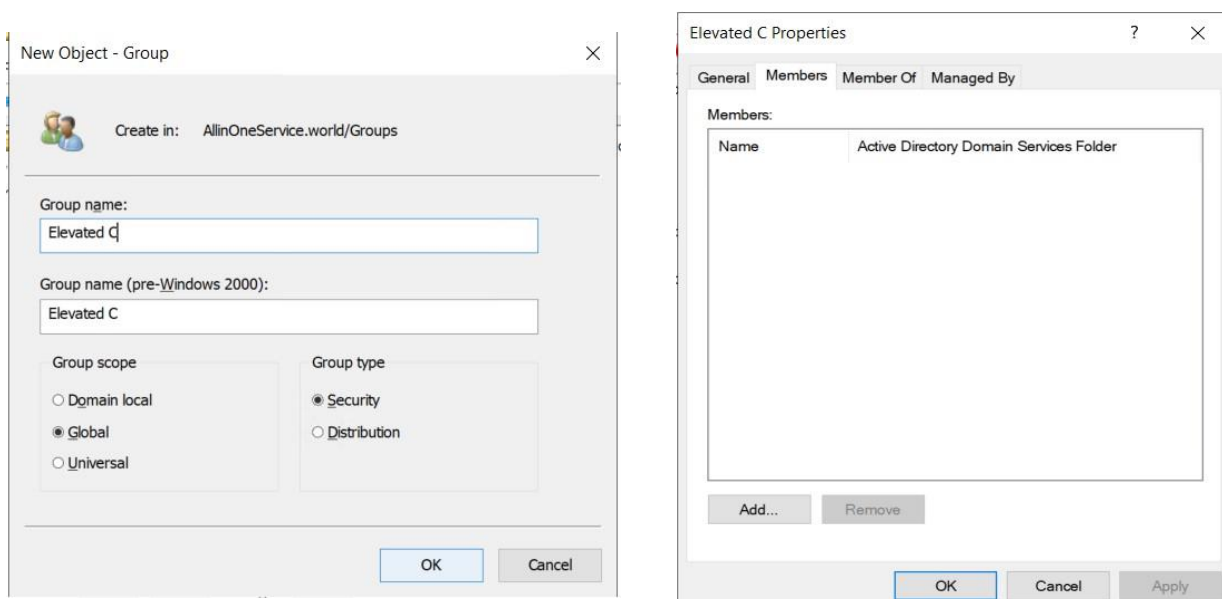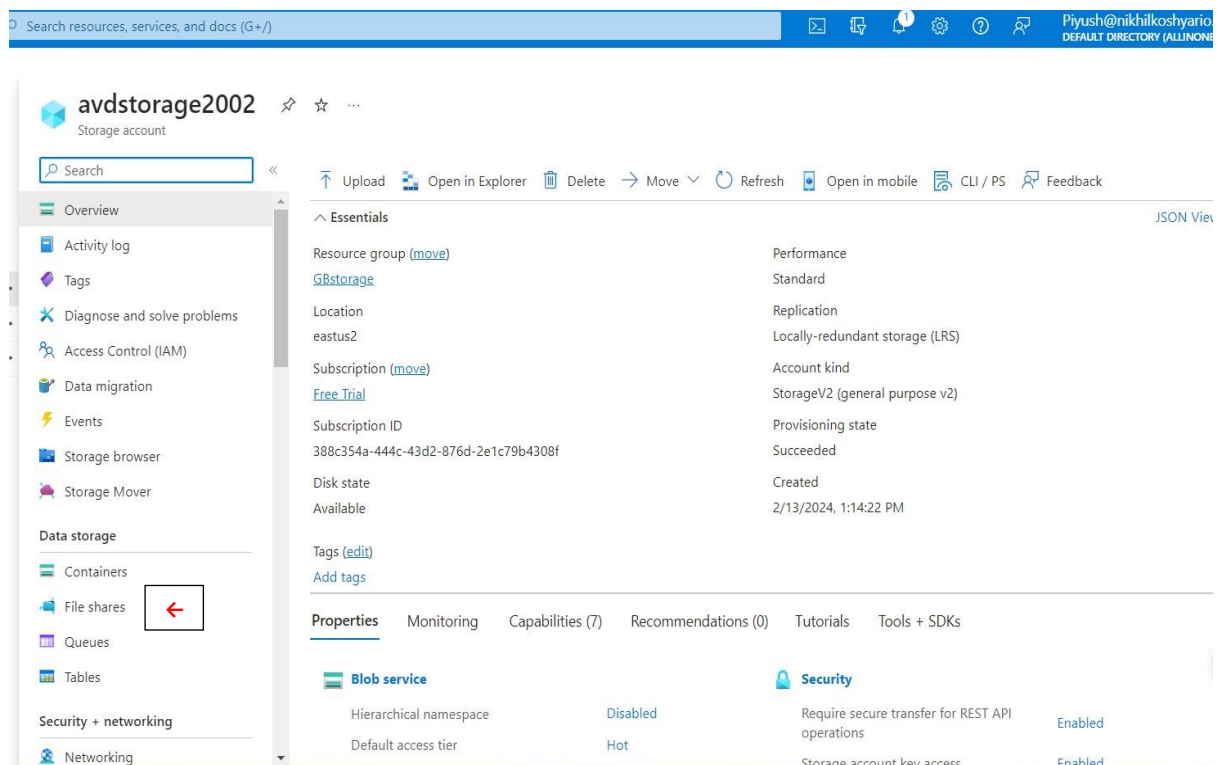

- Add member AVDDomain
- Then click ok

Section 4: Implementing Fslogix on AVD

2. Mount FS in VM and Config NTFS permission:

- Now Go to Azure portal, Created Storage Account
- Click to File share

Section 4: Implementing Fslogix on AVD

- Open avdfiles

- Need to assign Roles in Fileshare
- Click to IAM
- And Click to ADD roles

Section 4: Implementing Fslogix on AVD

- Click to Storage Files Data SMB share Contributor

- Click to Select member and Add all Dc created members

Section 4: Implementing Fslogix on AVD

- Same steps again Click to Storage Files Data SMB share Elevated Contributor

- Click to Select member and Add AVDDomain, Dc created members

