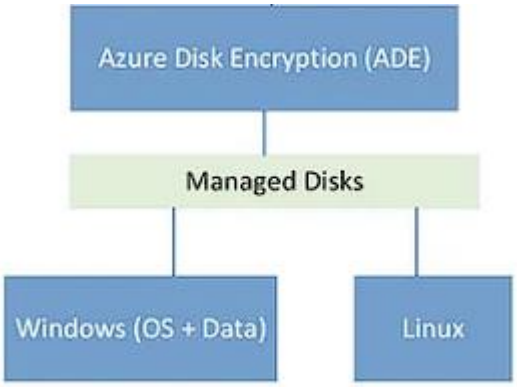
AZURE LAB 6 (ADE)

😁 AZURE DISK ENCRYPTION

Azure Disk Encryption is a feature in Microsoft Azure that helps protect and secure data on Azure Virtual Machines (VMs) by encrypting the operating system and data disks. It uses the BitLocker feature for Windows VMs and DM-Crypt for Linux VMs to perform the encryption. Here are some key points about Azure Disk Encryption:

1. **Encryption Process:** For Windows VMs, Azure Disk Encryption uses BitLocker to encrypt the OS and data disks. For Linux VMs, it uses DM-Crypt for encryption.
2. **Key Components:**
    a. **Key Vault:** Azure Disk Encryption stores encryption keys in Azure Key Vault, providing a centralized and secure location for key management.
    b. **Azure AD:** Azure Active Directory (Azure AD) is used for user authentication and authorization during the encryption process.
3. **Supported Operating Systems:** Azure Disk Encryption supports both Windows and Linux virtual machines.
4. **Prerequisites:** Before enabling Azure Disk Encryption, ensure that your VM is supported, and the operating system is compatible. You need to configure Azure Key Vault and set up an Azure AD application for authentication.
5. **Role Requirements:** The user enabling Azure Disk Encryption must have the necessary permissions, including access to the Key Vault and Azure AD.
6. **Encryption States:**
    Unencrypted: Disks are not encrypted.
    Encrypting: The encryption process is in progress.
    Encrypted: The disks are successfully encrypted.
7. **Monitoring and Management:** You can monitor the encryption process and status using Azure Monitor and Azure Security Center. Disk encryption can be managed through the Azure portal, Azure PowerShell, Azure CLI, and Azure Resource Manager (ARM) templates.
8. **Backup Considerations:** Ensure that you have a backup of critical data before enabling disk encryption, as the process involves resealing the VM.
9. **Performance Impact:** There may be a slight performance impact during the initial encryption process, but it is generally minimal.
10. **Virtual Machine Size Limitations:** Some VM sizes do not support Azure Disk Encryption. Check the documentation for the latest information on supported VM sizes.



Server-side Encryption (SSE) on Managed disks versus Azure Disk Encryption (ADE)

SSE encrypts data on disks but it DOES NOT have access to the operating system and applications. So, when SSE enabled managed disk is created, the disk is encrypted with a disk encryption key (DEK) that is managed by Azure. The DEK encrypts all the data on the disk, but not the OS and the application files. So even though OS and application files are residing on an encrypted disk, they are not themselves encrypted by DEK.

Operating System files are booting loader, kernel, system libraries, configuration files, registry keys, etc. Application files are executables, libraries, configuration files, data files, etc. Examples include binaries and configuration files for web servers like IIS, and Apache, database engines like SQL, MySQL, and messaging services like Kafka or RabbitMQ.

On the other hand, Azure Disk Encryption (ADE) enables encryption of the entire operating system and data disks for VMs, including temporary disks, and any additional disks. ADE uses a combination of BitLocker disk encryption and a customer-managed key stored in Azure Key Vault to encrypt and protect the data. This means that ADE can encrypt both the data at rest and the operating system and application files on the virtual machine.

You can use ADE and SSE together to provide end-to-end encryption for your data. When ADE and SSE are enabled together, the data is encrypted at the VM host level and then encrypted again at the storage account level. Together, it provides end-to-end encryption for your data and helps meet your compliance requirements.

