Part of my ongoing daily update to Principal Manager during the platform re-organization project.

Update as per deploying domain services and joining window server virtual machine to managed domain

- First update is that on AADDS-ad.sdpg.tv-NSG with consultation with Microsoft identity support, I changed the Port 443 source to AzureActiveDirectoryDomainservices source service tag. Instead of leaving it open to ANY.
- The domain services health is running healthy and the domain services is provisioned

As a test attempt to provision **a windows virtual machine** to join to the managed domain;

- I created new windows server machine. I have this new VM server in different data centre region, it's better to have the vm server on same region with other vms, though its in same developer-vm RG.

Here are the details of the vm:

Virtual machine name: doaminservervm

Username: devadmin

Password: Devadmin234

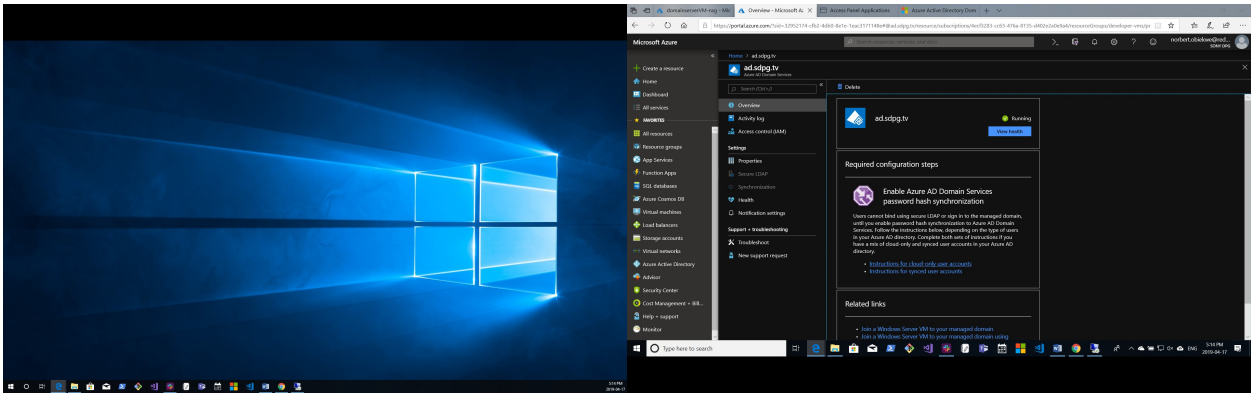
I configure the virtual network with the vnet of hosted domain services using the VPN peering features. I changed the dns server of the new vm to be same with other custom dns server.

I couldn't join the server to domain because of role permissions and we need to perform password hash synch first.

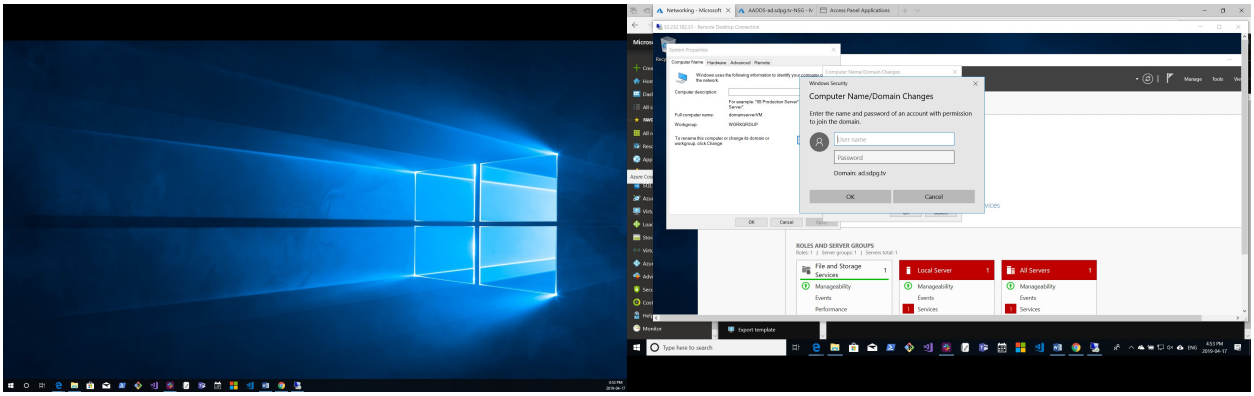
One best practise step is to have a separate account for Admin task. For that means creating separate admin user name and password for global admin task.

So , we have a windows server machine which we can join to the domain services and from this server once its join to domain, it should be able to pick up other vms and users in the active directory, the management of the users and vms would be from this server , few other server role/features would need to be installed in the server.

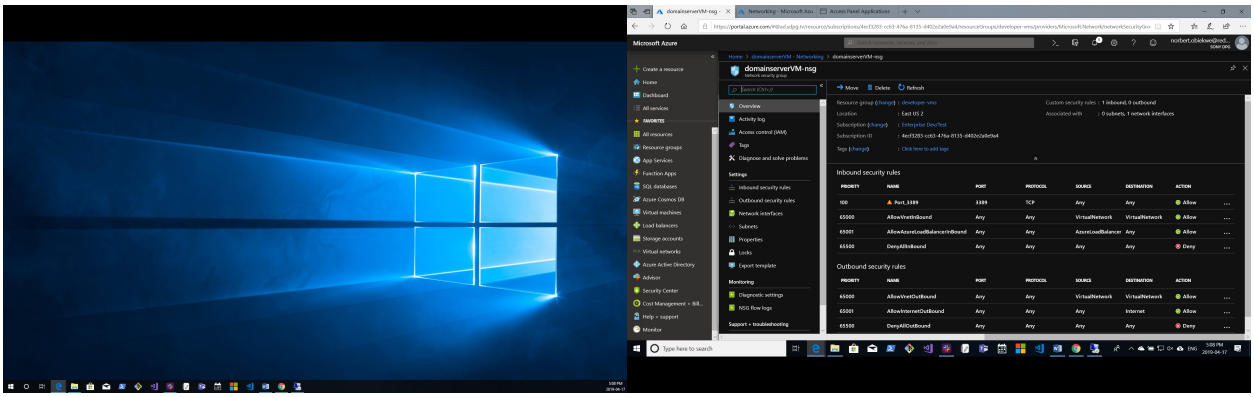
The next step is enable azure ad domain services password hash sync.



Users cannot bind using secure LDAP or sign in to the managed domain, until the password has sync to azure AD DOMAIN SERVICES is enabled. Steps here: https://aka.ms/aadds-pwsynccloud



Newly provisioned windows server vm (domainservervm) **I tried joining the server to domain but doesn't have correct credentials, and we need to have separate account for admin tasks**



New domainserverVM-nsg (this is more of testing. The 3389 port is source; ANY.) need to have the ips, mostly your network ip and mine in there as we both would be one having to rdp to the server.

Protecting Ad and Admin privileges:

1- Separate account for admi tasks

2- Set up unique privileged access workstations for active directory admin

3- Local admin passwords for each host

4- Unique local admin passwords for servers

Securing privileged access roadmap

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access (edited)

Norbert Obiekwe - 2019