

How to enable Disk Encryption on Azure VM (BitLocker/DM-Crypt)

Azure Disk Encryption is a capability that helps you encrypt your Windows and Linux IaaS VM disks. When you apply the Disk Encryption management solution, you can satisfy the following business needs:

- IaaS VMs are secured at rest by using industry-standard encryption technology to address organizational security and compliance requirements.
- IaaS VMs boot under customer-controlled keys and policies. You can audit their usage in your key vault.

Since Azure has recently supports DR for Azure Disk Encryption-enabled VMs [Link](#). To enable disk encryption, we need to leverage Azure AD App and Azure Key Vault service from Azure which help in encryption and decryption.

Prerequisites:

- Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted. [Link](#)
- Encrypting or disabling encryption may cause the VM to auto-reboot once.

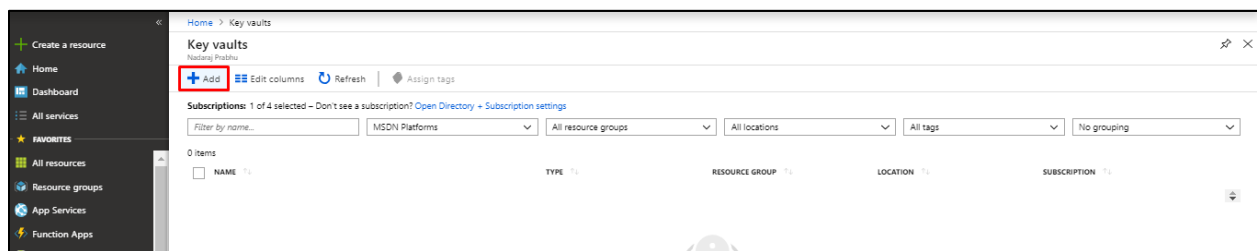
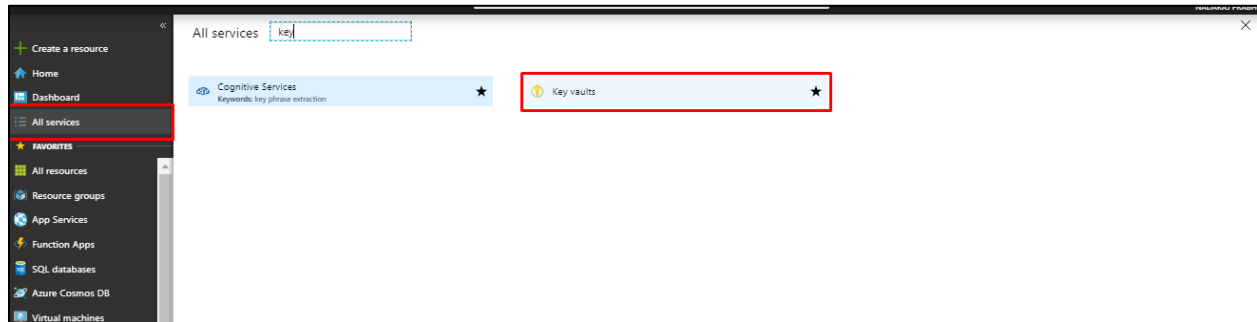
Summary:

Below are the steps we need to perform to enable encryption for disks in Azure VM:

1. Create a key vault.
2. Set the key vault access policy.
3. Set key vault advanced access policies.
4. Run PowerShell script to enable encryption (since enabling encryption from portal is not yet available)

Create an Azure Key Vault and provide appropriate permission

Step 1: Go to “Azure Key Vault” and click on new “key Vault”.



Step 2: Enter the following details and click on “Create”

Name: *Azure Key Vault Name*

Subscription: Select the subscription

Resource Group: *Any resource group*

Location: Any location

Pricing Tier: *Standard/Premium*

Access Policy: Need to select appropriate policy as mentioned in next Step.

Virtual Network Access: Select any or appropriate virtual network where the VM is located

Home > Key vaults > Create key vault

Key vaults
Nadaraj Prabhu

+ Add Edit columns More

Filter by name...

NAME

No key vaults to display
Try changing your filters if you don't see what you're looking for.

Create key vault

Create key vault

* Name vmcyphekeys ✓

* Subscription MSDN Platforms

* Resource Group Dev-RG
[Create new](#)

* Location East US

Pricing tier Standard >

Access policies
1 principal selected >

Virtual Network Access
All networks can access. >

Create Automation options

Step 2: Select the access policy and enter the following details and click on “ok”.

Configure from templet: Select “Key & Secret Management”

Key Permission: Select “Decrypt, Encrypt, unwrap key, wrap key, verify”

Key Permission: No need to change (applied from “key & secret Management” templet)

Certificate Permission: No need to change (applied from “key & secret Management” templet)

Create key vault

Name

vmcypkerkeys

Subscription

MSDN Platforms

Resource Group

Dev-RG

Location

East US

Pricing tier

Standard

Access policies

1 principal selected

Virtual Network Access

All networks can access.

CreateAutomation options

Access policies

Click to show advanced access policies

Add new

Nadaraj Prabhu

USER (Directory ID: 0a...