Section 4: Implementing Fslogix on AVD

- We can see all users assign Roles for Fileshare

3. **Configure Fslogix container and config ntfs**

- Now Go to Azure portal, Created Storage Account
- Click to File share

Section 4: Implementing Fslogix on AVD

- Open avdfiles

- Click to Connect

Section 4: Implementing Fslogix on AVD

- Copy that Script

Connect
avdfiles

Hide Script

```
$connectTestResult = Test-NetConnection -ComputerName
avdstorage2002.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:`"avdstorage2002.file.core.windows.net`"
/user:`"localhost\avdstorage2002`"
/pass:`"DXOHJJscw/e9yUxk+eNNEE+3L06XULXktsMbJz/Np6QHlcUOhR95I2af
QCgh39enEK+nx0Smwysg+AStFJkdKA==`""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\avdstorage2002.file.core.windows.net\avdfiles" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port
445. Check to make sure your organization or ISP is not blocking port 445, or
use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic
over a different port."
}
```
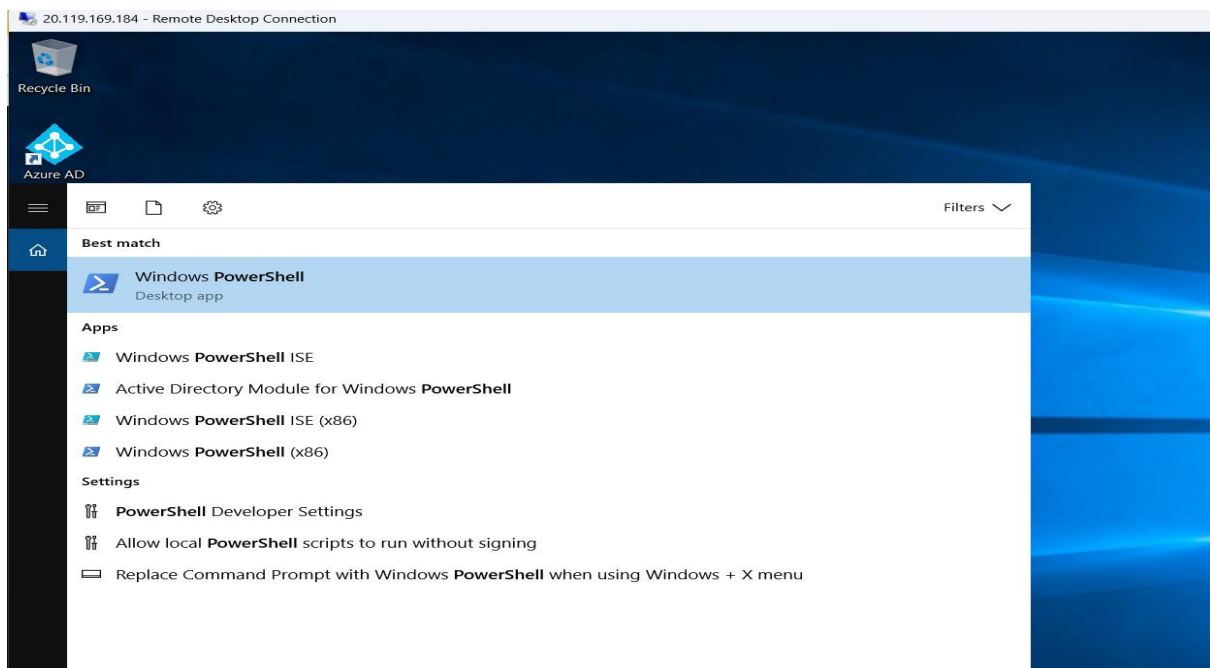
This script will check to see if this storage account is accessible via TCP port 445,
which is the port SMB uses. If port 445 is available, your Azure file share will be
persistently mounted. Your organization or internet service provider (ISP) may block
port 445, however you may use Azure Point-to-Site (P2S) VPN, Azure Site-to-Site
(S2S) VPN, or ExpressRoute to tunnel SMB traffic to your Azure file share over a
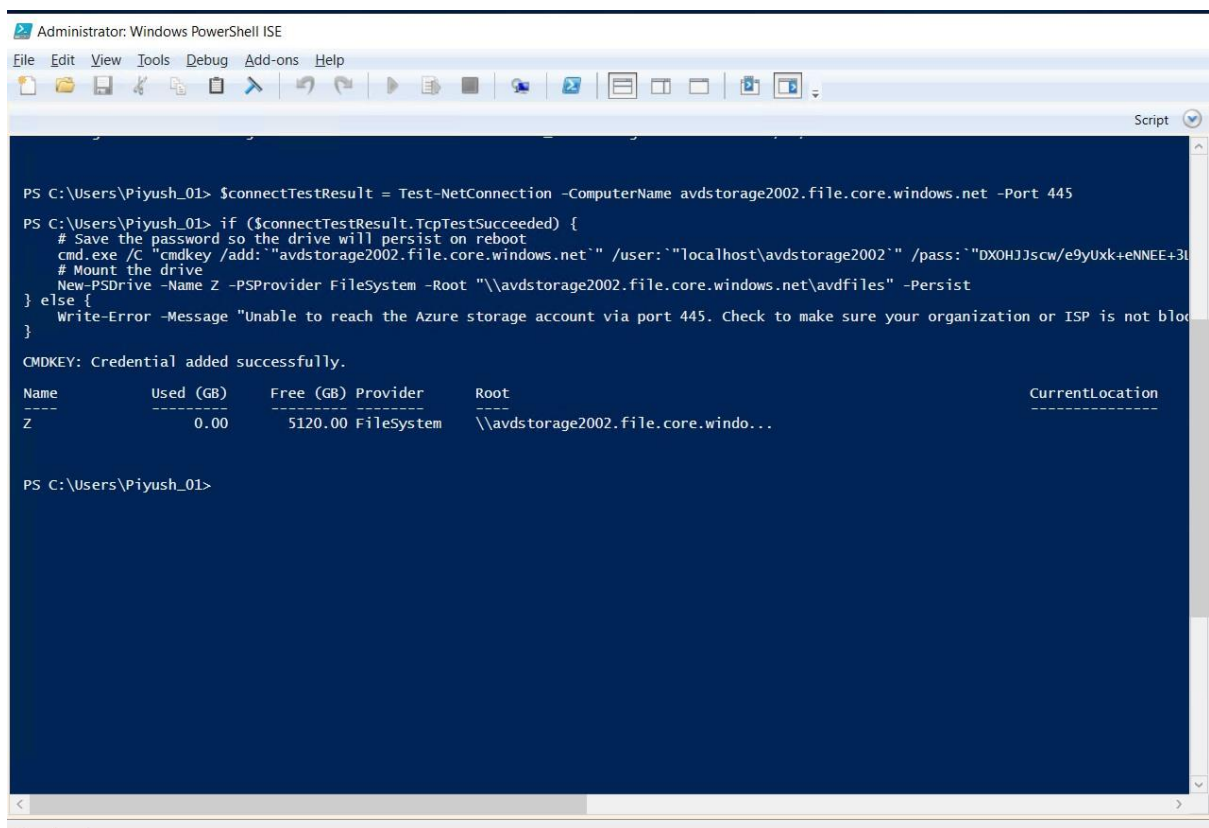different port.

