Why We need custom Image?

Custom images are like marketplace images, but you create them yourself. Custom images can be used to bootstrap deployment tasks like preloading applications, application configurations, and other OS configurations.

Before Moving to the image definitions lets discuss something about the shared Image Gallery. We will proceed further with creating the Image definition within shared image gallery. We will also discuss how to share the gallery across the tenant and to individual user.

Shared image Gallery

The Shared Image Gallery lets you share your custom VM images with others in your organization, within or across regions, within an AAD tenant. Choose which images you want to share, which regions you want to make them available in, and who you want to share them with. You can create multiple galleries so that you can logically group shared images.

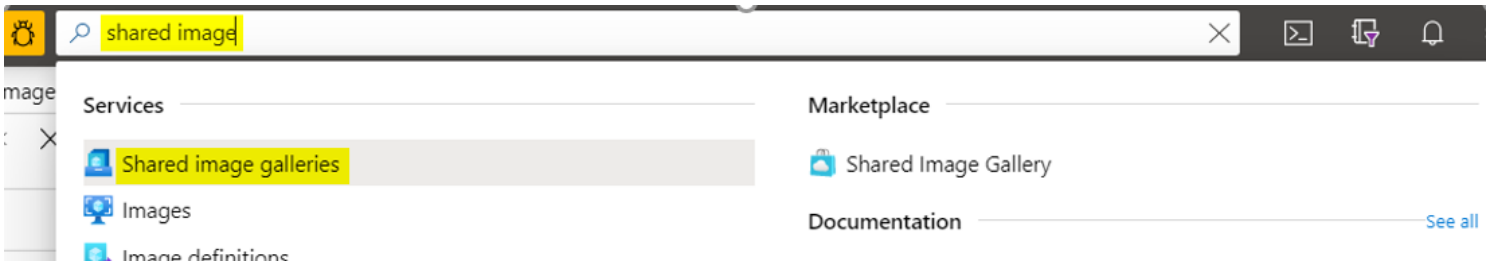
Shared Image Gallery is a service that helps you build structure and organization around your managed images. Shared Image Galleries provide:

- Managed global replication of images.
- Versioning and grouping of images for easier management.
- Highly available images with Zone Redundant Storage (ZRS) accounts in regions that support Availability Zones. ZRS offers better resilience against zonal failures.
- Sharing across subscriptions, and even between Active Directory (AD) tenants, using RBAC.
- Scaling your deployments with image replicas in each region.

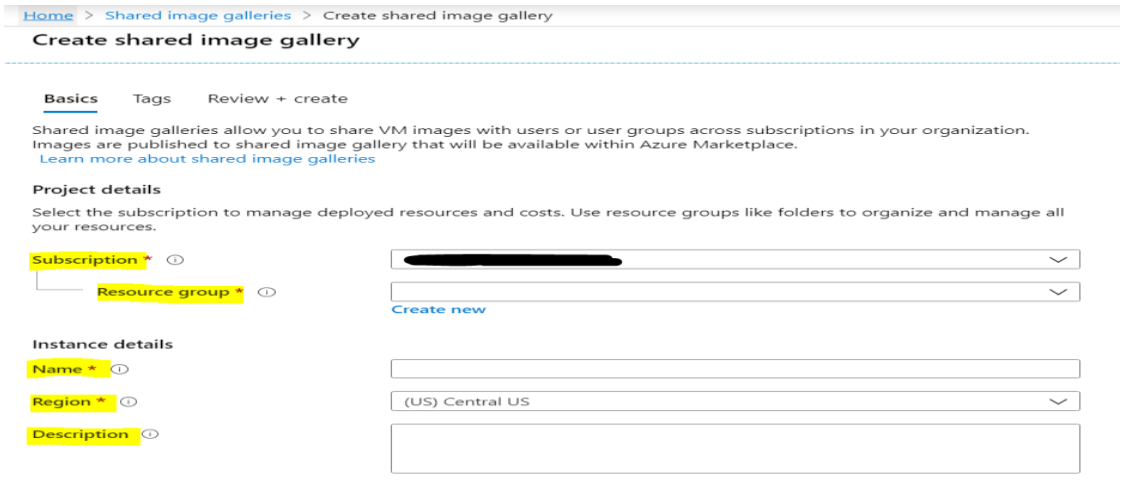
Using a Shared Image Gallery you can share your images to different users, service principals, or AD groups within your organization. Shared images can be replicated to multiple regions, for quicker scaling of your deployments.

