Bulk ADE VM Operations_Encryption

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

Tags

cw.Azure-Encryption cw.How-To

Contents

Summary

There are only two scenarios where the steps below will be helpful: 1- Encrypting Windows VMs with Single Pass by first time 2- Decrypting Windows VMs which were encrypted with Single Pass

Note: This does not work for VMs with dual pass

Considerations

- Make sure the VMs are running.
- Virtual Machine Scale Sets – would require different cmdlets.
- If Azure Backup/ Azure Site Recovery are being used at the same time these steps may need to be adjusted to reflect that or to make sense for the customer scenario (restoring from backups will be different after this point).
- Key vault resources remain in the user subscription and are billed to the user. This might not be obvious to them.
- If the user deletes the key vault they will not be able to restore from an older backup.
- If Azure Security Center is enabled on the subscription it will detect that the VM's are no longer encrypted.
- If customer has an advanced configuration – such as on Windows storage spaces, or containers, or on Linux a custom LVM scheme or docker, then special steps may not be required.
- If the VMs on the resource group uses a different keyvault each one, then this will not work.

Bulk Encryption of VMs with BEK

1. Get virtual machines for a specific resource group

```
$vmlist = Get-AzVM -ResourceGroupName "BulkEncryption";
```

2. Get the keyvault used to encrypt the VMs on that resource group. This will get only one keyvault so it is important to clarify this should be the one used for the VMs on that resource group.

```
$KeyVault = Get-AzKeyVault -VaultName BulkKV1 -ResourceGroupName "BulkEncryption"
```

3. This loop will be in charge of enabling the encryption and installing the extension.

```
foreach($vm in $vmlist)
{
Set-AzVMDiskEncryptionExtension -ResourceGroupName $vm.ResourceGroupName -VMName $vm.Name -DiskEncryption
}
```

Disable and Remove of ADE in Bulk

1. Get virtual machines for a specific resource group

```
 $vmlist = Get-AzVM -ResourceGroupName "BulkEncryption";
```

2. This loop will be in charge of disable the encryption and remove the extension.

```
foreach($vm in $vmlist) {
Disable-AzVMDiskEncryption -ResourceGroupName $vm.ResourceGroupName -VMName $vm.Name -VolumeType "all" -C
Remove-AzVMDiskEncryptionExtension -ResourceGroupName $vm.ResourceGroupName -VMName $vm.Name -Confirm
}
```

You will get the confirmation boxes below where you must indicate Y to proceed with the operation.

Bulk Encryption of VMs with KEK

1. Get virtual machines for a specific resource group

```
 $vmlist = Get-AzVM -ResourceGroupName "BulkEncryption";
```

2. Get the keyvault used to encrypt the VMs on that resource group. This will get only one keyvault so it is important to clarify this should be the one used for the VMs on that resource group.

```
$KeyVault = Get-AzKeyVault -VaultName "BulkKV1" -ResourceGroupName "BulkEncryption"
```

3. Name of the key used for the encryption

```
$keyEncryptionKeyName = 'MyKey';
```

This will get the URL automatically.

```
$keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName "BulkKV1" -Name $keyEncryptionKeyName).Key.kid;
```

4. This loop will be in charge of enabling the encryption and installing the extension.

```
foreach($vm in $vmlist)
{
Set-AzVMDiskEncryptionExtension -ResourceGroupName $vm.ResourceGroupName -VMName $vm.Name -DiskEncryption
}
```

5. Once it succeeds you should get an output like this

```
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
----------                    ----------- ----------
                              True        OK OK
                              True        OK OK
                              True        OK OK
```

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!