⟨ฅ⟩ Give feed

- Now in Windows Search menu → Search Windows PowerShell ISE
- Run as administrator

Section 4: Implementing Fslogix on AVD

- Fllow this steps:
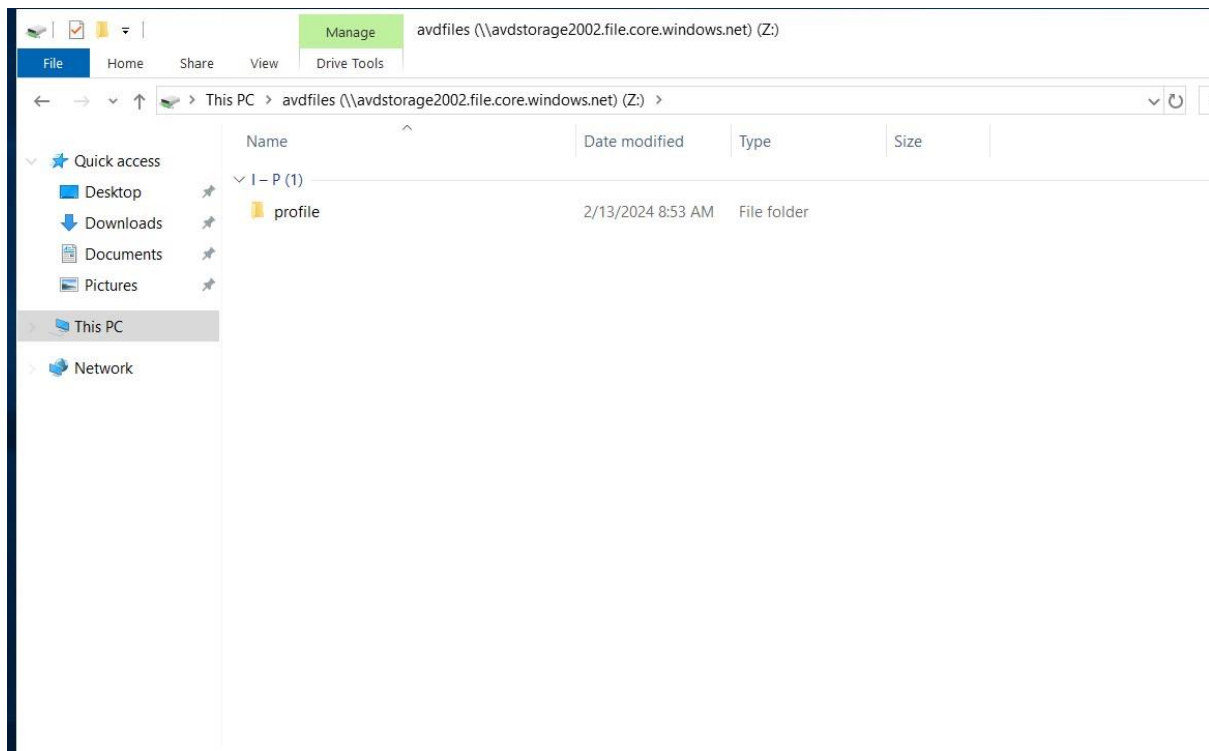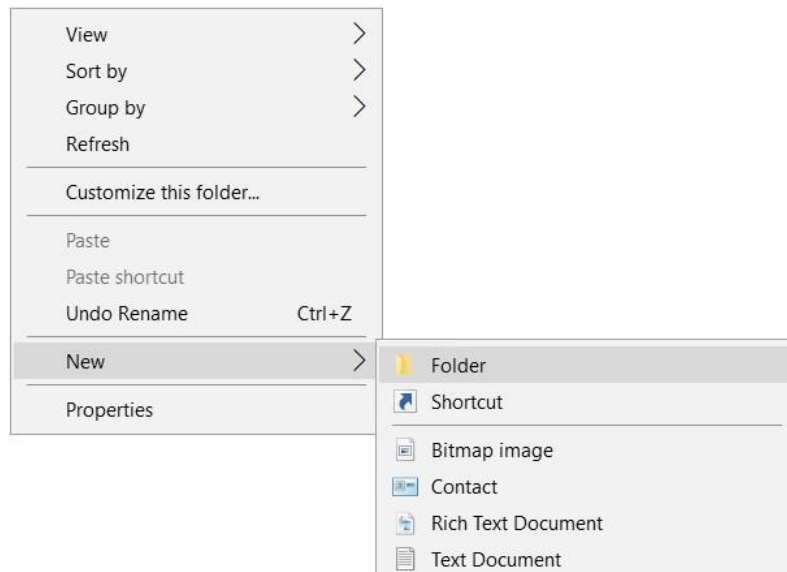