Creating the new shared Image Gallery:

In the azure portal search for the “Shared image galleries”. It will give you the following:



After moving to the shared Image gallery click on the “Add” button and fill the details required:



After filling all the details click on Review + create button to create the Image gallery.

After creating the image successfully we may need to share the image gallery to the individual user or tenant. Below are the steps you need to follow :

Share Image gallery to user :

- Open the Azure portal.
- In the menu at the left, select Resource groups.
- In the list of resource groups, select your resource group. The blade for your resource group will open.
- In the menu on the left of the your gallery page, select Access control (IAM).
- Under Add a role assignment, select Add. The Add a role assignment pane will open.
- Under Role, select Reader.
- Under assign access to, leave the default of Azure AD user, group, or service principal.
- Under Select, type in the email address of the person that you would like to invite.

If the user is outside of your organization, you will see the message This user will be sent an email that enables them to collaborate with Microsoft. Select the user with the email address and then click Save.

Share Image gallery across tenant :

Create an application registration that will be used by both tenants to share the image gallery resources.

- Open the App registrations (preview) in the Azure portal.
- Select New registration from the menu at the top of the page.
- In Name, type app name.
- In Supported account types, select Accounts in any organizational directory and personal Microsoft accounts.
- In Redirect URI, type https://www.microsoft.com and then select Register. After the app registration has been created, the overview page will open.
- On the overview page, copy the Application (client) ID and save for use later.
- Select Certificates & secrets, and then select New client secret.
- In Description, type Shared image gallery cross-tenant app secret.
- In Expires, leave the default of In 1 year and then select Add.
- Copy the value of the secret and save it to a safe place. You cannot retrieve it after you leave the page.
- Give the app registration permission to use the shared image gallery.

In the Azure portal, select the Shared Image Gallery that you want to share with another tenant.

- Select Access control (IAM), and under Add role assignment select Add.
- Under Role, select Reader.
- Under Assign access to:, leave this as Azure AD user, group, or service principal.
- Under Select, type your app name with which you have registered the above application and select it when it shows up in the list. When you are done, select Save.

VM Image

The fundamental difference between the VM image and Image Definition is that the VM image will give you the option to create the VM with that image where as the definition will allow you to create VM as well as VMSS with that image.

1) **Creating the VM Image**

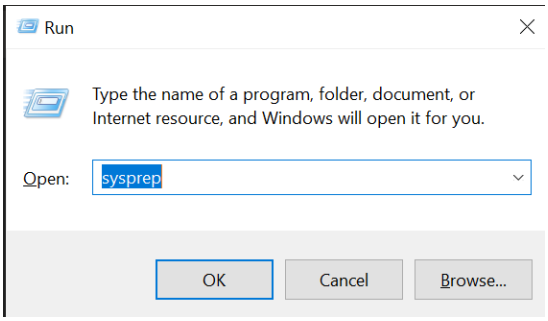
There are two ways of creating the VM image and use that in future to create a VM from that.