TO BEGIN WITH THE LAB

STEP 1: CREATE A WINDOWS VIRTUAL MACHINE

1. The steps are same what you did in the previous labs while creating a windows virtual machine.

Create a virtual machine ...

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Free Trial

Resource group * : app-grp

Create new

Instance details

Virtual machine name * : WindowsVm

Region * : (Asia Pacific) Central India

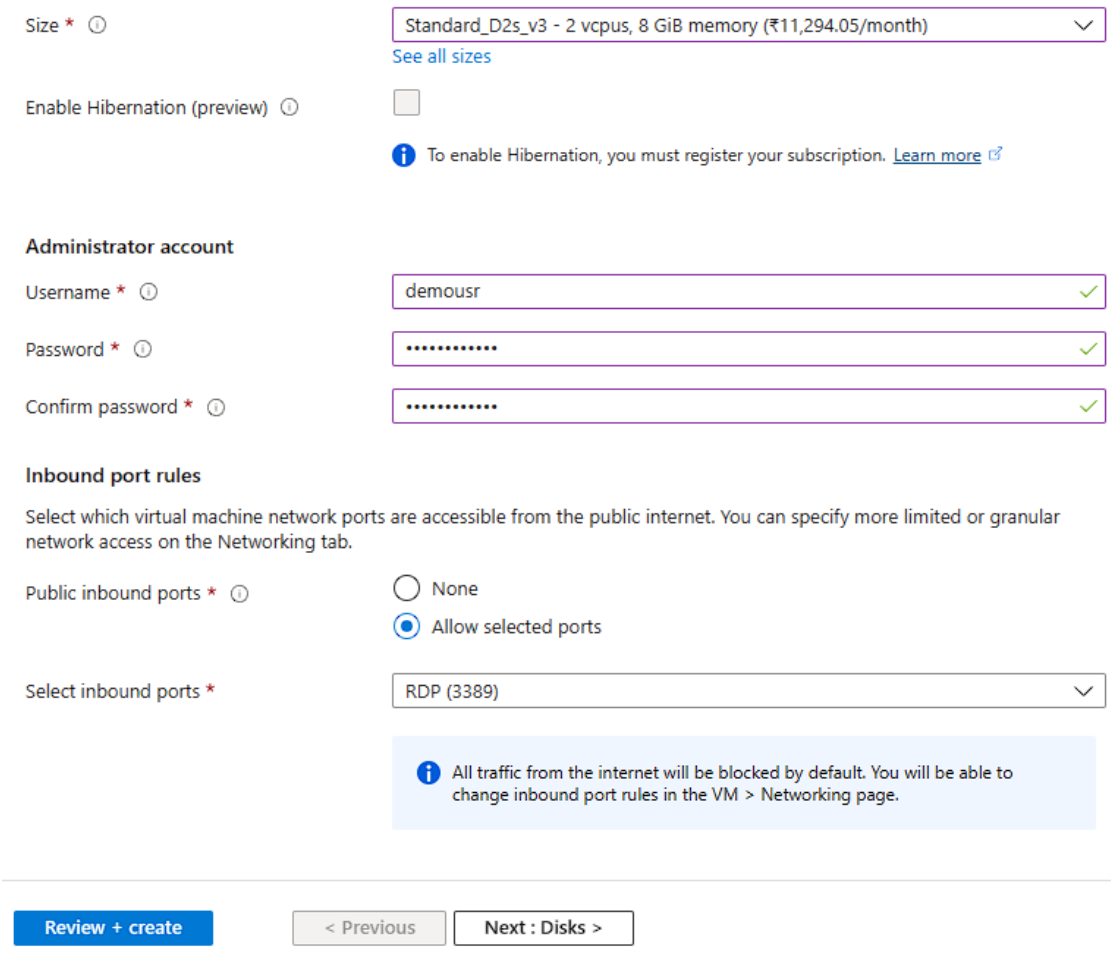
Availability options : No infrastructure redundancy required