- Open File Manager → this PC
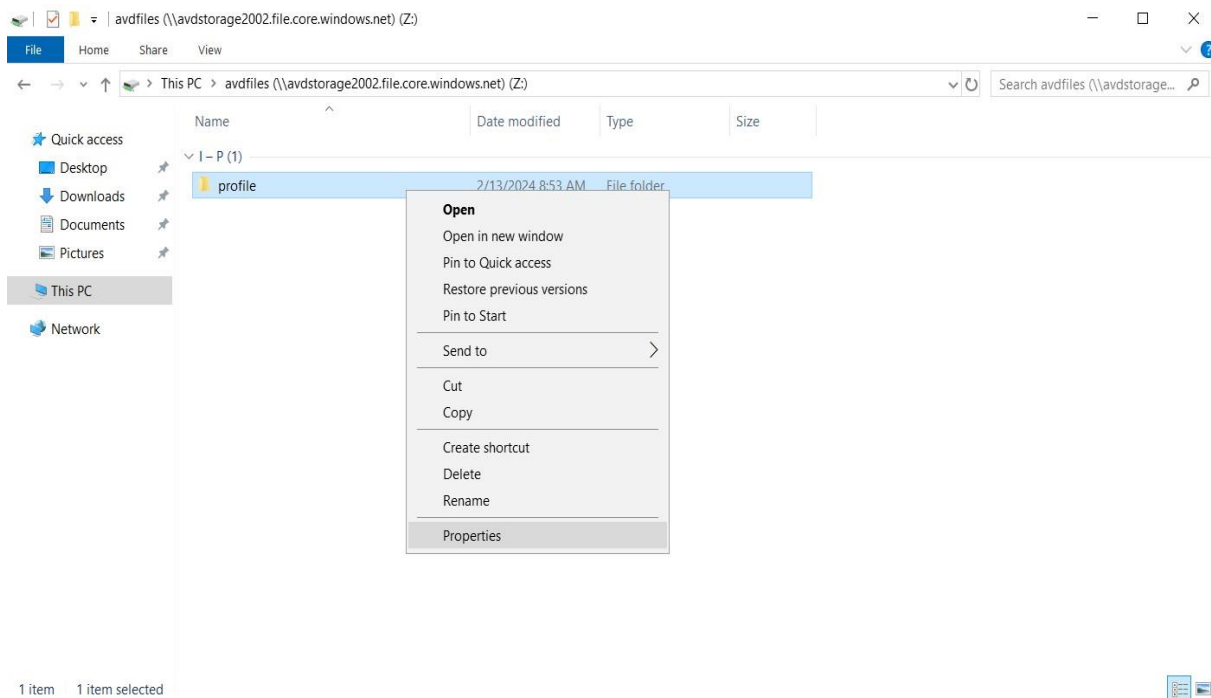- We can see Fileshare Storage Z dive is available
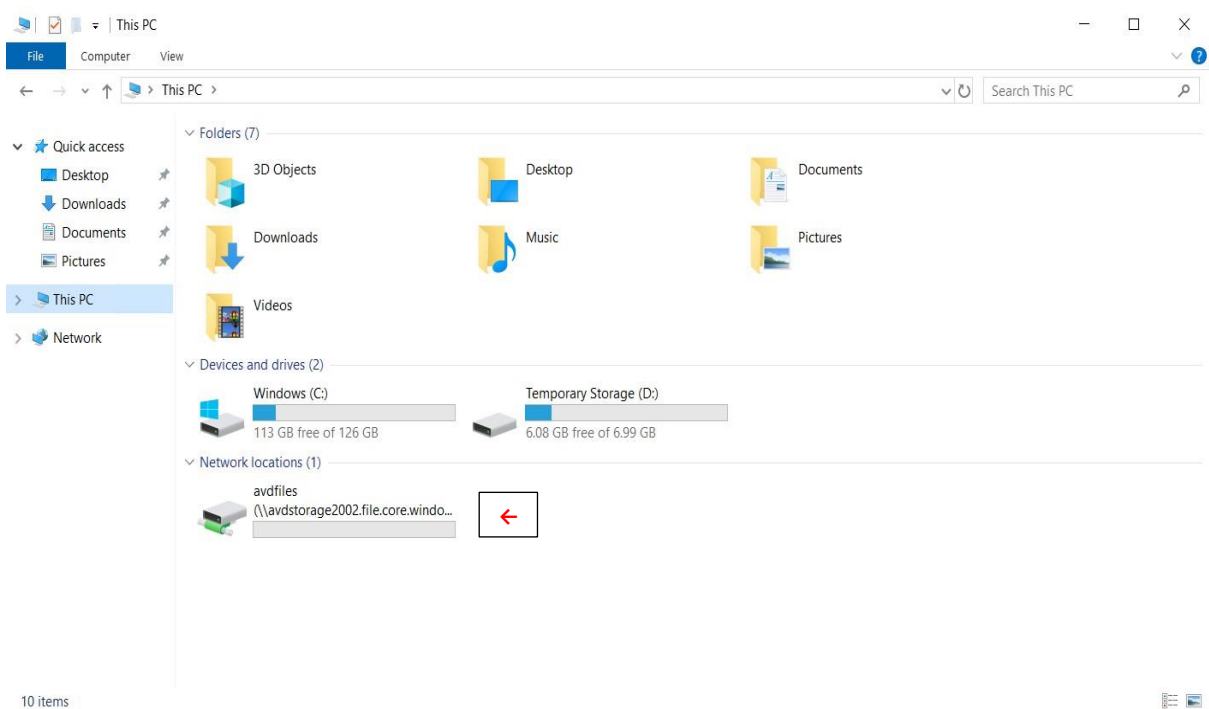
Section 4: Implementing Fslogix on AVD

