

Get Keyvault Secret Used by Encrypted VM_Encryption

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

Tags

cw.Azure-Encryption

cw.How-To

Contents

- [Scenario](#)
- [Windows VM](#)
 - [Conclusion](#)
- [Need additional help or have feedback?](#)

Scenario

When a customer wants to recover an encrypted VHD and should know the secret to download the BEK file and unlock/recover the VHD.

Windows VM

1. The encryption settings are exposed in VM Model. Use the following PowerShell commands to get the VM model details which contains the encryption settings for the VM under the StorageProfile.

```
$rgName = "<RESOURCE GROUP>"
$kvrgName = 'ToTestEncryption'
$vmName = "<VM NAME>"
$KeyVaultName = "<KEY VAULT NAME>"
$keyvaultkeyname = "<KEY NAME>"
$location = "<LOCATION>"
```

```
Get-AzVM -ResourceGroupName $rgName -Name $vmName -DisplayHint Expand
```

2. The SecretUrl contains the BEK file name and the version of the secret.

```

StorageProfile :
ImageReference :
Publisher      : MicrosoftWindowsServer
Offer         : WindowsServer
Sku           : 2012-R2-Datacenter
Version       : latest
OsDisk        :
OsType        : Windows
EncryptionSettings :
DiskEncryptionKey :
SecretUrl      : https://aman.vault.azure.net/secrets/74453CE0-1F17-470B-8523-00D66AA5D46A/c069978508a646bd8a78e6b2d56f8ea0
SourceVault    :
Id             : /subscriptions/615ff5fc-.../resourceGroups/ToTestEncryption/providers/Microsoft.KeyVault/vaults/aman
Enabled        : True
Name           : Enw1_OsDisk_1_2d63e36a78f64a84893b2c22a9879b77
Caching        : ReadWrite
CreateOption   : FromImage
ManagedDisk   :
Id             : /subscriptions/615ff5fc-.../resourceGroups/ToTestEncryption/providers/Microsoft.Compute/disks/E
nw1_OsDisk_1_2d63e36a78f64a84893b2c22a9879b77
  
```

This is the BEK/Secret used to encrypt the VM.

This is the version of the secret.

3. The second pull that we can do to narrow down the search if the "Expand" feature does not work from above.

```

$vm = Get-AzVM -ResourceGroupName $rgName -Name $vmName
$vm.StorageProfile.OsDisk.EncryptionSettings.DiskEncryptionKey.SecretUrl
  
```

```

$vm = Get-AzureRmVM -ResourceGroupName $rgName -Name $vmName
$vm.StorageProfile.OsDisk.EncryptionSettings.DiskEncryptionKey.SecretUrl
https://mdrondom.vault.azure.net/secrets/32489CFE-0DB5-4B2E-8448-B7D3DA3EBF50/111f49e3a7da41efabc376ab9ed3efa5
  
```

This is the BEK/Secret used to encrypt the VM.

This is the version of the Secret.

4. The third way to check is by viewing it in the Keyvault from the portal:

5. The extension for Windows VMs creates the following Tags for the Secret which makes it easy for us to identify the Secret used by a particular VM.

- MachineName
- VolumeLetter

Note: These tags are only applicable for Windows VM. For Linux VMs, the extension does not create these tags.

