# Key Vault not Found to Unwrap Encryption Key_Encryption

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

Tags

cw.Azure-Encryption cw.TSG

Contents



Non-get VM operations failing with “The key vault key is not found to unwrap the encryption key” - The remote server returned an error: (403) Forbidden.

**Issue**

VM Start/Stop/PUT/PATCH operations failing with “The key vault key is not found to unwrap the encryption key” - The remote server returned an error: (403) Forbidden.

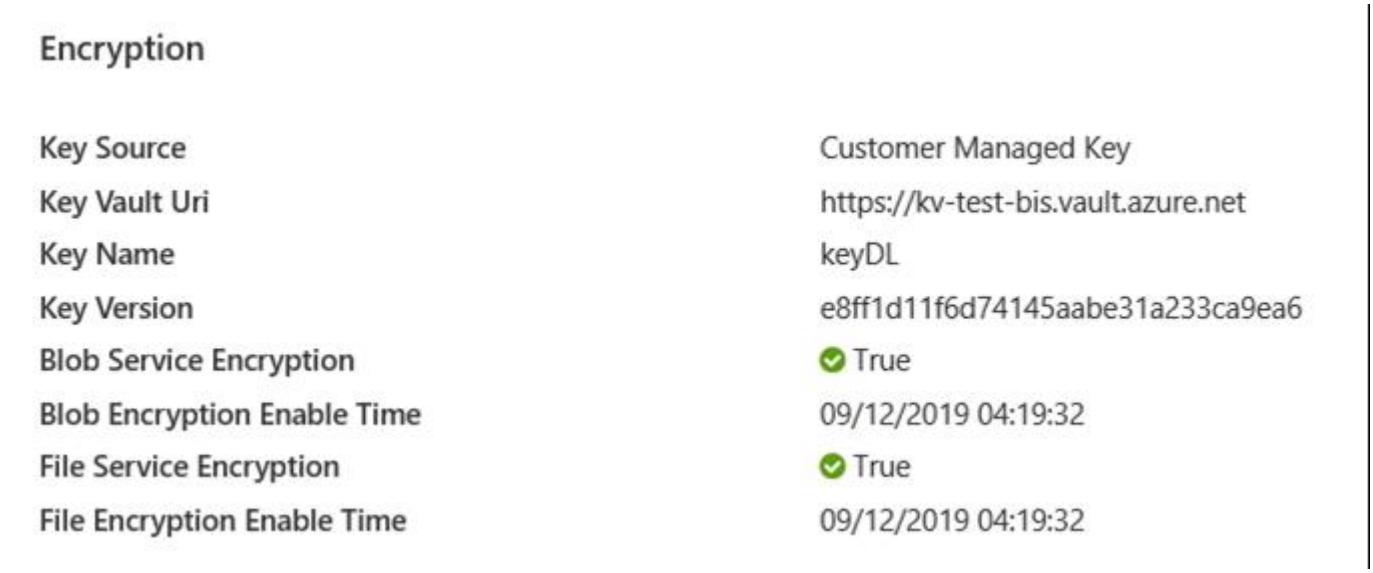
Sample error as below :-

```
Got Authentication error with Microsoft.WindowsAzure.Storage.StorageException: The remote server returned an error: (403) Forbidden. --->
System.Net.WebException: The remote server returned an error: (403) Forbidden.
  at Microsoft.WindowsAzure.Storage.Shared.Protocol.HttpResponseParsers.ProcessExpectedStatusCodeNoException[T](HttpStatusCode
expectedStatusCode, HttpStatusCode actualStatusCode, T retVal, StorageCommandBase`1 cmd, Exception ex)
  at Microsoft.WindowsAzure.Storage.Blob.CloudBlobClient.<>c__DisplayClass13.<GetBlobReferenceImpl>b__12(RESTCommand`1 cmd,
HttpWebResponse resp, Exception ex, OperationContext ctx)
  at Microsoft.WindowsAzure.Storage.Core.Executor.Executor.EndGetResponse[T](IAsyncResult getResponseResult)
  --- End of inner exception stack trace ---
Request Information
RequestID:190bebd3-501c-0027-3d99-a4741e000000
RequestDate:Tue, 26 Nov 2019 20:39:02 GMT
StatusMessage:The key vault key is not found to unwrap the encryption key.
, attempting storage account key refresh for bc55storageaccount, current retry count 0, should retry : true
```

**Possible Reason**

One scenario is where VM is using unmanaged disks and the storage account is using Encryption for data at rest. Furthermore the storage account is encrypted using “Customer Managed Keys” . Can pull this information using ASC (check on storage account properties) or else go to “Encryption” option on portal for the storage account.