- Open avdfiles drive
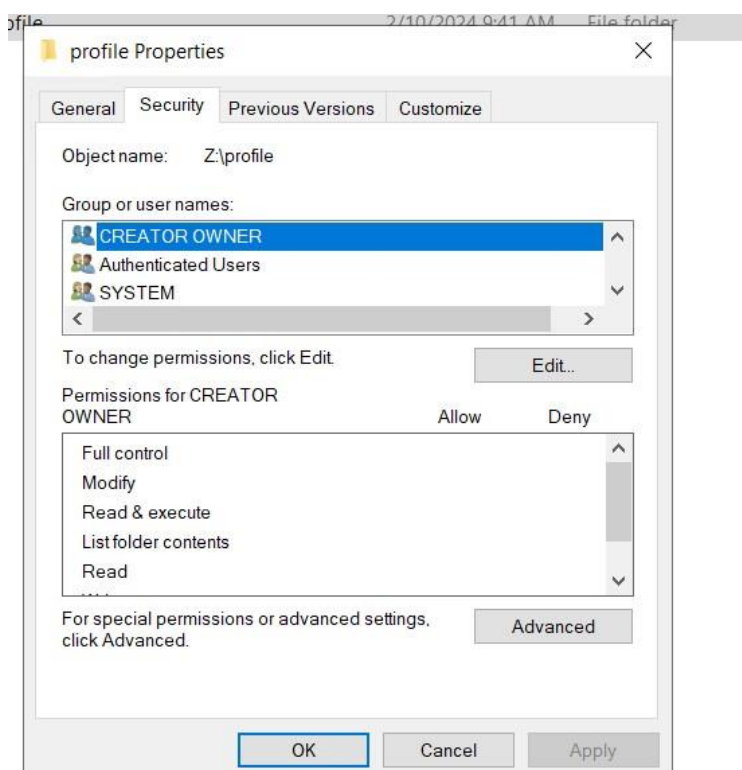- Create a new Folder name profile