First way (The easy way)

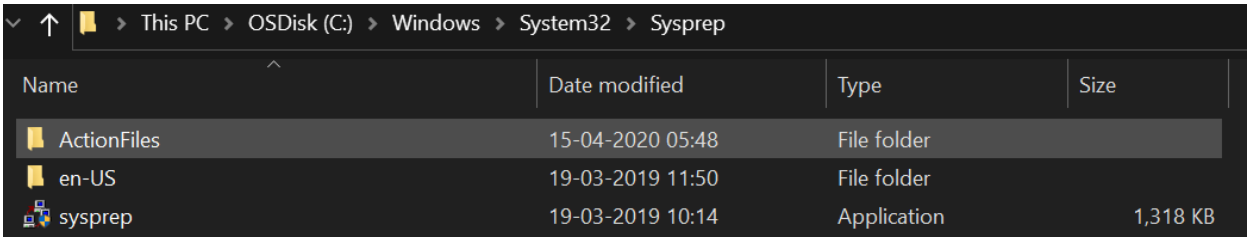
In this procedure you need to create a VM in the resource group using normal procedure. Then follow the below instructions:

- Login to the VM you created above and install all the software you want to be installed in your VM Image.

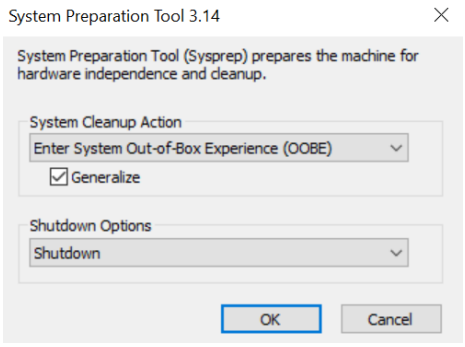
- After all the Software has been installed run the “sysprep” command. To do that press win+R and enter “sysprep”



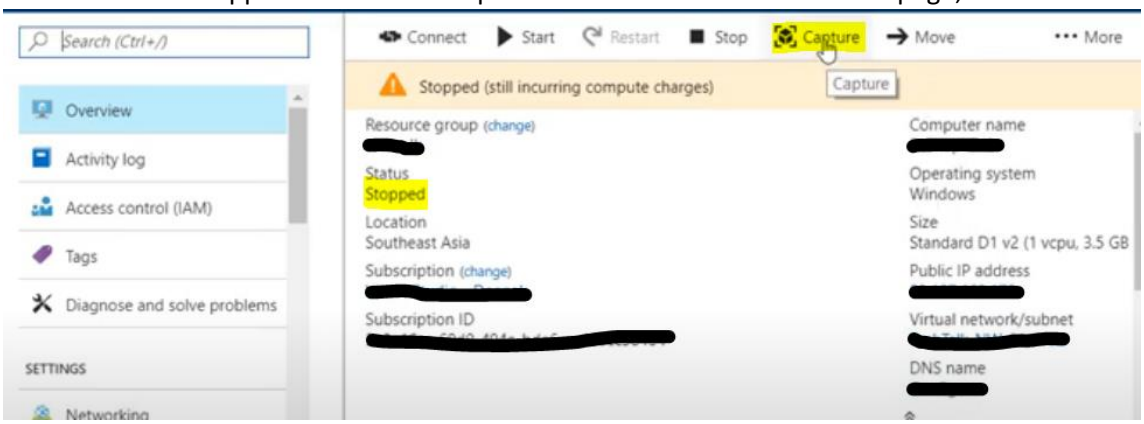
- Upon clicking on “Ok” button you must be redirected to the sysprep inside your VM. Below is the sample screenshot:



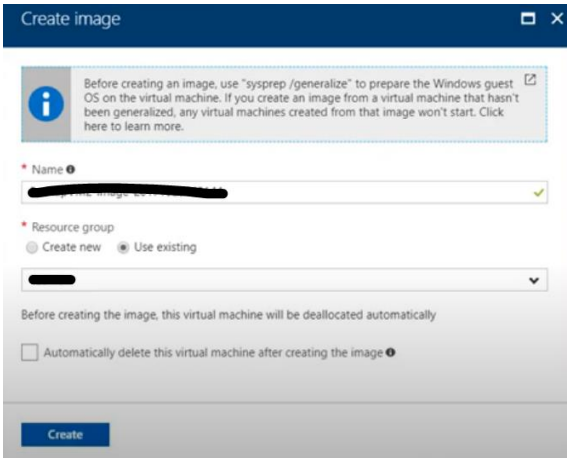
- Double click on the sysprep to start it. It will show you a small dialogue box, select the parameter as shown below:



- After the machine has been shutdown, go back to azure portal and wait for the VM to move to “Stopped” state.
- Once the VM is stopped click on the “capture” button on the VM overview page, below is the image for reference.