Security type : Standard

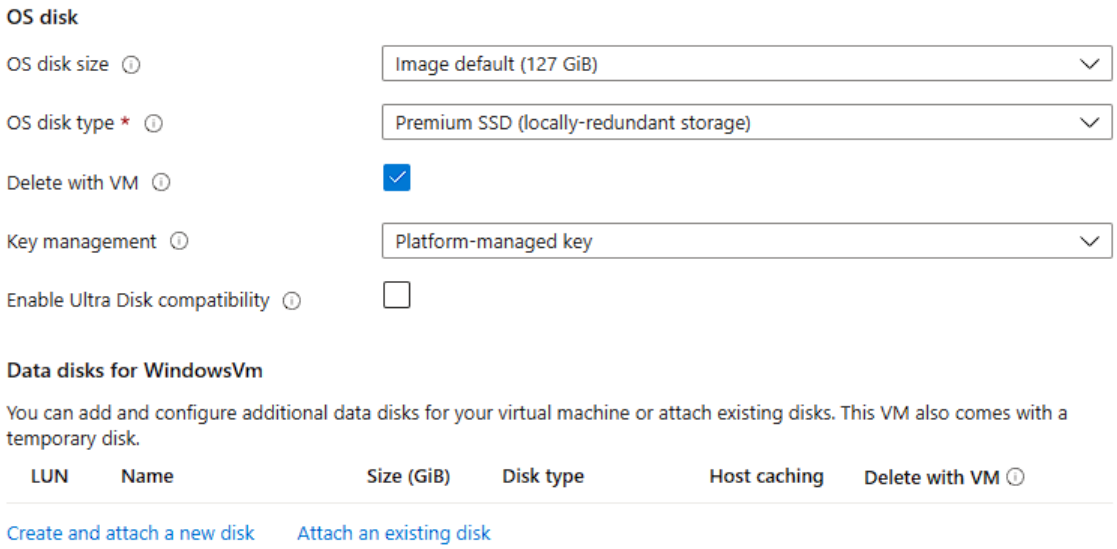
Image * : Windows Server 2022 Datacenter - x64 Gen2 (free services eligible)

See all images | Configure VM generation

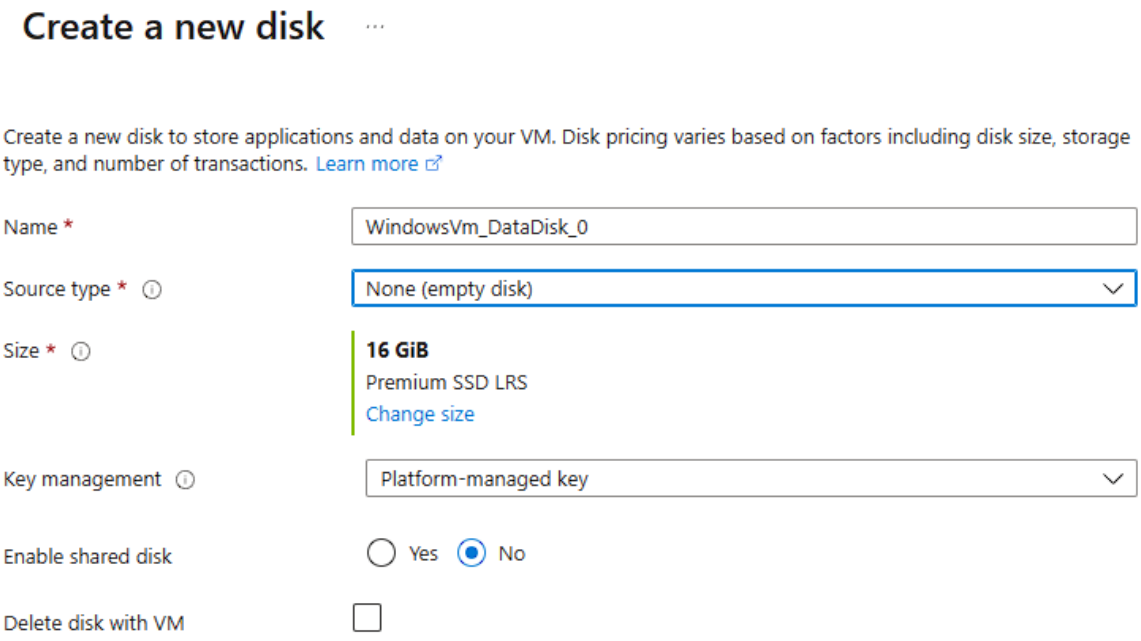
This image is compatible with additional security features. Click here to swap to the Trusted launch security type.



