Azure Windows and Linux Disk Encryption

**Azure Windows and Linux Disk Encryption**

Contributor

Kash

28/01/20

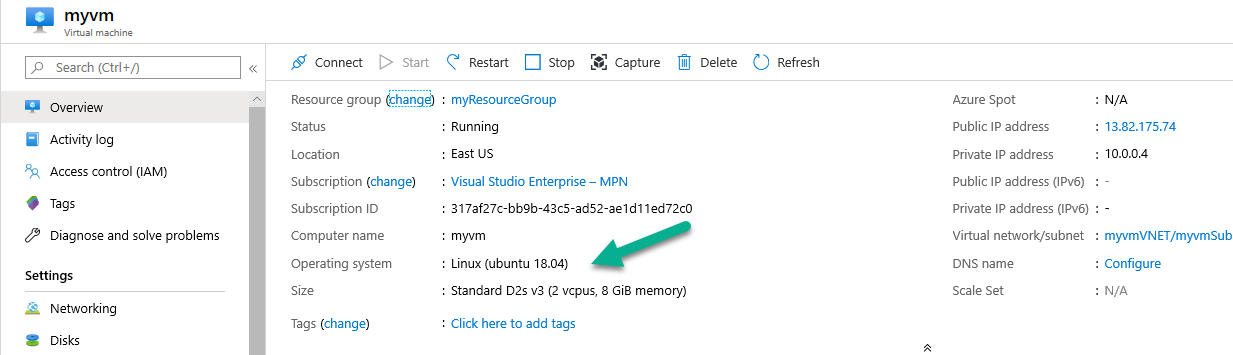
The purpose of this document is to describe how to encrypt Windows and Linux virtual machines in Azure using AZ Command line interface, Azure Powershell and Azure Portal, this will include methods, scripts, command execution with print screens.

Imp: Make sure take snapshot of disks or full backup of vms before proceeding.

In this scenario I have deployed two VMs one is Linux Ubuntu and second one is Windows 2016 data centre

Encrypting disks in Linux virtual machines using Azure CLI

Create a resource group



#### create a resource group###

az group create --name "myResourceGroup" --location "eastus"

### creating a keyvault

## This creation of vault will enable automatically enable for disk encryption and access policies.

az keyvault create --name "kashlinuxvault" --resource-group "myResourceGroup" --location "eastus" --enabled-for-disk-encryption

#### creating key in keyvault key

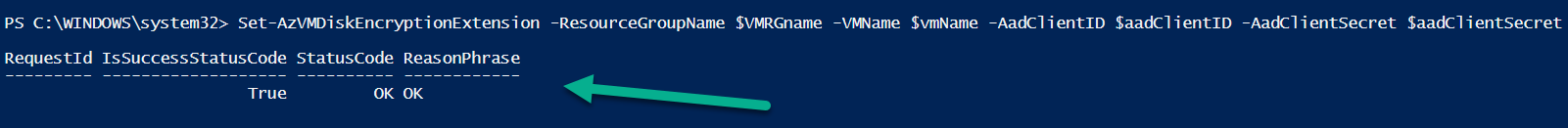
az keyvault key create --vault-name kashlinuxvault --name mykey --protection software

az vm create --resource-group myResourceGroup --name "myvm1" --image UbuntuLTS --size Standard\_D2s\_v3 --generate-ssh-keys

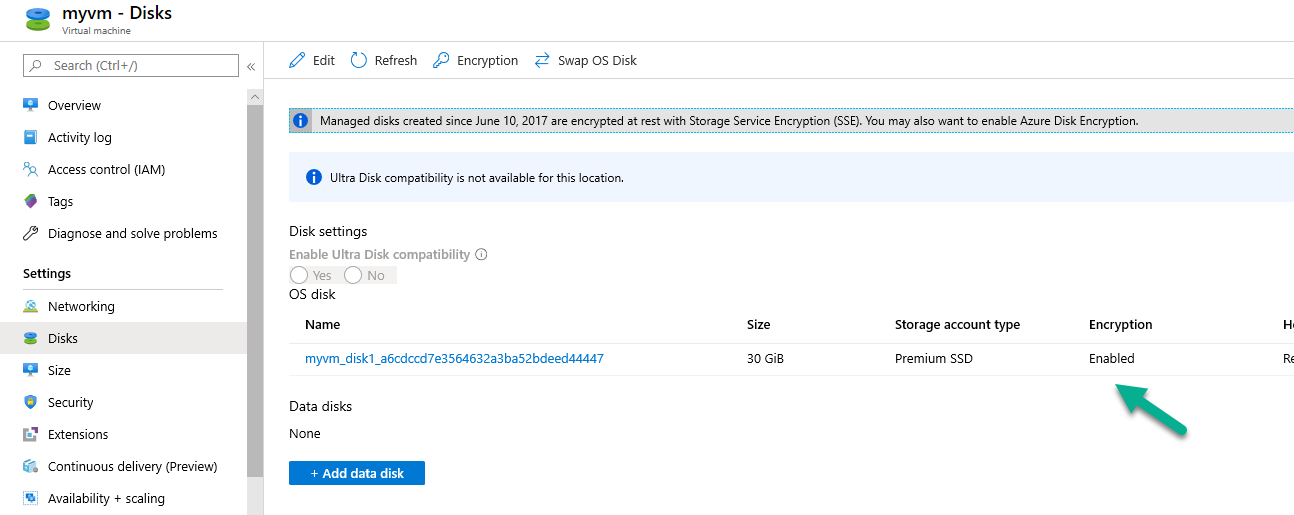
az vm encryption enable --name myvm --resource-group myResourceGroup --disk-encryption-keyvault kashlinuxvault --key-encryption-key mykey –volume -type ALL