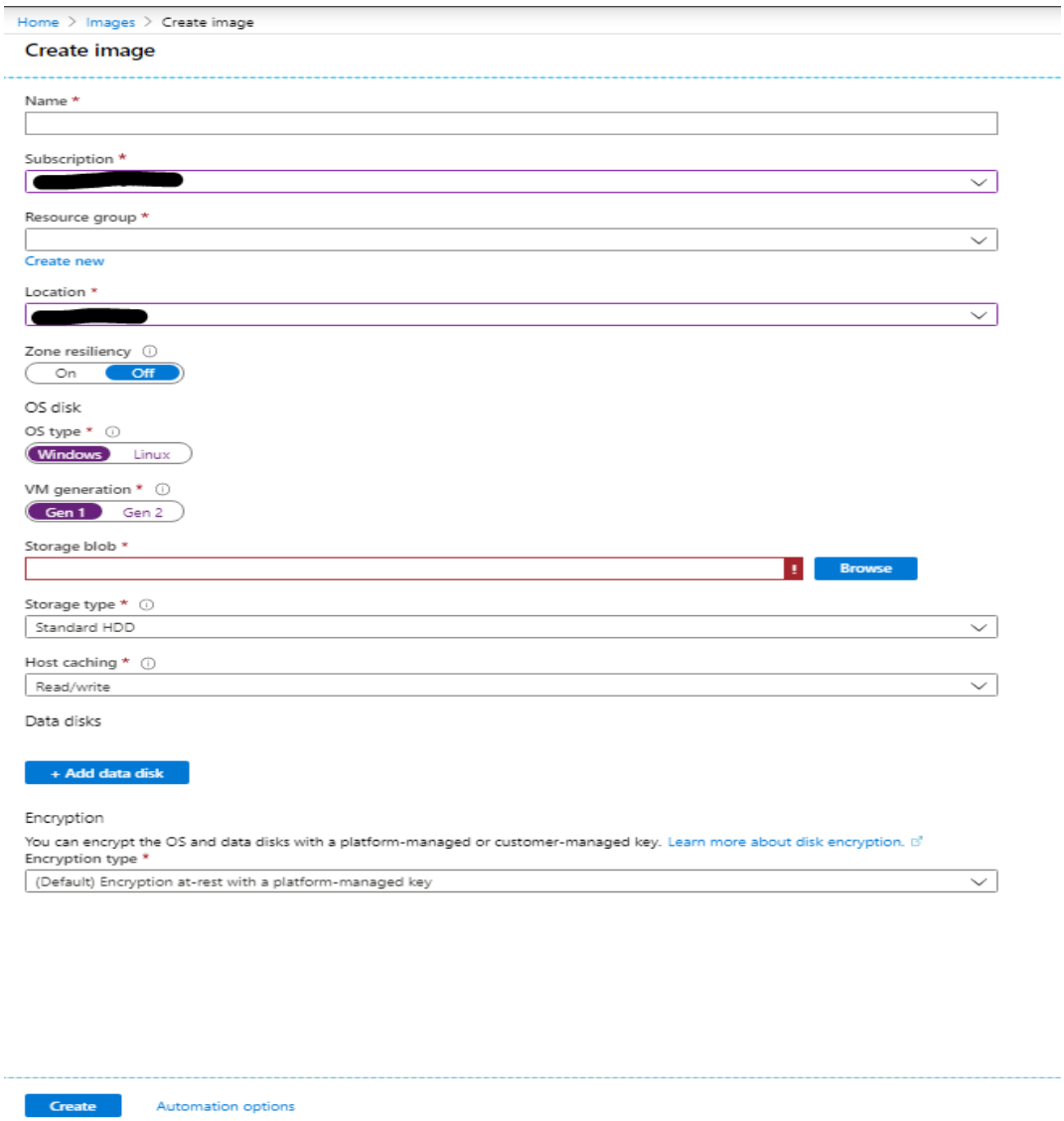


- When you will click on the capture button it will give you a form to fill up in order to create an image. Upon filling the form you will end up in creating the image of the desired state. While creating the image you may choose whether to delete the VM or not. Below is the form you will get.