OK

Add access policy

Add a new access policy

Configure from template (optional)

Key & Secret Management

Select principal

Bitlocker-AppID

Key permissions

9 selected

Secret permissions

7 selected

Certificate permissions

0 selected

Authorized application

None selected

OK

Principal

Select a principal

Invite

Select

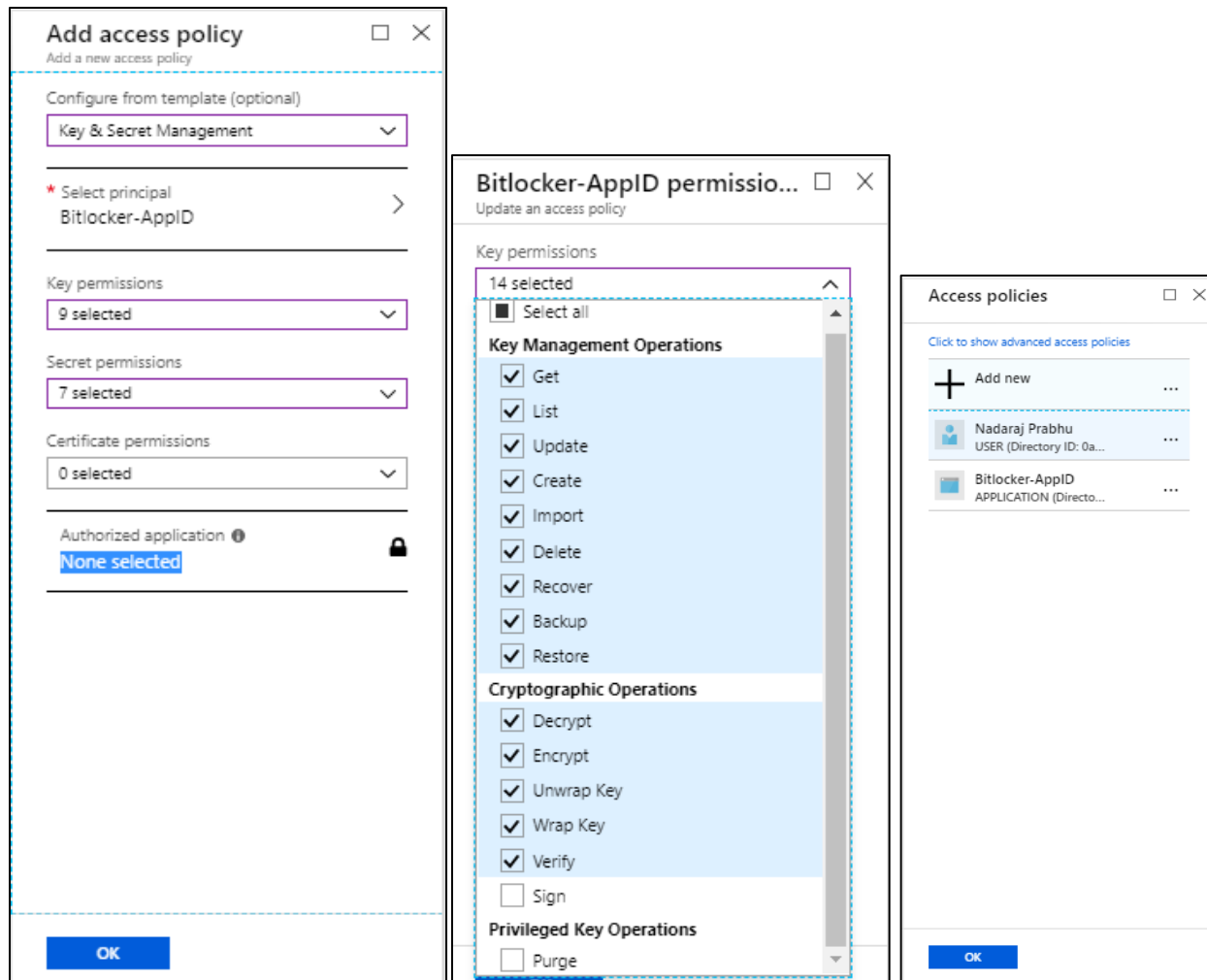
bitlocker

Bitlocker-AppID

Selected

Bitlocker-AppID

Select



Step 3: After configuration click on “create”. Now wait for the deployment to succeed.

Home > Key vaults > Create key vault

Key vaults

Nadaraj Prabhu

+ Add Edit columns More

Filter by name...

NAME

No key vaults to display

Try changing your filters if you don't see what you're looking for.

Create key vault

Create key vault

* Name vmcypkerkeys ✓

* Subscription MSDN Platforms

* Resource Group Dev-RG

Create new

* Location East US

Pricing tier Standard

Access policies 1 principal selected

Virtual Network Access All networks can access.

Create Automation options

Step 4: After the key vault deployment, go the created key vault.