## to check linux vm is encrypted

az vm show --name kashvm1 --resource-group kashrg







Encrypting Linux virtual disk in using powershell

Before we run this script below

1. Need a service principal app and this app should be authenticated in Azure Active Directory.
2. Key Vault creation, make sure it should be in the same region where VM is provisioned.
3. Key secret creation.
4. Need application id.
5. Need secret.

See the script below.

##Access policy

$keyVaultName = 'kashlinuxvault'

$aadClientID = '8557b9c5-2f43-434f-a138-f8587c32f20c'

$rgname = 'myResourceGroup'

Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ServicePrincipalName $aadClientID -PermissionsToKeys 'WrapKey' -PermissionsToSecrets 'Set' -ResourceGroupName $rgname

## 2nd step

$sequenceVersion = [Guid]::NewGuid();

$KVRGname = 'myresourcegroup';

$VMRGName = 'myresourcegroup';

$vmName = 'myvm1';

$aadClientID = '8557b9c5-2f43-434f-a138-f8587c32f20c';

$aadClientSecret = '5L-rOFI425gWroHkfA.Bm[\_Gg1/7sfwd';

$KeyVaultName = 'kashlinuxvault';

$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGname;

$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;

$KeyVaultResourceId = $KeyVault.ResourceId;

# 3rdstep

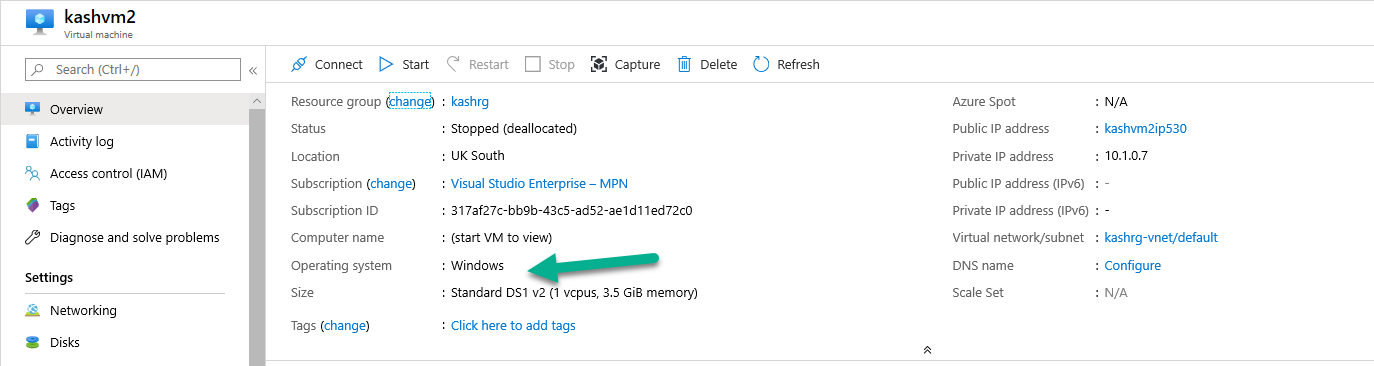
Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName -AadClientID $aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId $KeyVaultResourceId -VolumeType 'all' –SequenceVersion $sequenceVersion -SkipVmBackup ;

When encrypting Linux machines we need to use -SkipVMBackup parameter otherwise it will fail.

Encrypting Windows virtual machines

Exactly the same process as above using Azure powershell.

I have used similar script as above for my windows virtual machine and see the results below after encryption the only thing we do not have to use -SkipVmBackup parameter for windows machines.



After encryption