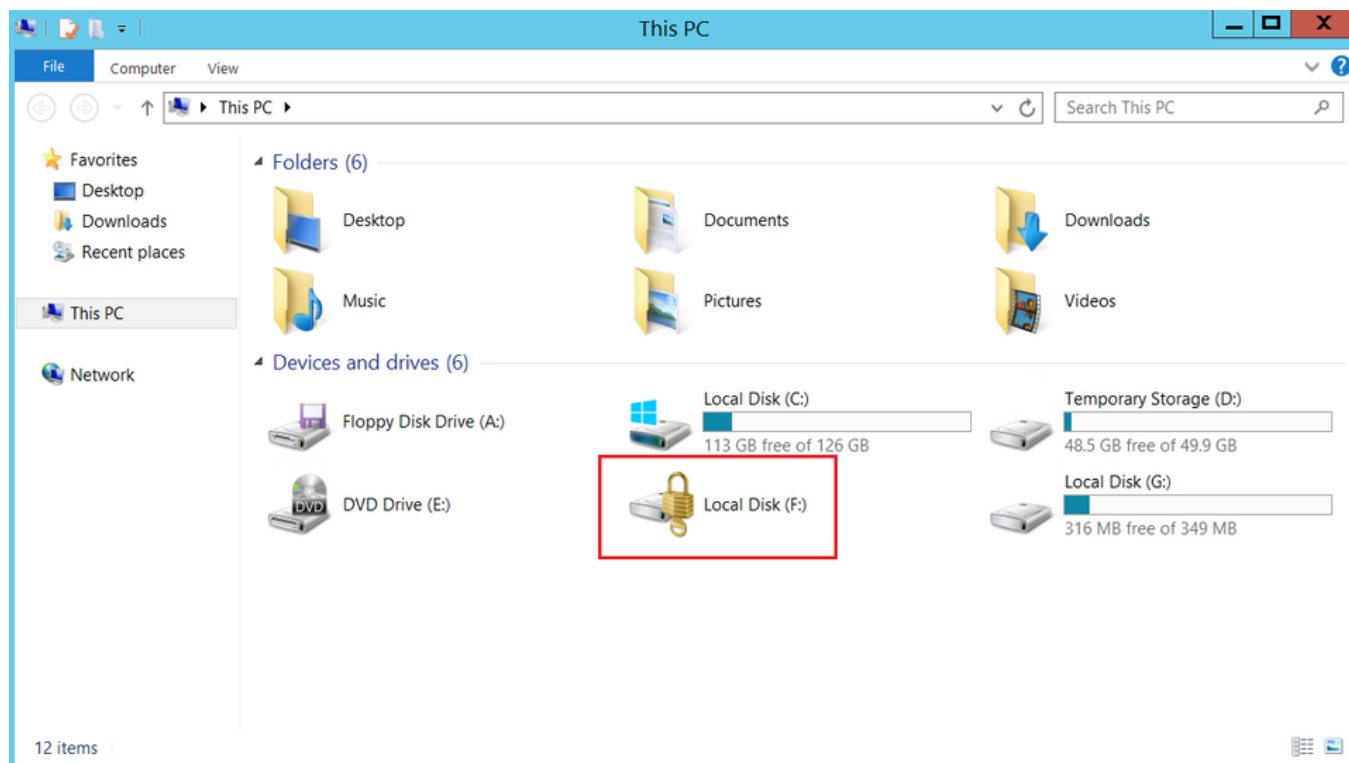
The screenshot shows the Azure Key Vault portal interface. On the left, there's a sidebar with navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Keys, Secrets, and Certificates. The 'Secrets' section is expanded. The main area shows a list of secrets under the 'UNMANAGED' section. One secret is highlighted with a red box, showing its details: NAME (74453CE0-1F17-470B-8523-00D66AA5D46A), TYPE (BEK), STATUS (Enabled), and EXPIRATION DATE. The secret is also tagged with 'MachineName' and 'VolumeLetter'.

The screenshot displays the Microsoft Azure portal interface. The top navigation bar shows the breadcrumb path: « aman - Secrets > 74453...D46A > c0699785...J56f8ea0. The main content area is split into two panes. The left pane, titled 'Versions', shows a table with columns: VERSION, STATUS, ACTIVATION DATE, and EXPIRATION DATE. A single row is visible with the version 'c0699785...' and status 'Enabled'. A red box highlights this row, and a red line points from it to the 'Tags' section in the right pane. The right pane, titled 'Secret Version', shows the 'Properties' section with 'Created' and 'Updated' dates of 9/21/2017. The 'Secret Identifier' is 'https://aman.vault.azure.net/secrets/74453...D46A/c0699785...J56f8ea0'. The 'Settings' section has checkboxes for 'Set activation date?' and 'Set expiration date?', both unchecked, and a 'Enabled?' toggle set to 'Yes'. The 'Tags' section shows '4 tags'. The 'Secret' section shows 'Content type (optional)' as 'BEK' and a 'Show secret value' button. Below this, a second screenshot shows the 'Tags' page for the same secret. The breadcrumb path is « 74453CE0-...00D66AA5D46A > c069978508a646bd8a78e6b2d56f8ea0 > Tags. The main content area shows a table with columns 'TAG NAME' and 'TAG VALUE'. The table contains four rows: 'DiskEncryptionKeyFileName' with value '74453CE0-...00D66AA5D46A.BEK', 'VolumeLetter' with value 'C:', 'DiskEncryptionKeyEncryptionAlgorithm' with value 'RSA-OAEP', and 'MachineName' with value 'Enw1'. A red box highlights the entire table.

