

# Internal error occurred while processing encryptionSettings\_Encryption

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

Tags:

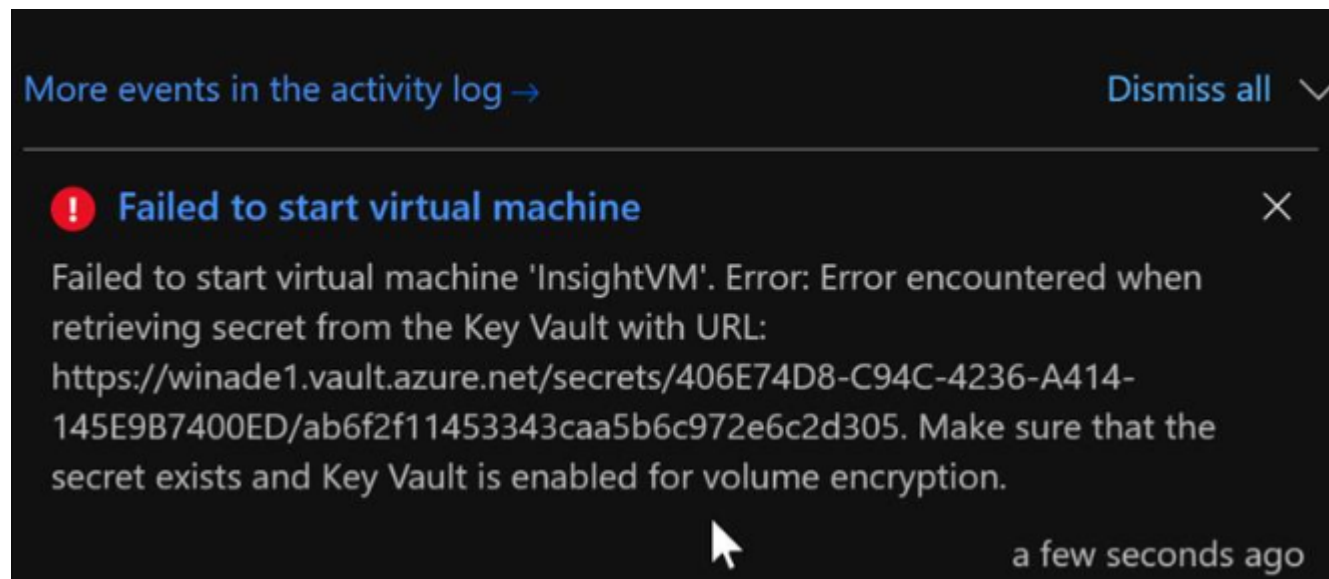
- cw.Azure-Encryption
- cw.TSG
- cw.Reviewed-10-2021

## Contents

- 
- [Summary](#)
  - [Troubleshooting Steps](#)
  - [Mitigation](#)
- [Need additional help or have feedback?](#)

## Summary

For any encrypted VM or VMSS in a stopped state that does no longer has access to the Secret and Key, i.e secret and/or key has been deleted from the Key Vault or permissions have been removed, when the customer Starts the machine, they will get an error message for **""Failed' error message in the portal: "Provisioning failed. Internal error occurred while processing encryptionSettings. DiskEncryptionInternalError"** from ASC, and **"Error: Error encountered when retrieving secret from the Key Vault with URL . Make sure that the secret exists and Key Vault is enabled for volume encryption."** from the Portal.



## Troubleshooting Steps

1. 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.
2. Make sure the secret exists. To check what secret has been used, go to ASC and click on the affected VM and select Disks. Scroll down until you find the Encryption Settings.

Is Disk Encrypted      True (Encryption without AAD Credentials)

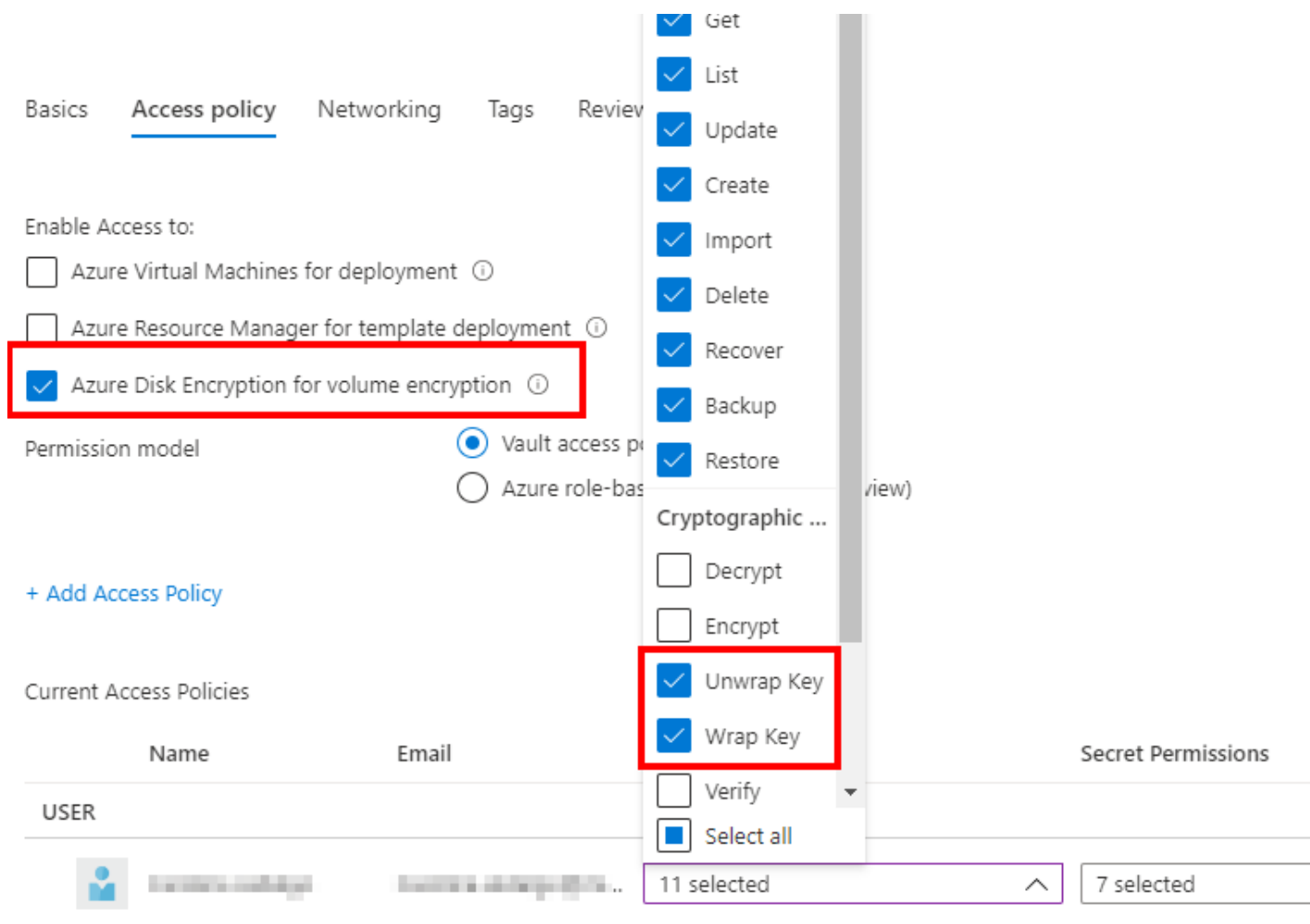
Source Vault ID      /subscriptions/[REDACTED]/resourceGroups/ADEbasicsLab/providers/Microsoft.KeyVault/vaults/winADE1