Home > Key vaults

Key vaults

Nadaraj Prabhu

+ Add Edit columns Refresh Assign tags

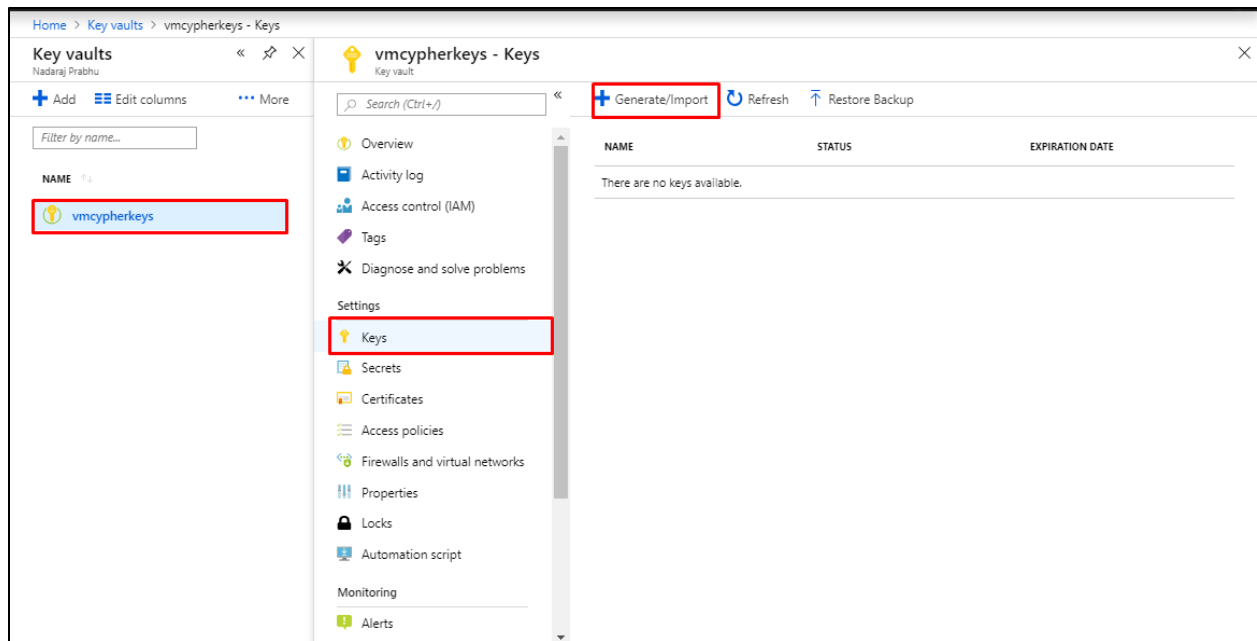
Subscriptions: 1 of 4 selected – Don't see a subscription? [Open Directory](#) • [Subscription settings](#)

Filter by name... MSDN Platforms All resource groups All locations All tags No grouping

1 items

	NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION	
<input type="checkbox"/>	vmcypkerkeys	Key vault	Dev-RG	East US	MSDN Platforms	...

Step 5: Next create a key, go to “Keys” blade in key vault and click on “Generate/import”



Step 6: Enter the following details to create a key and click on “create”

Option: “Generate”

Name: Give a name for the key which will be used in `$KeyVaultKey` parameter.

Key Type: “RSA”

RSA Key Size: “2048” (Standard)

Set activation Date: Set a date mostly today.



Set expiration Date: Set a key expiry date (Not mandatory, but most of the organization has the policy on changing key every year or the time which is set by their governance team)


Enabled: “Yes”

Home > Key vaults > vmcypherkeys - Keys > Create a key


Create a key


Options
Generate

* Name 
Bitlocker-Key 

Key Type 
RSA EC

RSA Key Size
2048 3072 4096

Set activation date?  ☐

Set expiration date?  ☐

Enabled? Yes No

Create

Step 7: Once the key is created check it under keys to confirm its status, activation date by selecting them.

Home > Resource groups > Dev-RG > vmcypherkeys - Keys > Bitlocker-Key

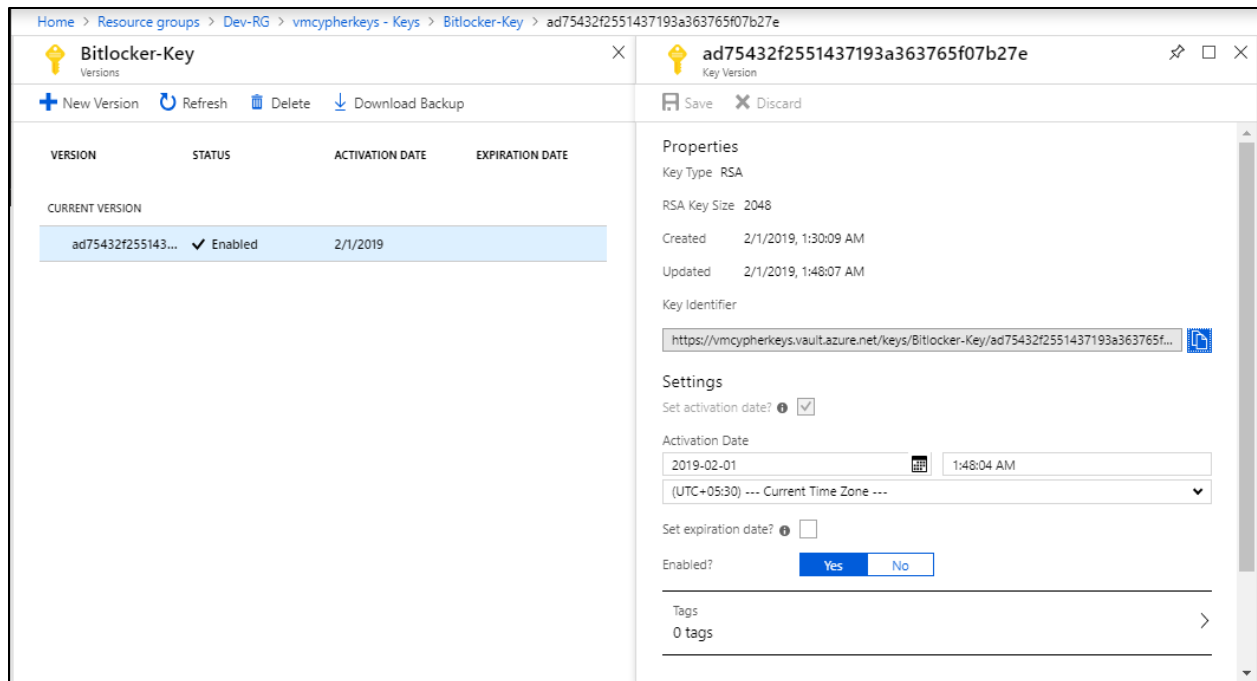
vmcypherkeys - Keys
Key vault

Search (Ctrl+/)