TAG NAME	TAG VALUE
DiskEncryptionKeyFileName	74453CE0-...00D66AA5D46A.BEK
VolumeLetter	C:
DiskEncryptionKeyEncryptionAlgorithm	RSA-OAEP
MachineName	Enw1

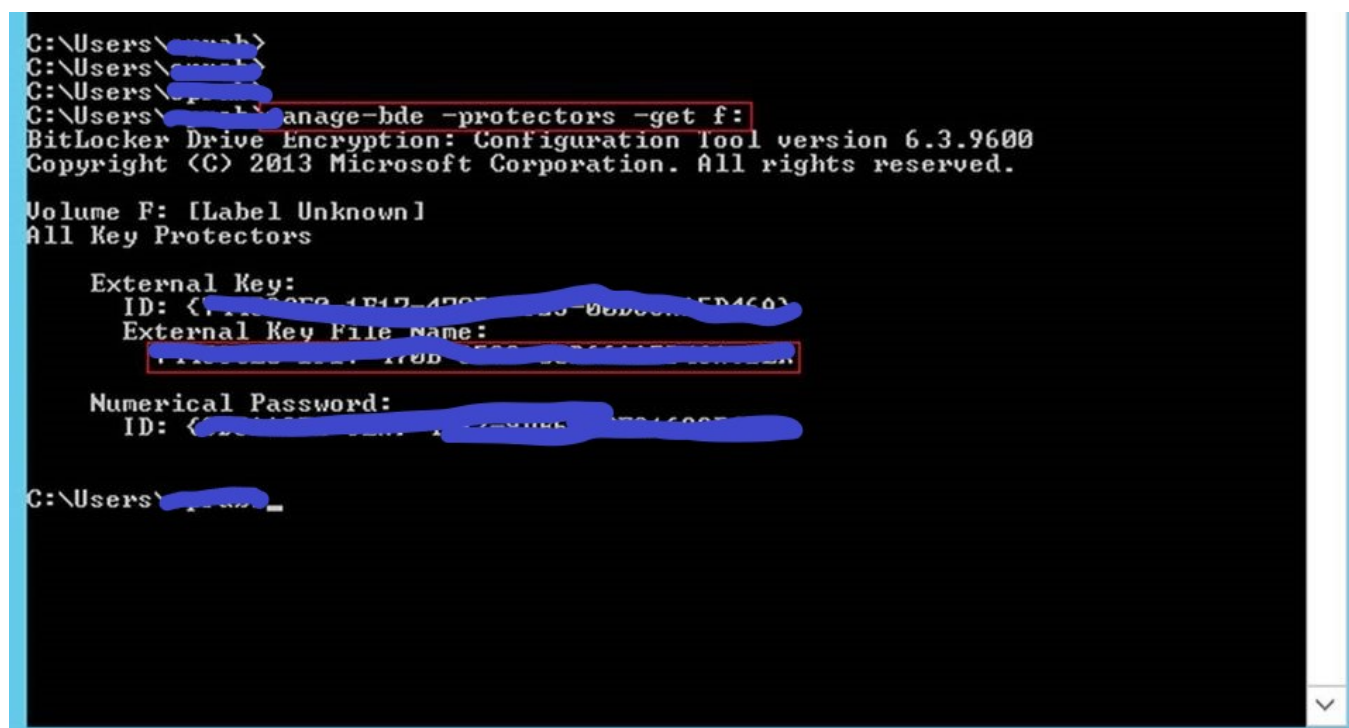
6. From the Guest OS:

1. Attach the disk as data disk to another VM. Once attached to the VM, the explorer window will look like the one below. The encrypted drive will have a lock icon.