ASC Sample selecting Storage Account properties :-




Error 403 Forbidden followed by “The key vault key is not found to unwrap the encryption key” during “write” operation can be because of multiple reasons. Few of them as below :-

- The Key version is not latest in the key vault.
- Key is deleted from the key vault.
- Customer removed access to storage account on the key vault.

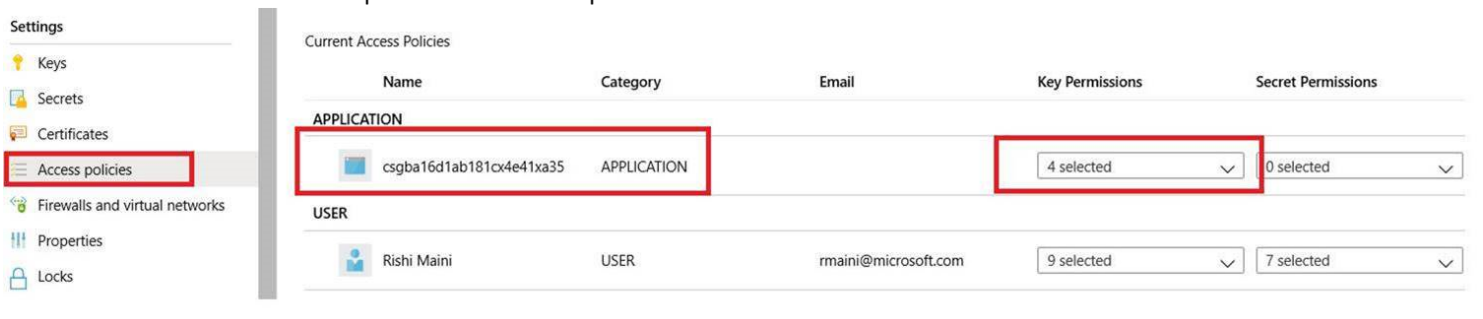
**Mitigation Steps**

Confirm if the Key vault ”VaultName” has “Key” named “KeyName” with latest version as “XYZ” as you see in ASC ?

If the Key Name and Versions are not available , try to restore the same using
Undo-AzKeyVaultKeyRemoval -VaultName "VaultName" -Name " KeyName"

If the Key Name is there but the latest version does not match to “XYZ”. Go to the storage account -> Encryption and point to the latest version of the key and retry the VM operation. Reference link.

If KeyName and Latest version all looks good for the vault , check if storage account is listed as Application under key vault “Access Policies” section . Sample as in below snapshot.




If the storage account is not listed as having access to the key vault, we need to add it back with permission (-PermissionsToKeys wrapkey,unwrapkey,get,recover).

See if you can add the storage account to key vault directly from portal (giving key permissions wrapkey, unwrapkey, get and recover).

If you can't see the storage account on portal to be added as Application to key vault , try below PowerShell commands . Reference Link.

```
$account = Set-AzStorageAccount -ResourceGroupName "RGName" -AccountName "StorageAccountName" -AssignIdentity

$keyVault = Get-AzKeyVault -VaultName "VaulName" -ResourceGroupName "VaultRGName"

Set-AzKeyVaultAccessPolicy -VaultName $keyVault.VaultName -ObjectId $account.Identity.PrincipalId -PermissionsToKeys wrapkey,unwrapkey,get,recover
```

Do evaluate the same approach (with assistance from your Technical Advisor) if you are seeing same error "The key vault key is not found to unwrap the encryption key" but the overall scenario is slightly different (example "Customer Managed Keys" are not used but you are getting same error for other issues like disk encryption etc.) . The idea of TSG is to give you some information around possible reasons of seeing "key is not found to unwrap" errors. Mitigation might be different based customers scenario in hand.

## 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.<br><br>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.<br><br>***Please note*** the link to the page is required when submitting feedback on existing pages!<br>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!<br><br>***Please note*** the link to the page is required when submitting kudos! |