+ Generate/Import Refresh Restore Backup

NAME	STATUS	EXPIRATION DATE
Bitlocker-Key	✓ Enabled	

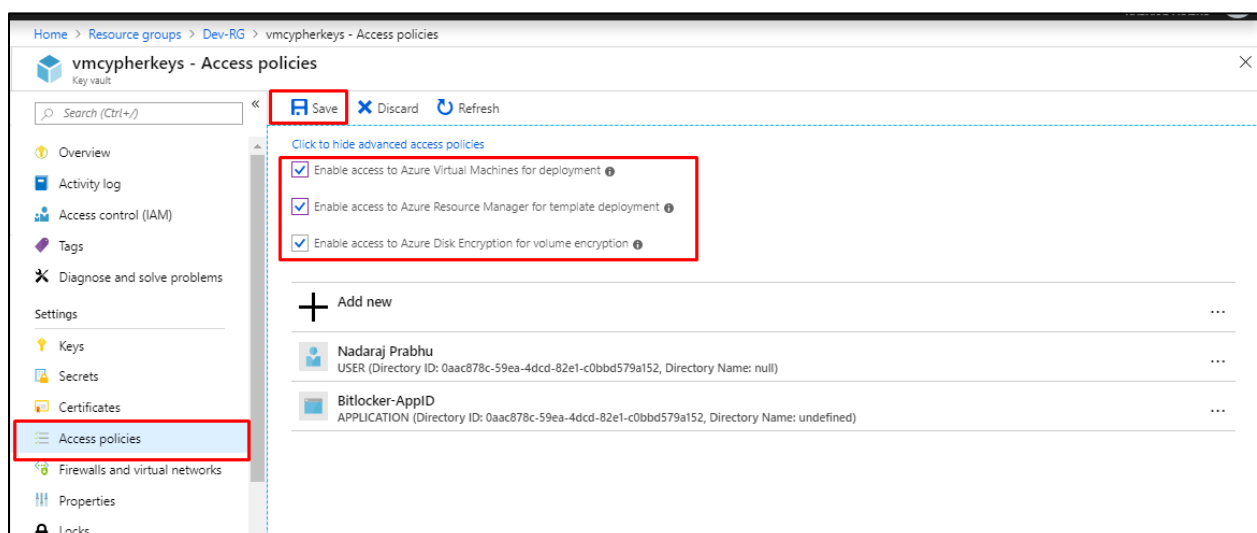
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Keys
Secrets
Certificates
Access policies
Firewalls and virtual networks

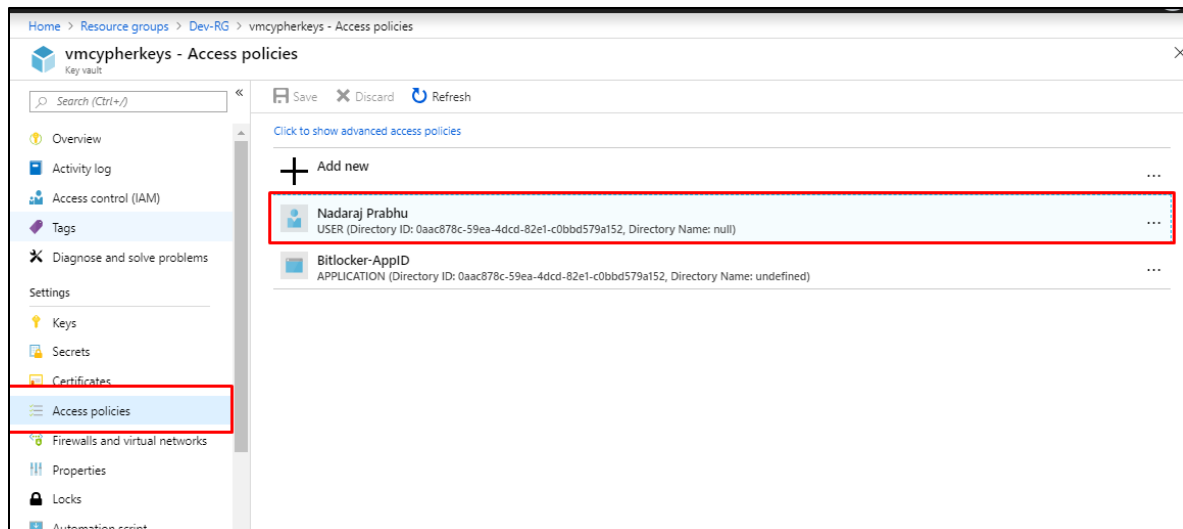


Step 8: Go to Access Policies in key vault. Under “show advanced access policy” there will be 3 options:

1. Enable access to Azure Virtual Machine for deployment (**Check this if you have enabled ASR, else let it be unchecked**)
2. Enable access to Azure Resource Manager for templet deployment (**Check this if you have enabled ASR, else let it be unchecked**)
3. Enable access to Disk Encryption for volume encryption. (**check this box to allow volume/disk encryption**)