- 

Second Way (Using VHDs)

To create a VM image search the “VM Image” in the home page of the azure portal. And then click on “Add Image” to create a new one.



Description of the parameters:

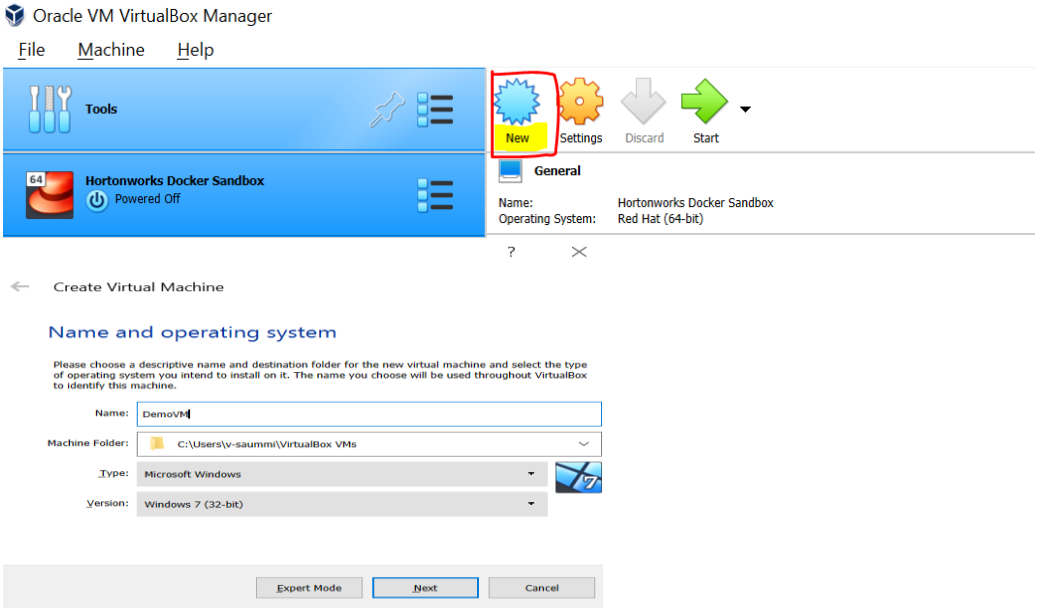
- **Name** : Name of the image you want to recognize with.
- **Subscription** : Subscription in which you want to create a VM image.
- **Resource Group**: RG in which you want to place your Image

- **OS Type** : Windows or Linux.
- **VM Generation**: Gen1 or Gen2 (Generation 2 VMs use the new UEFI-based boot architecture rather than the BIOS-based architecture used by generation 1 VMs.)
  Generation 2 VMs support key features that aren't supported in generation 1 VMs. These features include increased memory, Intel Software Guard Extensions (Intel SGX), and virtualized persistent memory (vPMEM). Generation 2 VMs running on-premises, have some features that aren't supported in Azure yet
  Generation 2 VMs use the new UEFI-based boot architecture rather than the BIOS-based architecture used by generation 1 VMs. Compared to generation 1 VMs, generation 2 VMs might have improved boot and installation times.
  You can choose which Generation you want to use based on your requirement.
- **Storage Blob** : Storage account blob containing your VHDs that will create a custom OS disk according to your requirement. Want to see how can we create VHDs. Its soon after this section.
- **Data Disk** : It is optional. If you want to add the data disk to the custom image you can do the same as above that is, browsing to the blob storage where your data disk is present.
- **Encryption** : We can encrypt the OS and data disks with a platform-managed or customer-managed key.
  Azure managed disks automatically encrypt your data by default when persisting it to the cloud. Server-side encryption protects your data and helps you meet your organizational security and compliance commitments. Data in Azure managed disks is encrypted transparently using 256-bit. By default, managed disks use platform-managed encryption keys. As of June 10, 2017, all new managed disks, snapshots, images, and new data written to existing managed disks are automatically encrypted-at-rest with platform-managed keys. We can choose to manage encryption at the level of each managed disk, with our own keys. Server-side encryption for managed disks with customer-managed keys offers an integrated experience with Azure Key Vault.

