

Failure to Send Disk Encryption Data_Encryption

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

Tags

cw.Azure-Encryption

cw.TSG

Contents

- [Symptom](#)
- [Root Cause Analysis](#)
- [Mitigation](#)
- [Helpful links](#)
- [Need additional help or have feedback?](#)

Symptom

When encrypting a VM, we have seen scenarios in which the encryption fails with the following error message:

Failed to send DiskEncryptionData, Check KeyVault inputs, ResourceIds and retry encryption operation

```
PowerShell
PS C:\> $KeyVaultResourceId = $KeyVault.ResourceId;
PS C:\> $SequenceVersion = [Guid]::NewGuid();
PS C:\> Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultResourceId $KeyVaultResourceId -VolumeType "All" -SequenceVersion $SequenceVersion;

Enable AzureDiskEncryption on the VM
This cmdlet prepares the VM and enables encryption which may reboot the machine and takes 10-15 minutes to finish. Please save your work on the VM before confirming.
Do you want to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
Set-AzVMDiskEncryptionExtension: Long running operation failed with status 'Failed'. Additional Info: 'VM has reported a failure when processing extension 'AzureDiskEncryption'. Error message: "[2.2.0.36] Failed to send DiskEncryptionData, Check KeyVault inputs, ResourceIds and retry encryption operation"
More information on troubleshooting is available at https://aka.ms/vmextensionwindowstroubleshoot '
Errorcode: VMExtensionProvisioningError
ErrorMessage: VM has reported a failure when processing extension 'AzureDiskEncryption'. Error message: "[2.2.0.36] Failed to send DiskEncryptionData, Check KeyVault inputs, ResourceIds and retry encryption operation"
More information on troubleshooting is available at https://aka.ms/vmextensionwindowstroubleshoot
ErrorTarget:
StartTime: 2/10/2021 3:00:40 PM
EndTime: 2/10/2021 3:07:59 PM
OperationID: ac1251cf-bd2f-41f0-a334-25a2190fb742
Status: Failed
```

STOP!!

Is the affected VM a Windows Server 2022 edition? If the answer is **YES** please check the [Emerging issue for Windows Server 2022](#)

Root Cause Analysis

This can be due to the following situations:

1. Having the Key Vault existing in a different region and subscription than the Virtual Machine.
2. Typo in the Resource ID or URL for the KEYVAULT or KEK certificate.
3. Special characters used while naming the resources. i.e _VMName, élite, etc.
4. Lack of permissions in the Key Vault or the Key Encryption Key from the Key Vault.
5. Network issues that prevent the VM/Host from accessing the required resources.

6. Unsupported encryption scenarios.

Mitigation

1. Make sure the Key Vault exists in the same region and subscription as the Virtual Machine, validate the VM has not been moved in an unsupported way (moved to new region, or new subscription - without also moving the key vault and re-enabling for the new key vault into that same region or subscription). They can be part of different resource groups but they cannot be in different regions.
2. Check for any typos in the Key Vault name or Key name, mostly if customer is using Powershell or CLI.

Note

The syntax for the value of disk-encryption-keyvault parameter is the full identifier string: /subscriptions/[subscription-id-guid]/resourceGroups/[resource-group-name]/providers/Microsoft.KeyVault/vaults/[keyvault-name]

The syntax for the value of the key-encryption-key parameter is the full URI to the KEK as in: https://[keyvault-name].vault.azure.net/keys/[kekname]/[kek-unique-id]

3. Check for any special characters used while naming the resources, please ask customer to recreate the resource without special characters.
4. From the customer's portal, go to the **Key Vault** and select **Access Policies**. Make sure the option for **Azure Disk Encryption for volume encryption** is enabled and that in the Key Permissions the **Wrap** and **Unwrapped** are included.

Basics Access policy Networking Tags Review

Enable Access to:

- ☐ Azure Virtual Machines for deployment ⓘ
- ☐ Azure Resource Manager for template deployment ⓘ
- ☒ Azure Disk Encryption for volume encryption ⓘ

Permission model

- ☒ Vault access policy
- ☐ Azure role-based access control (view)

+ Add Access Policy

Current Access Policies

Name	Email	Secret Permissions
USER		

11 selected 7 selected




5. Network issues can happen when the Key Vault is behind a firewall so the VM cannot reach the right resources. Another example is having a restricted NSG. The customer will have to work and find what is blocking. For more information: [Azure Disk Encryption behind a Firewall](#) ⓘ This can also happen when having a proxy server setting that blocks the access to the Azure Instance Metadata service endpoint. The VM must be able to access IP 169.254.169.254. You can find further information here: [Azure Instance Metadata Service](#) ⓘ and [What is IP address 168.63.129.16?](#) ⓘ


If by checking the logs you encounter error

```
2021-06-17T16:16:43.0092404Z [Info]: SendEncryptionSettingsToHost diskEncryptionPostUri: http://168.63.12
2021-06-17T16:17:13.5350231Z [Info]: HttpCallWrapper::SendEncryptionSettingsToHostHelper responseConte
<H1>504 Gateway Timeout</H1>
Gateway timeout expired while waiting for server response</HTML>
, ReasonPhrase:Gateway Timeout, StatusCode:GatewayTimeout
2021-06-17T16:17:13.5350231Z [Info]: SendEncryptionSettingsToHost failed. Attempting again. retryCount
```


This error is observed when the customer has implemented a proxy solution that is overly restrictive and blocking Azure Disk Encryption from being able to communicate with the Azure platform resources.

In the legacy version of Azure Disk Encryption, access to Key Vault endpoints from the VM used to be required. In the newer 2.2 version of the extension, direct access to Key Vault endpoints is no longer needed, but a communication channel with the Azure platform resources is needed instead. In this case that channel was being blocked.


Please share the following mitigation steps with the customer, that explain how to update their proxy settings to allow unaltered HTTP traffic to 168.63.129.16 and 169.254.169.254 as documented here: [Azure Instance Metadata Service](#)  , [What is IP address 168.63.129.16?](#)  [Azure Disk Encryption behind a Firewall](#) 

6. Unsupported scenarios like Virtual disk mounted within the VM. For more information please refer to [Azure Disk Encryption Unsupported Scenarios](#) 

Helpful links

1. [Azure Disk Encryption for Linux VMs troubleshooting guide](#) 
2. [Azure Disk Encryption for Windows VMs troubleshooting guide](#) 

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  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>