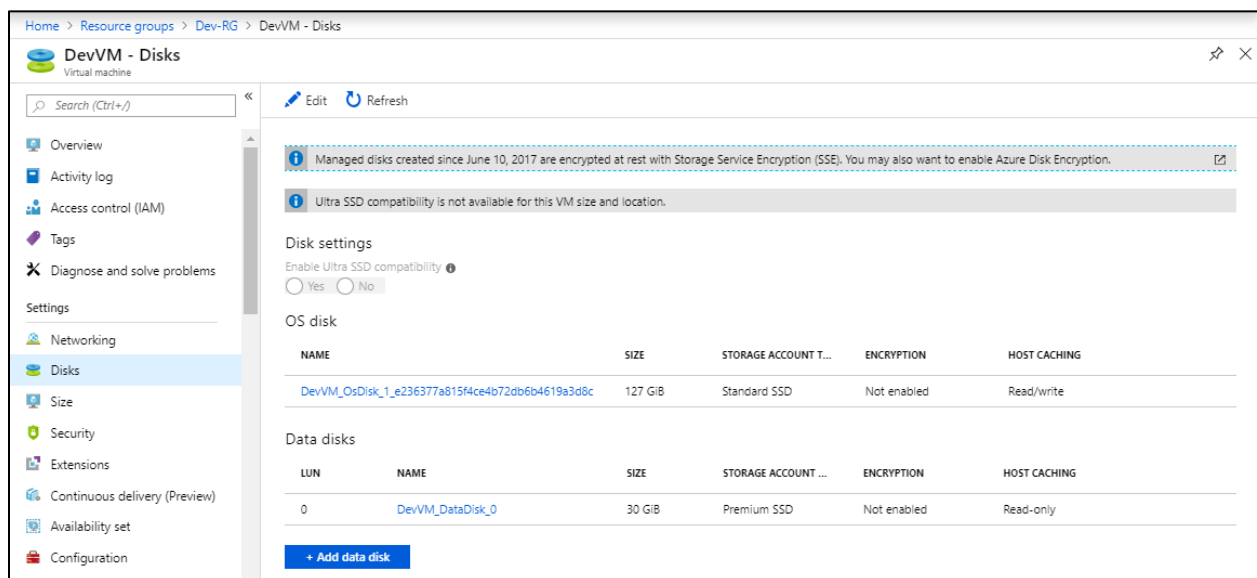
Note: ASR replication supports encrypted disk which was not the case earlier. [Link](#)





Note: Add yourself/ the user that requires the permission to access the policy

Step 9: Go to your Azure VM, under disk check for “encryption status”



Encrypt disk on Azure VM

Step 1: Download the attached PowerShell file, open it in PowerShell ISE or your favorite editor and change the parameters as mentioned: [Script Link](#)



VM_DiskEncrypt.ps
1

Note : Make sure you have installed Azure RM module [Link](#)

\$SubName - Subscription Name
\$KeyVaultrgName - Key Vault Resource Group Name
\$VMrgName - Resource Group Name
\$VMs - VM Name
\$aadClientID - Azure AD App's Application ID
\$clientSecret - Secret key created on Azure AD App
\$KeyVaultName - Azure Key vault Name
\$KeyVaultKey - Name of the key in the Key vault

Note: you can run encryption for multiple VM in same resource group like show below:

```
$VMs += "Dev1VM"  
$VMs += "Dev2VM"  
$VMs += "Dev3VM"
```

```

<#
*****Note*****
Replace the parametes before executing

by Nadaraj Prabhu

$SubName      - Subscription Name
$KeyVaultrgName - Key Vault Resource Group Name
$VMrgName     - Resource Group Name
$VMs          - VM Name

you can add multiple VM in same resource group:

$VMs += "Dev1VM"
$VMs += "Dev2VM"
$VMs += "Dev3VM"

#>
$SubName = "your Subscription name"
$KeyVaultrgName = 'Dev-RG';
$VMrgName = 'Dev-RG';
$VMs = @()
$VMs += "DevVM"

<#
$aadClientID - Azure AD App's Application ID
$clientSecret - Secret key created on Azure AD App
#>
$aadClientID = 'd3asdfd-0033-4e1d-a264-ef8cef90a944'
$clientSecret = 'mzGyW!SDAS33s:AzB1JH5[1PAE2@NzPTTL@r=7?zBmv01VeRN$GLButgjb]'

<#
$KeyVaultName - Azure Key vault Name
$KeyVaultKey - Name of the key in the Key vault
#>

$KeyVaultName = 'vmcypherkeys';
$KeyVaultKey = 'Bitlocker-Key';

```

```

25 $aadClientID - Azure AD App's Application ID
26 $clientSecret - Secret key created on Azure AD App
27 #>
28 $aadClientID = 'd3asdfd-0033-4e1d-a264-ef8cef90a944'
29 $clientSecret = 'mzGyW!SDAS33s:AzB1JH5[1PAE2@NzPTTL@r=7?zBmv01VeRN$GLButgjb]'
30
31 <#
32 $KeyVaultName - Azure Key vault Name
33 $KeyVaultKey - Name of the key in the Key vault
34 #>
35
36 $KeyVaultName = 'vmcypherkeys';
37 $KeyVaultKey = 'Bitlocker-Key';
38
39 Login-AzureRmAccount
40 Select-AzureRmSubscription -SubscriptionName $SubName
41
42 $KeyVault = Get-AzureRmKeyVault -VaultName $KeyVaultName -ResourceGroupName $KeyVaultrgName;
43 $diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
44 $KeyVaultResourceId = $KeyVault.ResourceId;
45 $sequenceVersion = [Guid]::NewGuid();
46 $KEK = Get-AzureKeyVaultKey -VaultName $KeyVaultName -Name $KeyVaultKey
47 $KeyEncryptionKeyUrl = $KEK.Key.kid;
48
49
50 #Script to enable Azure Disk Encryption
51 foreach ($VMName in $VMs) {
52 Set-AzureRmVMDiskEncryptionExtension -VMName $VMName -ResourceGroupName $VMrgName -AadClientID $aadClientID -AadClientSecret $clientSecret -DiskEncryption
53 };

```

Step 2: Now run the PowerShell command. You will be prompted twice to confirm and proceed with the VM encryption. Select “Yes to All” both the times.