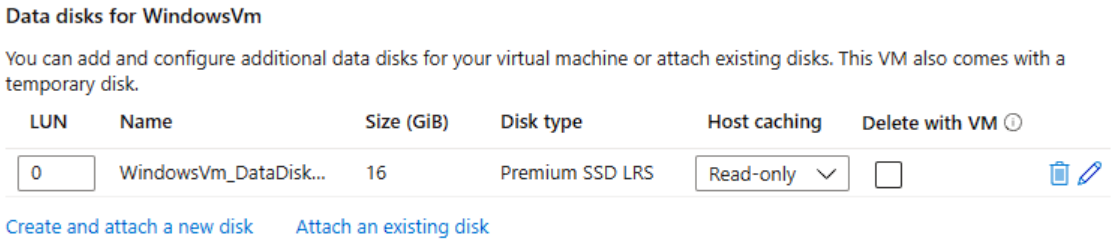
2. Click on next, on the disk option click on create and attach a new disk.



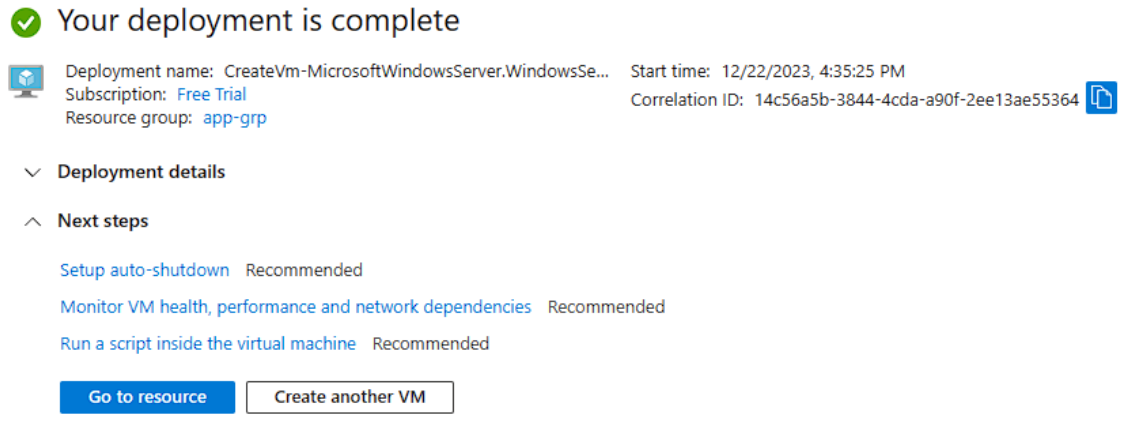
3. Select the options below for the new disk. Then click on Ok.