Section 4: Implementing Fslogix on AVD

- Right click that profile folder
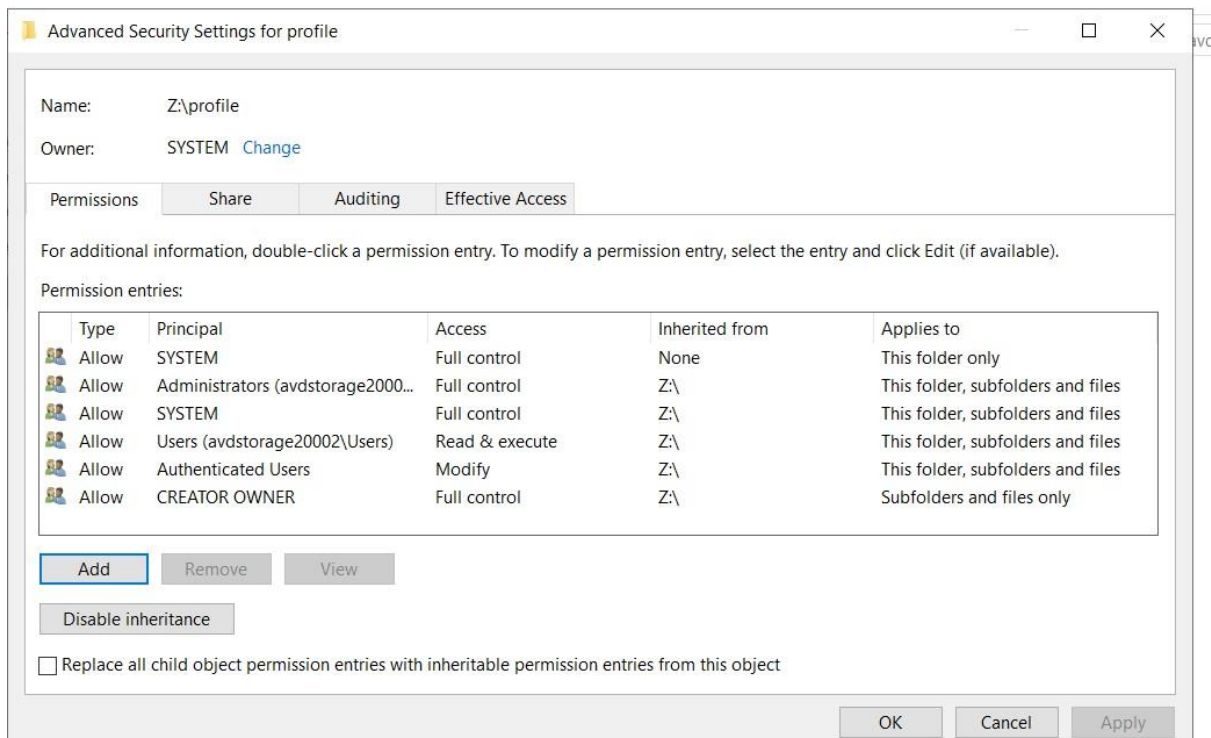- Select the properties option
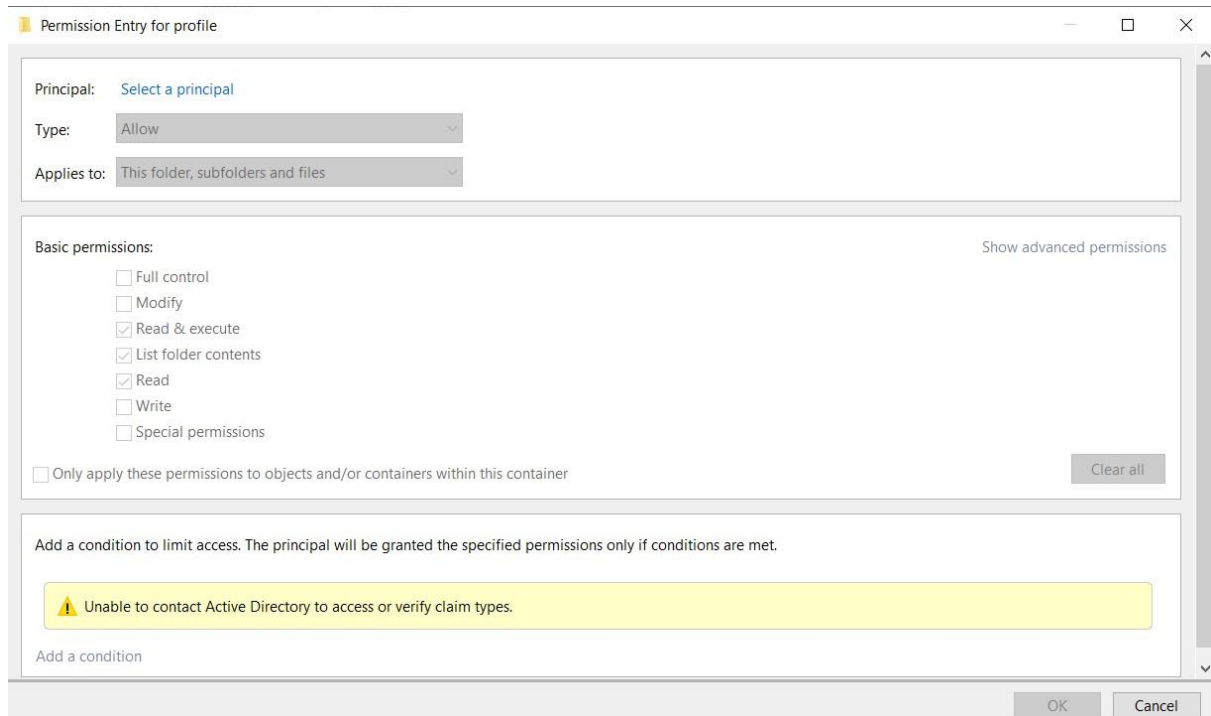