Note: During this process VM will reboot automatically.

```

VM_DiskEncryption.ps1 X
1 Login-AzureRmAccount
2 Select-AzureRmSubscription -SubscriptionName 'MSDN Platforms'
3 $rgName = 'Dev-RG';
4 $aadClientID = 'd3add78-0033-4e1d-a264-ef8cef90a944'
5 $clientSecret = 'mzGyw!@61f0_vD:AzB1JH5[1PAE2@NzPTTL@r=7?zBmv01VeRN$GLButgjb]'
6
7 $keyVaultName = 'vmcypherkeys';
8 $keyVaultKey = 'Bitlocker-Key';
9 $keyVault = Get-AzureRmKeyVault -VaultName $keyVaultName -ResourceGroupName $rgName;
10 $diskEncryptionKeyVaultUri = $keyVault.VaultUri;
11 $keyVaultResourceId = $keyVault.ResourceId;
12 $sequenceVersion = [Guid]::NewGuid();
13 $KEK = Get-AzureKeyVaultKey -VaultName $keyVaultName -KeyIdentifier $keyVaultResourceId -KeyVersion $sequenceVersion;
14
15 ;

```

Confirm
Continue with this operation?

Yes Yes to All Halt Command Suspend

Name Account Environment TenantId
MSDN Platforms (103ab456-30f8-4509-a5... nadaraj1527@gmail.com MSDN Platforms AzureCloud 0aac878c-59ea-4dcd-8...

DEBUG: 1:51:56 AM - SetAzureDiskEncryptionExtensionCommand begin processing with ParameterSet 'AADClientSecretParameterSet'.

```

VM_DiskEncryption.ps1 X
1 Login-AzureRmAccount
2 Select-AzureRmSubscription -SubscriptionName 'MSDN Platforms'
3 $rgName = 'Dev-RG';
4 $aadClientID = 'd3add78-0033-4e1d-a264-ef8cef90a944'
5 $clientSecret = 'mzGyw!@61f0_vD:AzB1JH5[1PAE2@NzPTTL@r=7?zBmv01VeRN$GLButgjb]'
6
7 $keyVaultName = 'vmcypherkeys';
8 $keyVaultKey = 'Bitlocker-Key';
9 $keyVault = Get-AzureRmKeyVault -VaultName $keyVaultName -ResourceGroupName $rgName;
10 $diskEncryptionKeyVaultUri = $keyVault.VaultUri;
11 $keyVaultResourceId = $keyVault.ResourceId;
12 $sequenceVersion = [Guid]::NewGuid();
13 $KEK = Get-AzureKeyVaultKey -VaultName $keyVaultName -KeyIdentifier $keyVaultResourceId -KeyVersion $sequenceVersion;
14
15 ;

```

Confirm
Are you sure you want to perform this action?
Performing the operation "Enable disk encryption" on target "DevVM".

Yes Yes to All No No to All Suspend

Name Account Environment TenantId
MSDN Platforms (103ab456-30f8-4509-a5... nadaraj1527@gmail.com MSDN Platforms AzureCloud 0aac878c-59ea-4dcd-8...

DEBUG: 1:51:56 AM - SetAzureDiskEncryptionExtensionCommand begin processing with ParameterSet 'AADClientSecretParameterSet'.
DEBUG: 1:52:51 AM - using account id 'nadaraj1527@gmail.com'...

Step 3: Now let the PowerShell run (execution of enabling the encryption is based on the disk size and disk type). Meanwhile the encryption is running you can go to you VM in portal and verify the disk encryption status.

Home > Resource groups > Dev-RG > DevVM - Disks

DevVM - Disks
Virtual machine

Search (Ctrl+/)

Edit Refresh

Updating

Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption.

Ultra SSD compatibility is not available for this VM size and location.

Disk settings

Enable Ultra SSD compatibility

Yes No

OS disk

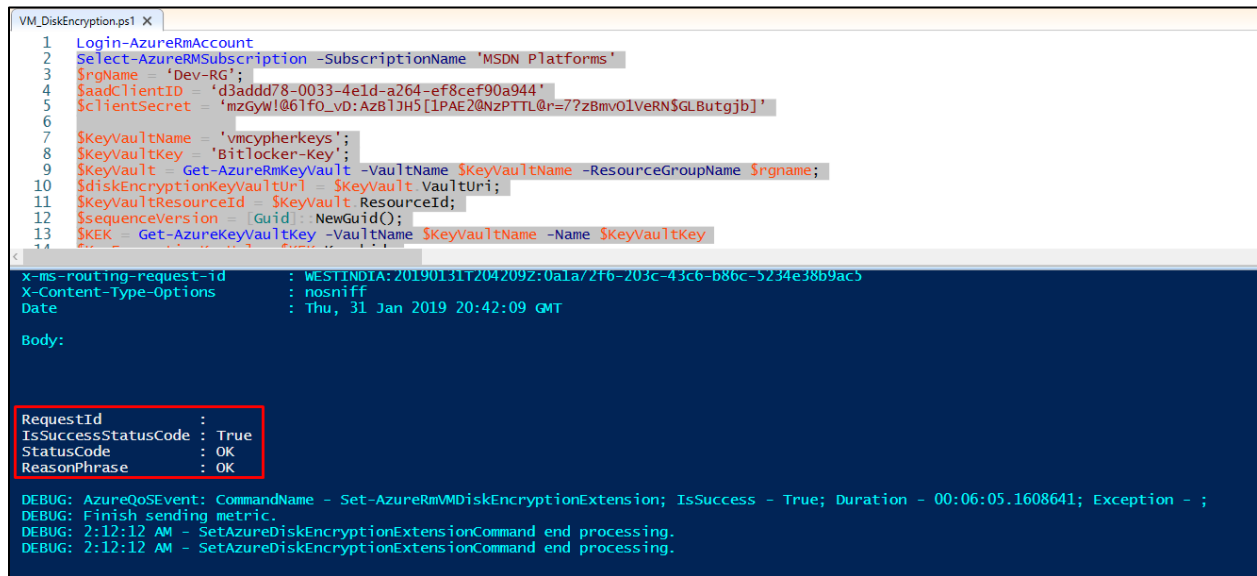
NAME	SIZE	STORAGE ACCOUNT T...	ENCRYPTION	HOST CACHING
DevVM_OsDisk_1_e236377a815f4ce4b72db6b4619a3d8c	127 GiB	Standard SSD	Enabled	Read/write