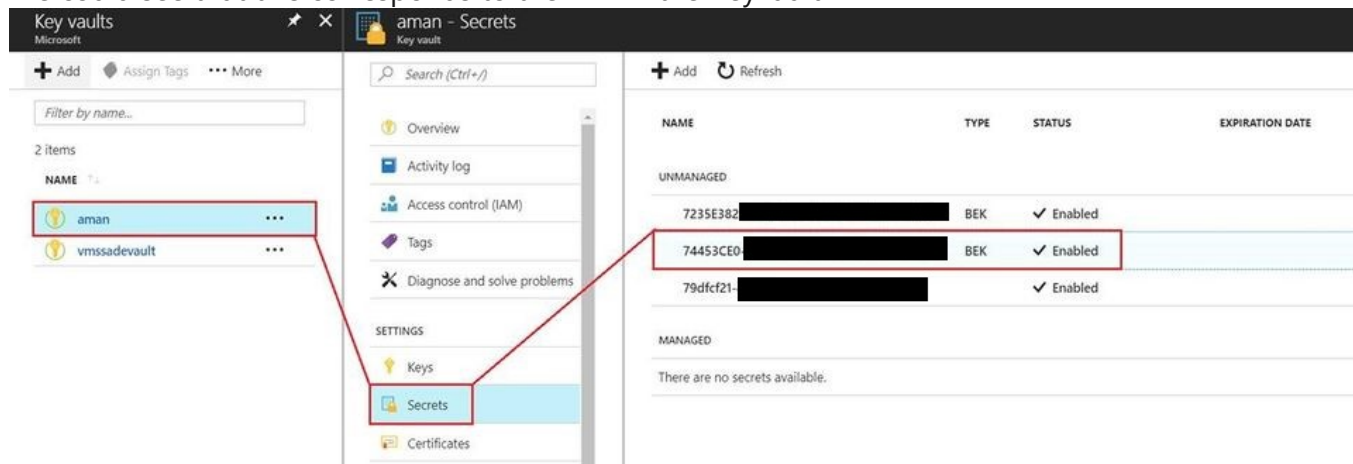


2. Open command prompt with administrator privileges and run the following command:

```
manage-bde -protectors -get <volume letter>
```



3. We could see that this corresponds to the BEK in the Keyvault



4. We can also use the following PowerShell commands to retrieve the secret against the VM name:

```
$rgName = "<RESOURCE GROUP>"
$kvrgName = 'ToTestEncryption'
$vmName = "<VM NAME>"
$KeyVaultName = "<KEY VAULT NAME>"
$keyvaultkeyname = "<KEY NAME>"
$location = "<LOCATION>"
```

```
Get-AzKeyVaultSecret -VaultName $keyvaultName | where {($_.Tags.MachineName -eq "$vmName") -and
```



```
PS C:\User\... Get-AzureKeyVaultSecret -VaultName $keyvaultName | where {($_.Tags.MachineName -eq "$vmName") -and ($_.ContentType -match 'BEK')}
```

```
Vault Name : ...
Name       : 74453CE0-...
Version    :
Id         : https://aman.vault.azure.net:443/secrets/74453CE0-...
Enabled    : True
Expires    :
Not Before :
Created    : 9/21/2017 2:11:10 PM
Updated    : 9/21/2017 2:11:10 PM
Content Type : BEK
Tags       : Name Value
              VolumeLetter C:\
              MachineName Enw1
              DiskEncryptionKeyFileName 74453CE0-1F17-...
              DiskEncryptionKeyEncryptionAlgorithm RSA-OAEP
```

Conclusion

This way we can find which SECRET is being used and then proceed to the next steps to recover the BEK file from the keyvault to unlock the VHD.

Need additional help or have feedback?

<i>To engage the Azure Encryption SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to the Azure Encryption SMEs <input type="checkbox"/> for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the Azure Encryption Feedback form to submit detailed feedback on improvements or new content ideas for Azure Encryption.</p> <p>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.</p>	<p>Use the Azure Encryption Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>