4. Here you can see that your disk has been created.



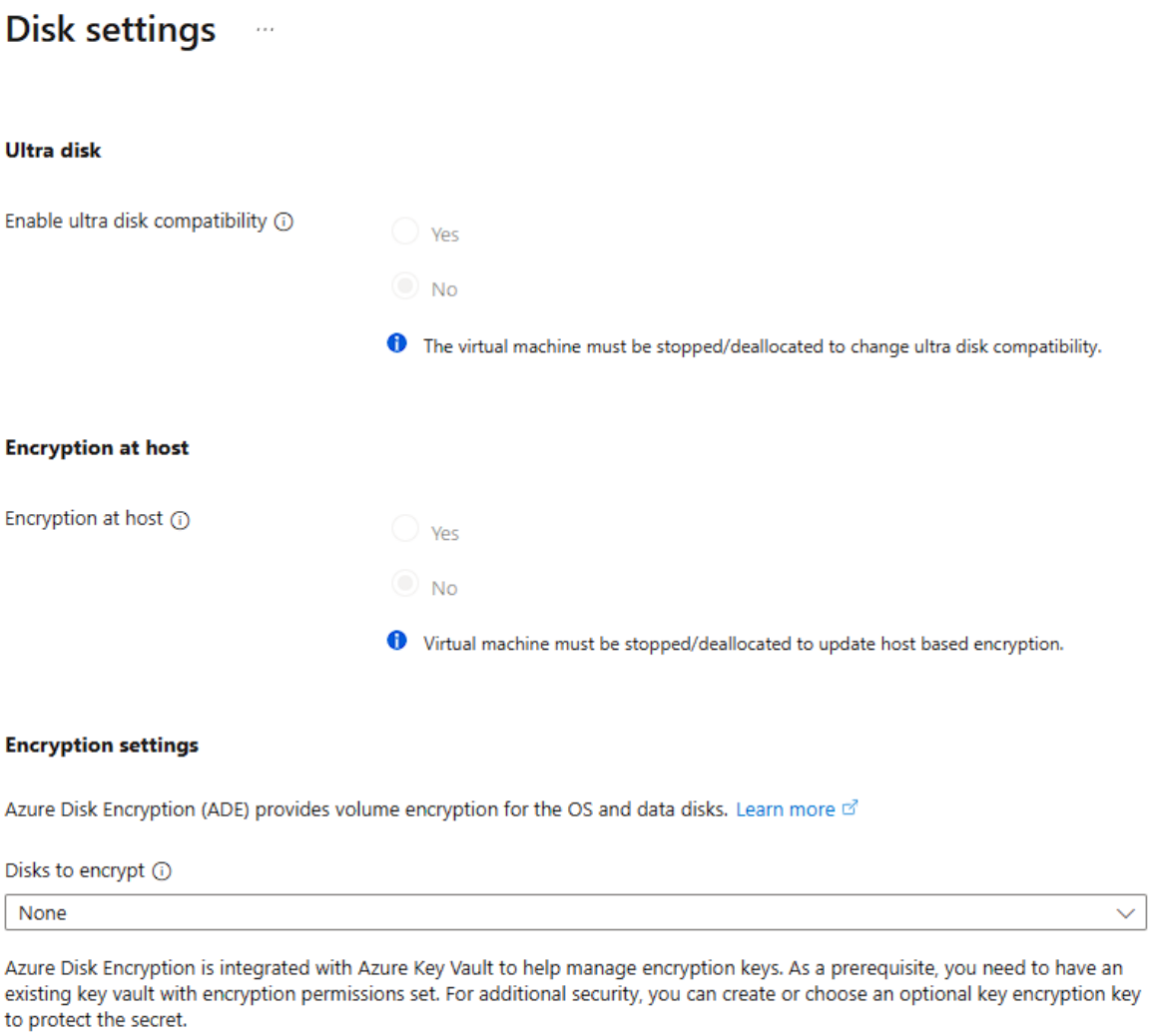
5. Now directly jump to the review and create page. There just create your virtual machine.
6. Once the deployment is complete, click on go to resources.