- Click to Advanced

Section 4: Implementing Fslogix on AVD
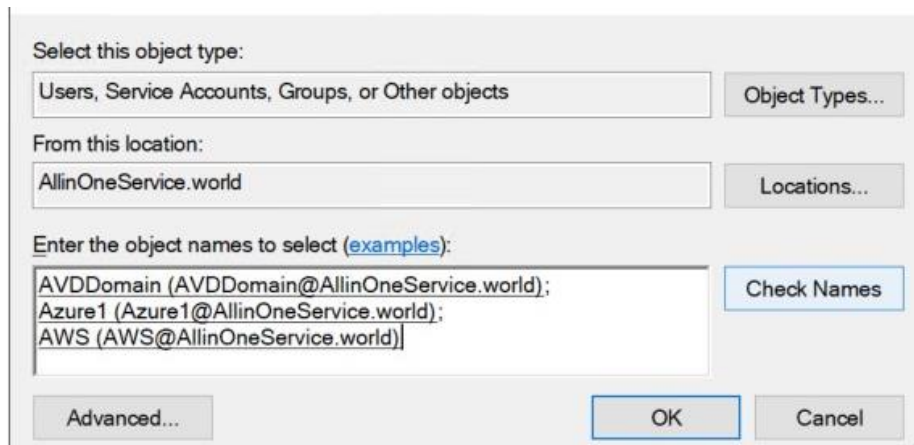
- Click to Add

- Click Select a principal

Section 4: Implementing Fslogix on AVD

- Asign members to Access the fileshare
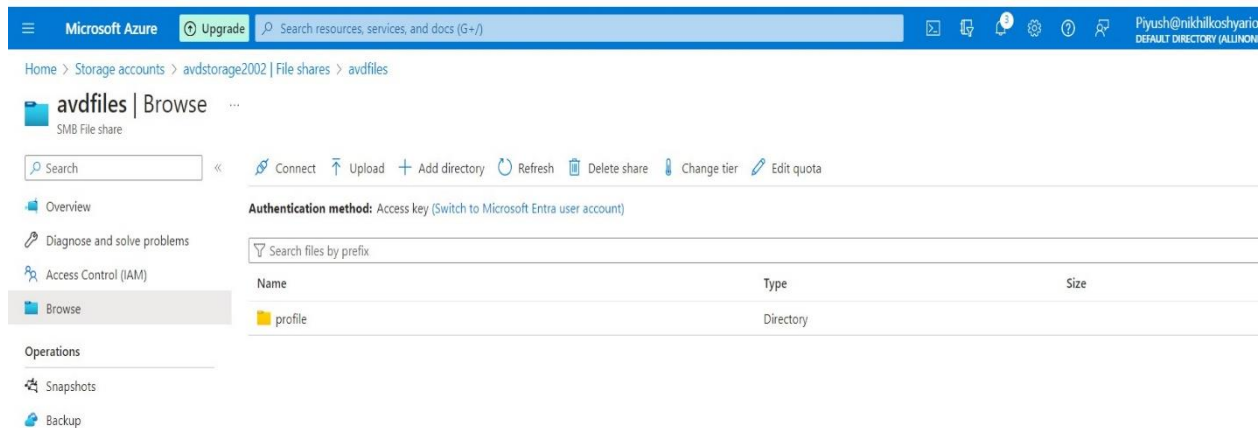
- Now Go to Azure portal, Created Storage Account →Click to File share →open avdfiles→ Browse
- We can see created folder in VM is available in azure storage portal