Data disks

LUN	NAME	SIZE	STORAGE ACCOUNT ...	ENCRYPTION	HOST CACHING
0	DevVM_DataDisk_0	30 GiB	Premium SSD	Enabled	Read-only

Step 4: After the successful enabling the encryption, you should be able to see the status as mentioned below:

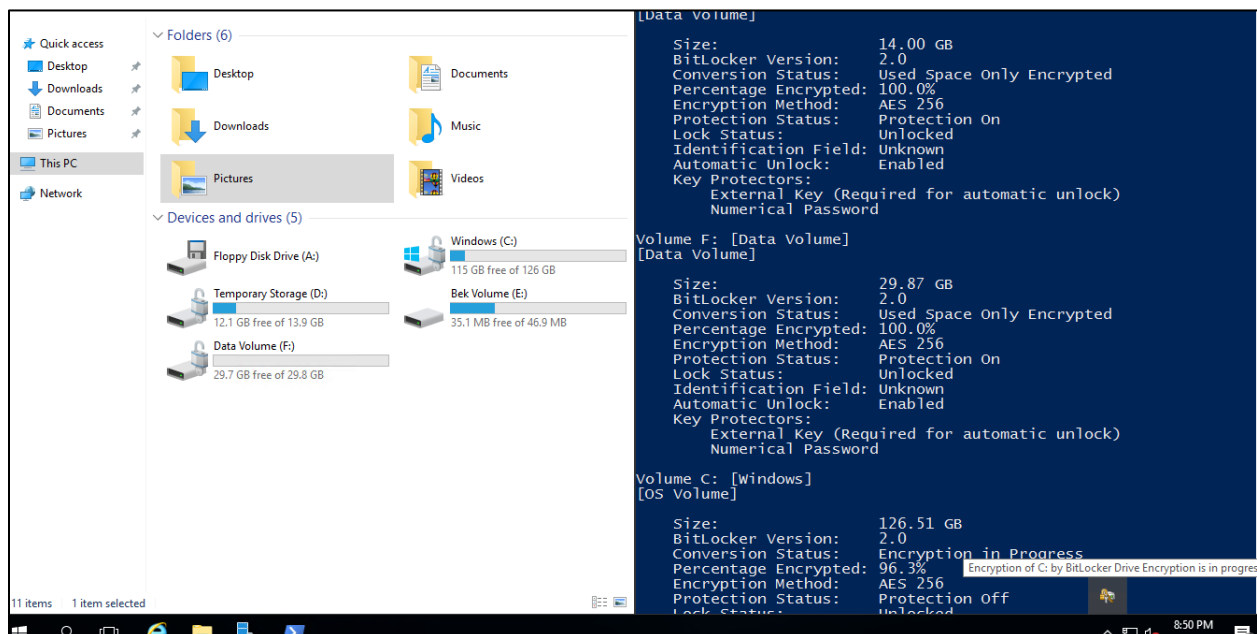
```
RequestId      :  
IsSuccessStatusCode : True  
StatusCode      : OK  
ReasonPhrase    : OK
```



