Convert BEK to KEK_Encryption

Last updated by | Kevin Gregoire | Mar 29, 2022 at 11:47 AM PDT

Tags

cw.Azure-Encryption cw.How-To

Contents

Summary

Customer has encrypted their VM using only BEK and now needs to enable using KEK to take advantage of Azure Backup and Recovery. A common desire is to convert Azure IaaS VM's that were encrypted using only BEK to also using KEK in order to take advantage of Azure Recovery Services. In this scenario, you do not need to decrypt your VM, rather simply enable with a KEK key using the following steps:

Reference

- Convert BEK Disk Encryption to KEK for Azure Recovery Services
- Deploy and manage backups for Resource Manager-deployed VMs using PowerShell
- Backup and restore encrypted VMs using Azure Backup
- Taking backup of encrypted Azure VMs with ADE (Azure Disk Encryption) using Azure Backup in OMS

Instructions for Single Pass Encryption

1. Install Azure Powershell

2. Connect to Azure Subscription using the below Azure Power Shell command.

   ```
   Connect-AzAccount
   ```

3. To use Azure backups there is a requirement to use KEK to encrypt the VHD files using azure disk encryption process. You will use your existing Key Vault Server which is used for backing keys and secrets for disk encryption.

   If you have a VM which is already encrypted without BEK, then you want to encrypt with KEK, use the ARM template or PS cmdlet below to change from *noKEK* to *KEK*. There are three options:

If you do not have a KEK yet, you can create one using the following:

```
Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITSoftware' -Destination 'Software'
```

For full details, use

```
Get-AzKeyVaultKey -VaultName 'contoso' -Name 'ITSoftware'
```

Now you have the KEK URL, use the below ARM template to encrypt the VM, supply the KEK.

Using the ARM Template Enable encryption on a running Windows VM without AAD

Using the Powershell script

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName -DiskEncryptionKeyVaultUrl $
```

Using *Azure Backup*. To enable the protection on encrypted VMs [encrypted using BEK and KEK], you need to give permissions for Azure Backup service to read keys and secrets from key vault.

```
Set-AzKeyVaultAccessPolicy -VaultName 'KeyVaultServerName' -ResourceGroupName 'RGName' -PermissionsTo
Get-AzKeyVault -VaultName $keyVaultName
Get-AzRecoveryServicesVault -Name "ARSName" | Set-AzureRmRecoveryServicesVaultContext
$pol=Get-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy"
Enable-AzRecoveryServicesBackupProtection -Policy $pol -Name "NameofVMtoBackup" -ResourceGroupName "R
```

Instructions for Dual Pass Encryption

1. Install Azure Powershell

2. Connect to Azure Subscription using the below Azure Power Shell command.

```
Connect-AzAccount
```

3. To use Azure backups there is a requirement to use KEK to encrypt the VHD files using azure disk encryption process. You will use your existing Key Vault Server which is used for backing keys and secrets for disk encryption.

   If you have a VM which is already encrypted without BEK, then you want to encrypt with KEK, use the ARM template or PS cmdlet below to change from *noKEK* to *KEK*. There are three options:

   If you do not have a KEK yet, you can create one using the following:

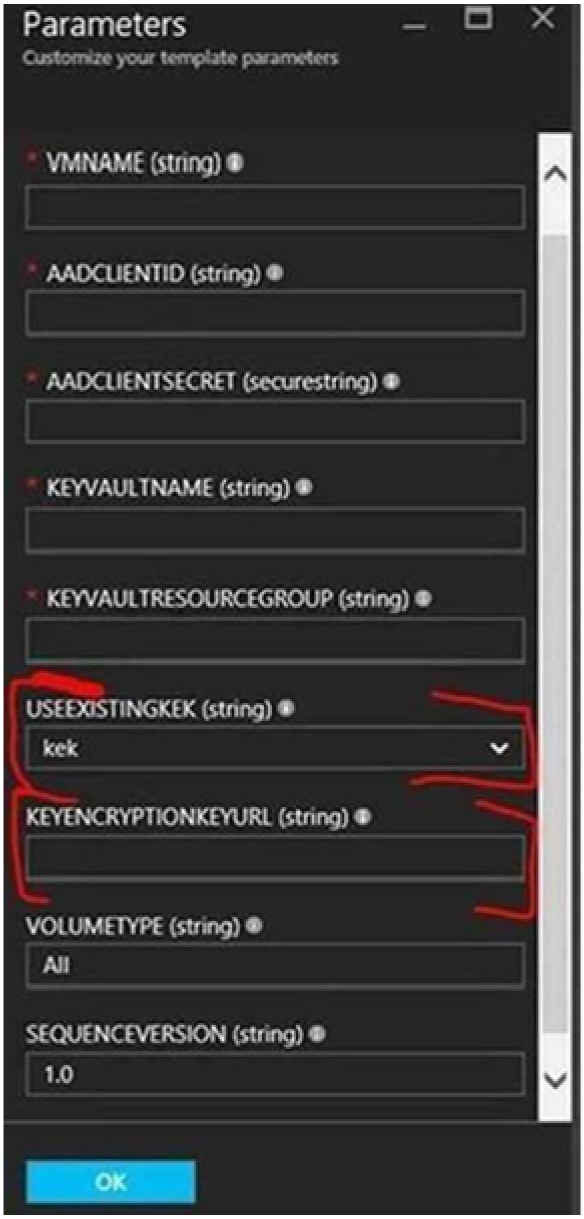
```
Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITSoftware' -Destination 'Software'
```

For full details, use

```
Get-AzKeyVaultKey -VaultName TSGKV -Name SSKey
```

Now you have the KEK URL, use the below ARM template to encrypt the VM, supply the KEK.

Using the ARM Template Enable encryption on a running Windows VM



Parameters
Customize your template parameters

* VMNAME (string)

* AADCLIENTID (string)

* AADCLIENTSECRET (securestring)

* KEYVAULTNAME (string)

* KEYVAULTRESOURCEGROUP (string)

USEEXISTINGKEK (string): kek

KEYENCRYPTIONKEYURL (string)

VOLUMETYPE (string): All

SEQUENCEVERSION (string): 1.0

Using the following powershell script:

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $rgname -VMName $vmName -AadClientID $aadClientID -
```

Using *Azure Backup*. To enable the protection on encrypted VMs [encrypted using BEK and KEK], you need to give permissions for Azure Backup service to read keys and secrets from key vault.

```
Set-AzKeyVaultAccessPolicy -VaultName 'KeyVaultServerName' -ResourceGroupName 'RGName' -PermissionsToK
Get-AzKeyVault -VaultName $keyVaultName
Get-AzRecoveryServicesVault -Name "ARSName" | Set-AzureRmRecoveryServicesVaultContext
$pol=Get-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy"
Enable-AzRecoveryServicesBackupProtection -Policy $pol -Name "NameofVMtoBackup" -ResourceGroupName "RG
```

Need additional help or have feedback?

To engage the Azure Encryption SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the Azure Encryption SMEs for faster assistance. Make sure to use the Ava process for faster assistance.	Use the Azure Encryption Feedback form to submit detailed feedback on improvements or new content ideas for Azure Encryption. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the Azure Encryption Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!