Disk Encryption Key Secret Url      https://winade1.vault.azure.net/secrets/406E74D8-C94C-4236-A414-145E9B7400ED/ab6f2f11453343caa5b6c972e6c2d305

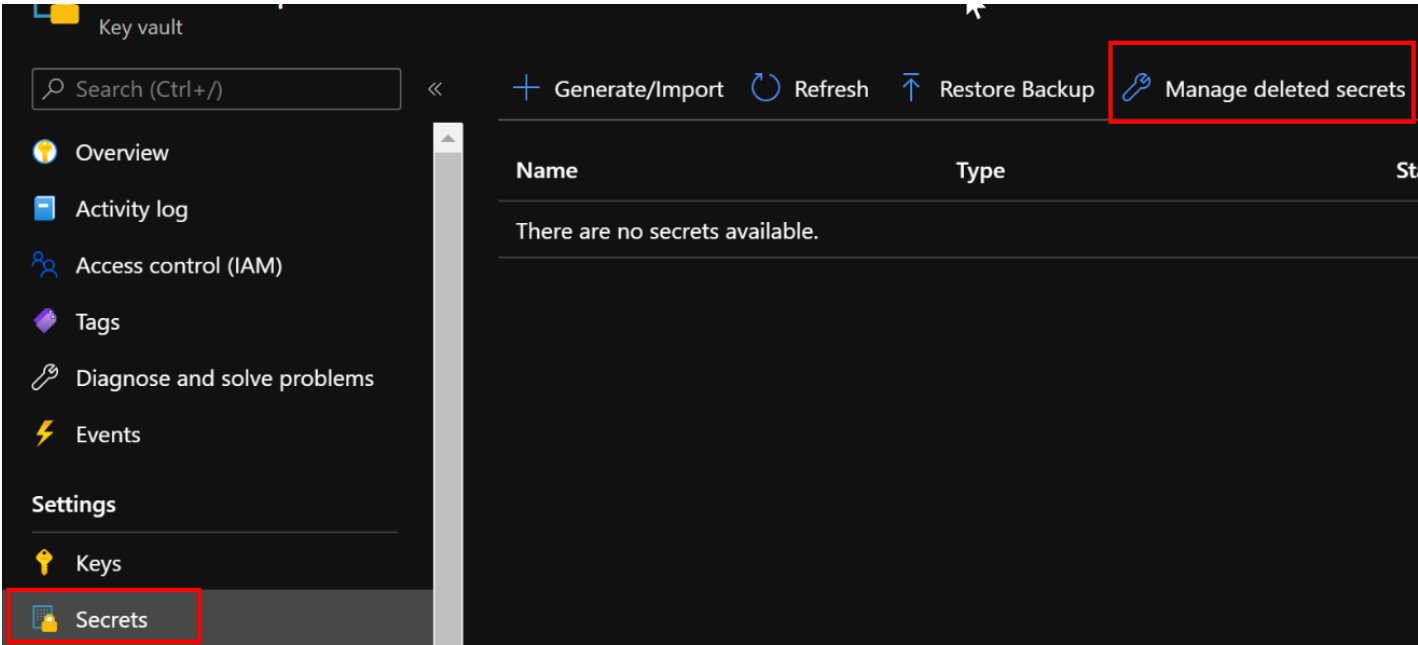
Key Encryption Key Url

## Mitigation

1. If there are any missing permissions, make sure to enable them as per picture below.



2. If the secret or Key do not exist inside the Key Vault, use the Manage deleted secrets button to check if the secret was deleted. If that is the case, use the Recover option. For more information, please check [Azure Key Vault Recovery overview](#)



If the secret or key cannot be recovered, the VM will no longer be usable and there is no possible way to get it back. Suggest customer to restore the VM from a backup.

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