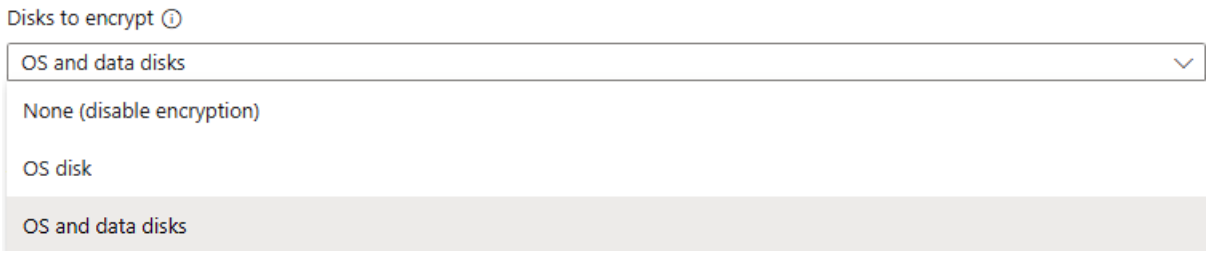
7. In the resource, from the left side in the settings menu, select disks.

8. On the disks page click on additional settings.
9. Last time around, when you were working with server-side encryption, you had to create something known as a disk encryption set. And then you had to go on to each individual disk. And if you want to use basically customer managed keys, you could associate that disk encryption set with the disk in terms of encryption settings.

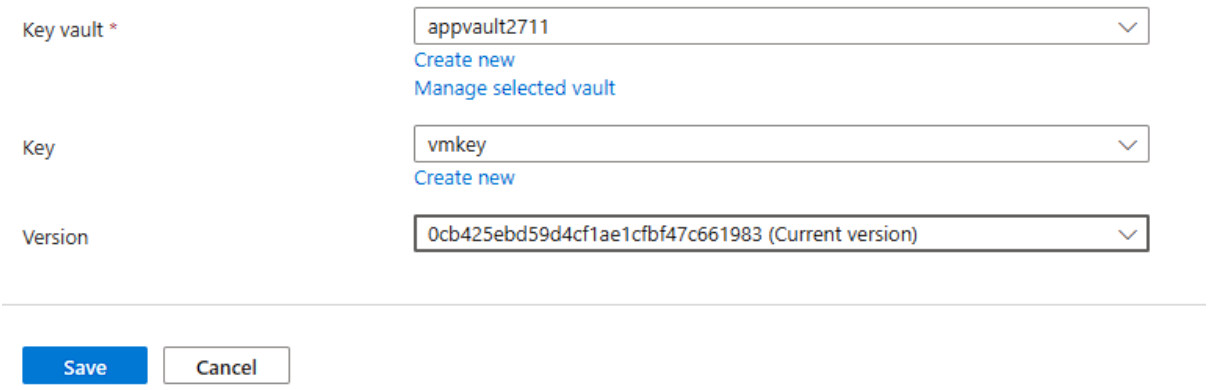
10. These are disk settings from where you can add encryption.



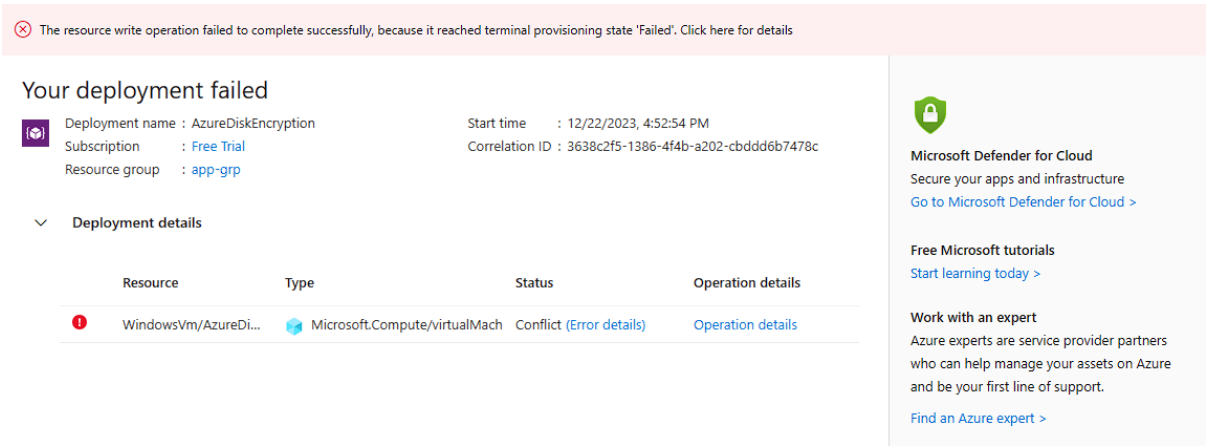
11. So, click on disks to encrypt, then select OS and data disks.



