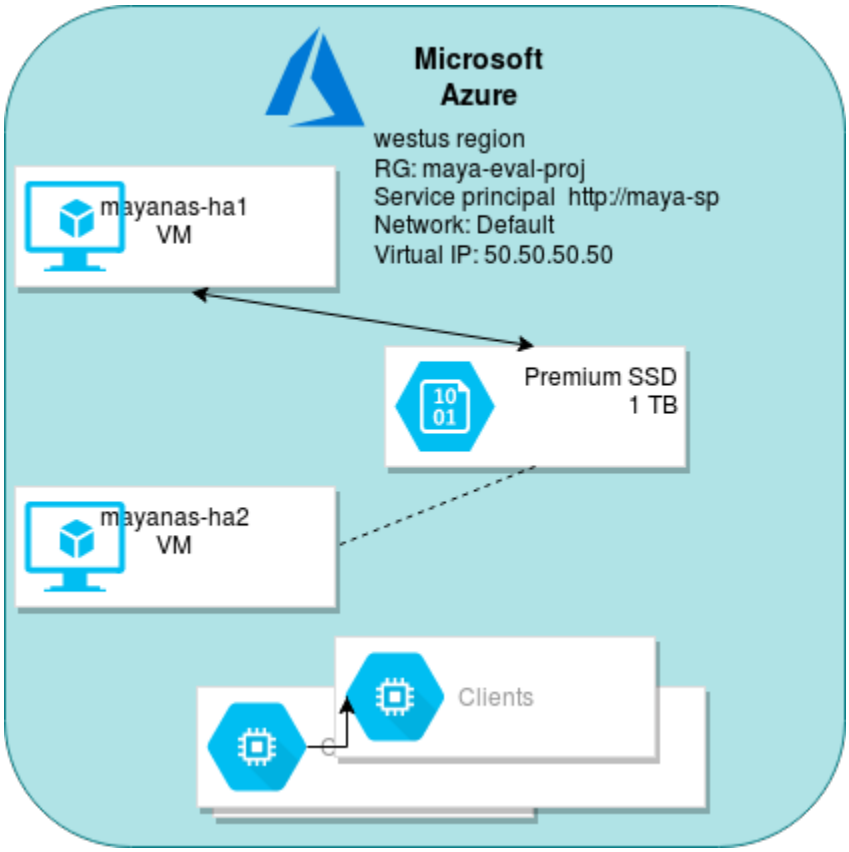
Getting Started on Azure Cloud

Azure Cloud Platform provides rich set of resources for building true enterprise-class NAS server readily. Please note that the network bandwidth is tied to the number of cpu cores of the compute instance. The storage IOPS is based on capacity of provisioned storage. Please refer to Azure cloud documentation for detailed configuration steps.

Purpose	Machine	Cores	Memory	Network	Storage
Shared block storage for IP-SAN or NVMeoF	Storage Optimized Lsv2-series	8	64GB	~3Gbps	Premium_LRS Ephemeral direct NVMe or SSD
Capacity Optimized NFS server LVM + VDO + XFS + NFS Server	General Family D-series	4	16GB	~8Gbps	Bcache(writeback) on Premium_LRS Data on Standard_LRS ssd:standard ratio 1:4
High Performance NFS Server	General Family DS-Series	8	30GB	~16Gbps	Bcache uses Premium_LRS Data on Standard_LRS
All Flash NFS server ZFS Storage Appliance	D32s_v3	32	128GB	~16Gbps	Data & Log uses SSD Persistent Disk (Premium_LRS)
High-Availability	High Availability Set Requires Service Principal			Azure internal LoadBalancer. Floating Virtual IP address	

Here is the sequence of steps involved in deploying High-Availability (HA) MayaNAS on Azure cloud platform. The next steps assume you've already deployed at two MayaNAS instances from Azure marketplace, with desired Availability Set. In this tutorial we will assume we are planning on deploying All Flash NFS Server configuration

- 2 compute instances `mayanas-ha1, mayans-ha2`
- 1TB Premium SSD persistent storage
- Default network for the internal
- Virtual IP: 50.50.50.50



1. Connect to mayanas instances using SSH to setup Service Principal account, which is required only if you are planning to configure HA services. Otherwise you may skip to Step 2. MayaNAS requires a Service Principal account with sufficient permissions to manipulate disk attachments for proper sharing and fencing, and also storage read-write access to object storage. It also needs sufficient permission to float the virtual IP across multiple instances. By having separate service account for all MayaNAS deployments you can enforce proper security measures as the assigned roles are limited to this project instance only.

   The service principal account is created from Azure cloud shell or **other system** where login credentials were already established, and not from the MayaNAS instances

   ```
   az ad sp create-for-rbac --name mayanas-sp --password Mayanas@123
   ```

   > Please take a note of the tenant ID for the newly created service principal account. You may choose the same service principal name but the password is given as an example only.

   ```
   On mayanas1:
   sudo az login--service-principal -u http://mayanas-sp --tenant  b9f7862a-7153-4501-8039-8d9b37d7c0a9

   On mayanas2:

   sudo az login--service-principal -u http://mayanas-sp --tenant  b9f7862a-7153-4501-8039-8d9b37d7c0a9
   ```

   > Please make sure login to service principal is done as root user. It is a one time setup only.

2. Change the default password to something random by running

   ```
   # /opt/mayastor/web/genrandpass.sh
   ```

   Or to set your own password

```
# /opt/mayastor/web/changepass.sh
Login name (default admin):
Login password:
Password again:
```

And then restart the web server for password changes to take effect

```
# /opt/mayastor/web/stop

# /opt/mayastor/web/start
```

3. Now you can proceed with High-Availability setup using the wizard from Administration Web console available on http://<mayanas-ip>:2020