  After creating an Image you should be excited to see how it goes creates an VM with the image. To do so that is, to create an VM with the custom image, You can browse to the Image section and click on the image you created above. You can see a button called "+ create VM". All you need to do is to just click on the VM and provide the parameters for the VM such as Name, password and public ports etc to create the VM, and Booommmm, You are all set to use your VM.

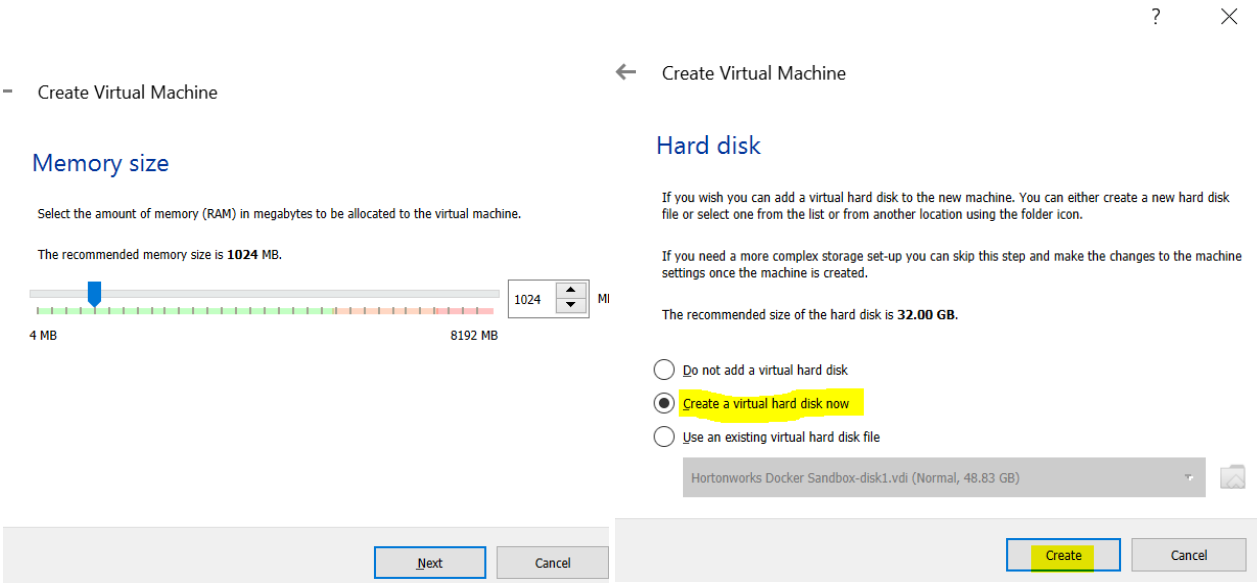
  Creating VHDs:

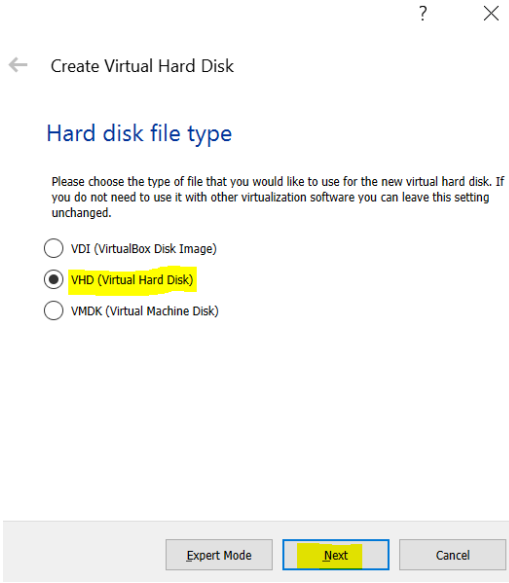
  Steps:
- Install the Oracle Virtual Box. You can also use Hyper-v to create the vhd.
- After installing the virtualBox click on new button. You will get a dialogue box shown below.

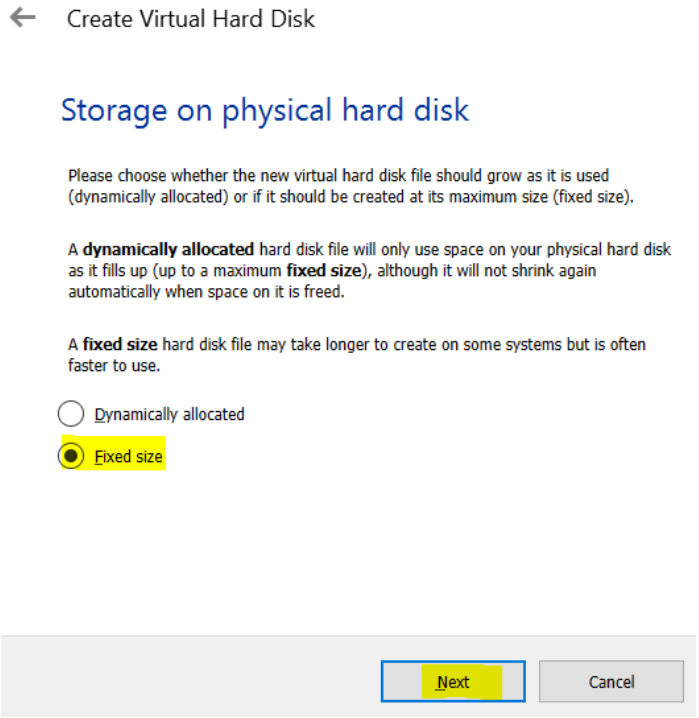


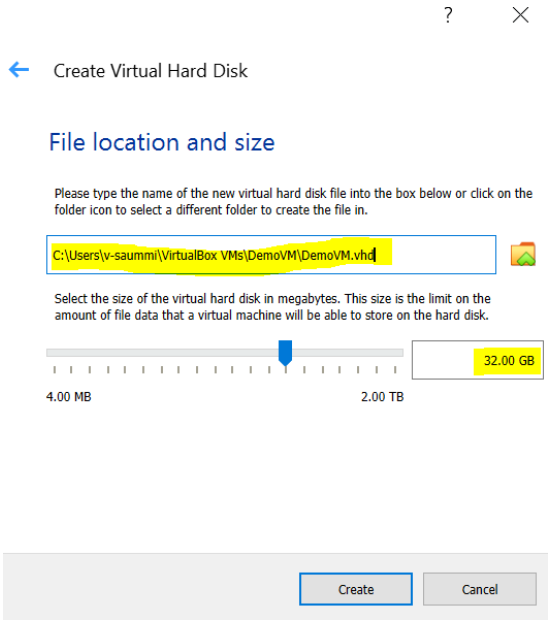
While creating the Virtual Machine you can choose the OS type (mac, windows or linux) and also version of the OS.

- Now its time to create the Harddisk for the above vm. Just click next on the above window and choose the hard disk configuration. Below are the screenshots of what you should choose.









Note : Copy the path where you have created the VHS and also the size should be a round up value rather than a decimal value. I am going with default in this.

Once you created the VHD. You must add this VHD to your storage account -> Blob in order to be able to reference to the blob while creating the VM image.