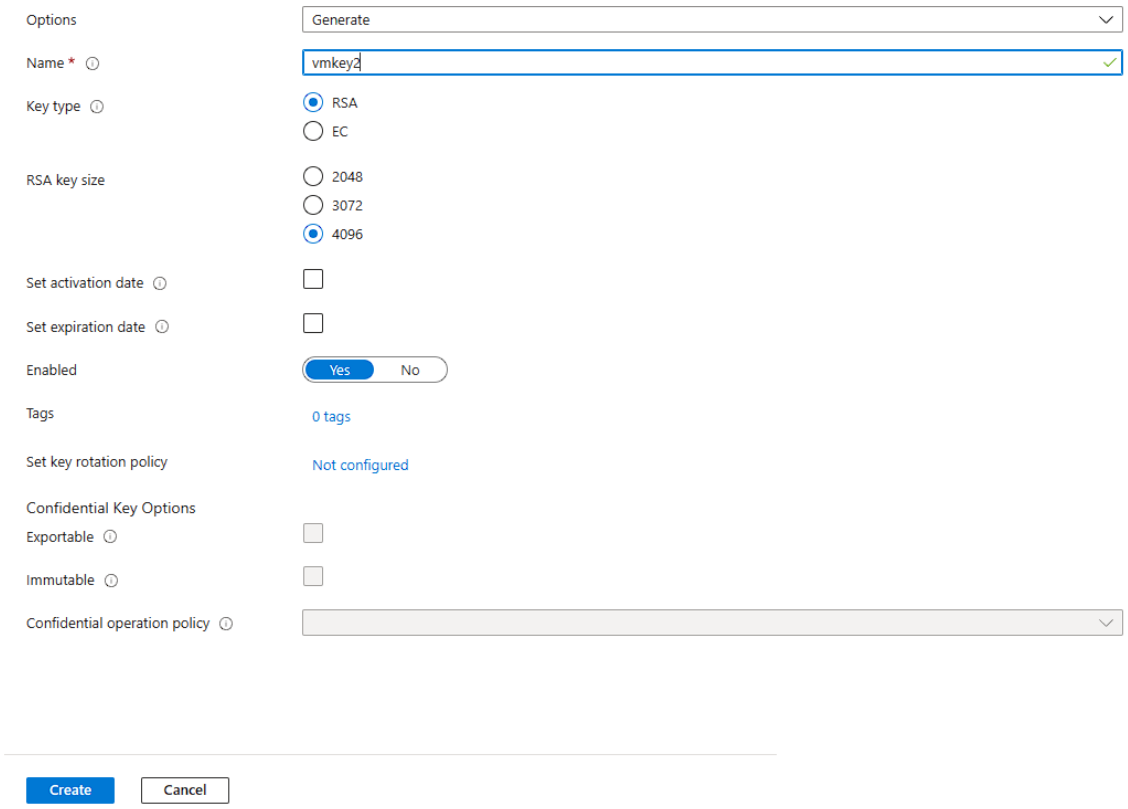
12. Then after, select your key vault, and select your existing key, which you created during the last lab. It will automatically pick version. Then click on save.



13. Once you've click on save option, it will start to deploy and you might get this message that the deployment failed.



14. This error occurred because the existing key you are using, its size is not compatible with the disks.
15. So, to make it work you need create a new, for that navigate to key vault, then go to keys and click on generate/import.
16. Here give it a name and just change its key size from 2048 to 4096 and create your key.



17. Once your key is created, go back to the virtual machine and try again to encrypt your disks with the new key.
18. You will see that your disks are now encrypted.