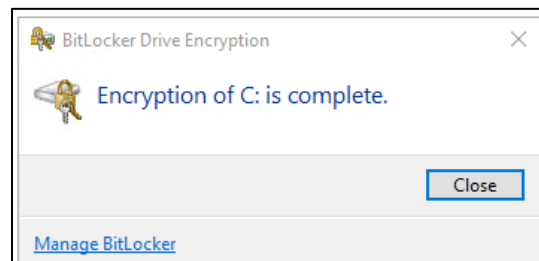
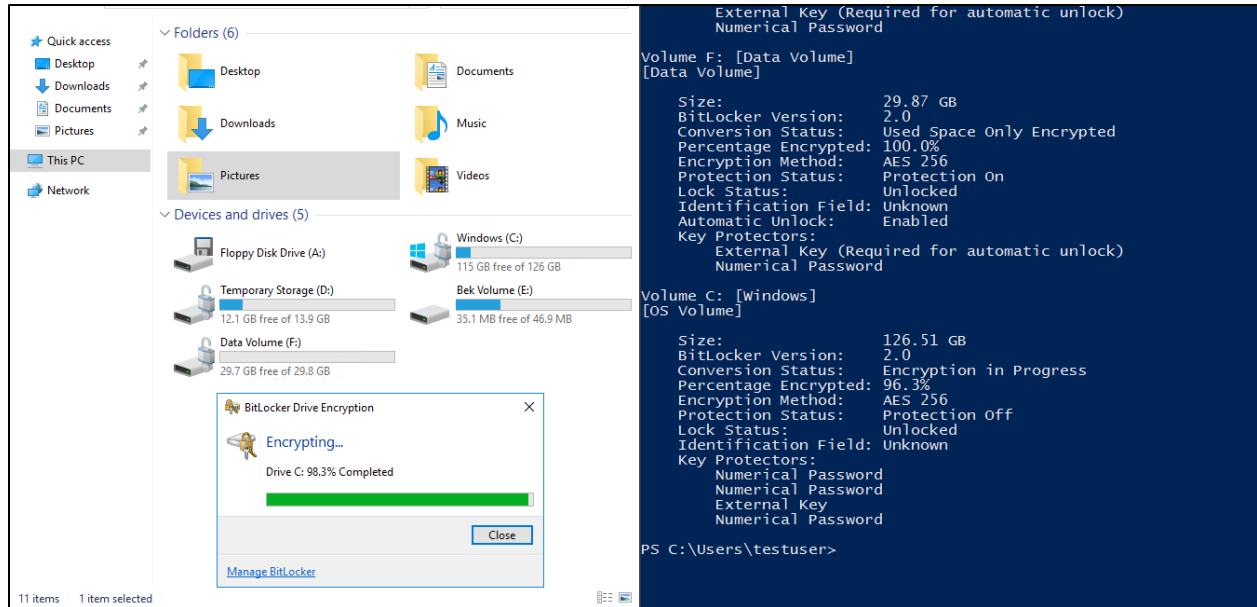
```
VM_DiskEncryption.ps1 X  
1 Login-AzureRmAccount  
2 Select-AzureRmSubscription -SubscriptionName 'MSDN Platforms'  
3 $rgName = 'Dev-RG';  
4 $aadClientId = 'd3add78-0033-4e1d-a264-ef8cef90a944'  
5 $clientSecret = 'mzGyW!@6lfo_vD:AzB1JH5[1PAE2@NzPTTL@r=?zBmv0lVeRN$GLButgjb]'  
6  
7 $keyVaultName = 'vmcypherkeys';  
8 $keyVaultKey = 'Bitlocker-Key';  
9 $keyVault = Get-AzureRmKeyVault -VaultName $keyVaultName -ResourceGroupName $rgName;  
10 $diskEncryptionKeyVaultUrl = $keyVault.VaultUri;  
11 $keyVaultResourceId = $keyVault.ResourceId;  
12 $sequenceVersion = ([Guid]: NewGuid());  
13 $SEK = Get-AzureKeyVaultKey -VaultName $keyVaultName -Name $keyVaultKey  
14  
X-ms-routing-request-id : WESTINDIA:20190131T204209Z:0a1a/2f6-203c-43c6-b86c-5234e38b9ac5  
X-Content-Type-Options  : nosniff  
Date                   : Thu, 31 Jan 2019 20:42:09 GMT  
  
Body:  
  
RequestId      :  
IsSuccessStatusCode : True  
StatusCode      : OK  
ReasonPhrase    : OK  
  
DEBUG: AzureQoSEvent: CommandName - Set-AzureRmVMDiskEncryptionExtension; IsSuccess - True; Duration - 00:06:05.1608641; Exception - ;  
DEBUG: Finish sending metric.  
DEBUG: 2:12:12 AM - SetAzureDiskEncryptionExtensionCommand end processing.  
DEBUG: 2:12:12 AM - SetAzureDiskEncryptionExtensionCommand end processing.
```

Step 5: Now login/RDP to your VM to check the encryption status. You can type the below mentioned command in PowerShell to check the BitLocker status for each disk for windows machine:

`manage-bde -status`



Step 6: If the encryption is still running you can see the progress in the BitLocker task bar notification. After the successful encryption you will be able to see “Encryption is Complete”.



Step 7: To check on the encryption status of a IaaS VM, use the Get-AzureRmVmDiskEncryptionStatus cmdlet

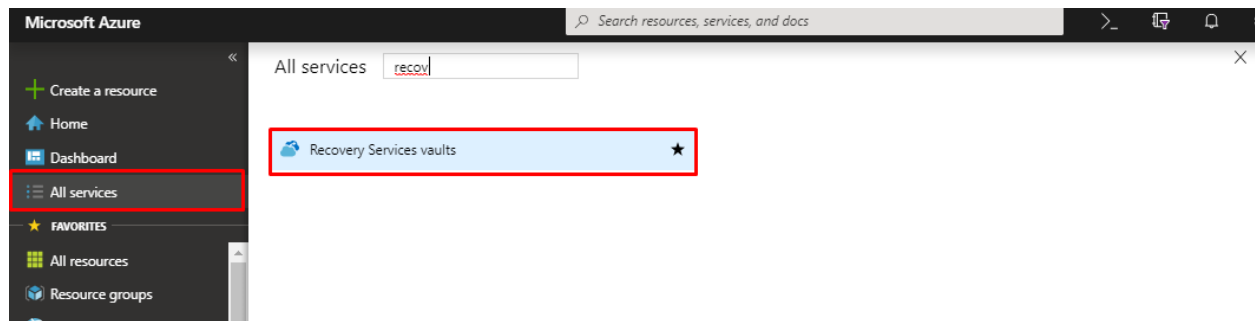
\$VMs - Virtual Machine Name

\$rgName - Virtual Machine Resource Group Name

\$VMs = ""

\$rgName = ""

Get-AzureRmVmDiskEncryptionStatus -ResourceGroupName \$rgName -VMName \$VMs



Disable disk encryption: To disable the encryption, use the Disable-AzureRmVMDiskEncryption cmdlet

\$VMs - Virtual Machine Name

\$rgName - Virtual Machine Resource Group Name

```
$VMs = ""  
$rgName = ""  
Disable-AzureRmVMDiskEncryption -ResourceGroupName "$rgName" -VMName "$VMs"
```

Note:

1. Before deleting a key vault, ensure that you did not encrypt any existing VMs with it. To protect a vault from accidental deletion, enable soft delete and a resource lock on the vault.

References:

1. <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview>
2. <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>
3. <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-appendix>
4. https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-windows#bkmk_RunningWinVMPSH