# Connection was Forcibly Closed by the Remote Host_Encryption

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

Tags

cw.Azure-Encryption cw.TSG

Contents

## Symptom

1. When the customer attempts to encrypt the disk, will get the following error:

```
    Error Message: Set-AzVMDiskEncryptionExtension : Long running operation failed with status 'Failed'.
```

2. You may also see connectivity issues in the waagent.log similar to (but not mutually exclusive):

```
 [00000020] [01/18/2017 22:45:36.98] [ERROR] Attempt 1: Direct upload of status from the VM failed. Excep
 [00000020] [01/18/2017 22:45:36.98] [ERROR] Attempt 3: Uploading status via HostGAPlugin failed. Status
    "errorCode": "UriNotAllowed",
    "message": "Requested Uri is not allowed.",
    "details": ""
```

## Data Collections

1. Collect the logs from the extension on `C:\ WindowsAzure\Logs\Plugins\Microsoft.Azure.Security.AzureDiskEncryption\<Version>\Bitlocker.log`

#### Sample Logs

```
Bitlocker Log: 2017-08-16T09:58:14.2873836Z    [Fatal]:    BitlockerExtension::OnEnable hit exception Serv
System.Net.WebException: The underlying connection was closed: An unexpected error occurred on a send. ---
```

## Root Cause Analysis

### Root Cause Analysis 1

TLS 1.1 disabled in VM

### Root Cause Analysis 2

This could happen wether:

1. Proxy service enabled on VM not allowing traffic bound for requisite Azure endpoints�
2. Stateful Packet Inspection (firewall or IPS) preventing access to requisite Azure endpoints

## Mitigation

### Mitigation 1

1. Connect to the VM and open a CMD instance and query how is TLS 1.1:

   ```
   reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server"
   ```

   1. If the key doesn't exist or exist and its value is 0, then it means the prototol is disabled. You can enable it by running:

      ```
      reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Serve
      ```

2. If you find TLS 1.1 is enabled property, just continue with the following mitigation section

### Mitigation 2

1. You can test the firewall/IPS or proxy blocking connection by requesting the customer to perform this from a different network than the corporative one

## Root Cause Closing Code - Service Desk

| | | |
|---|---|---|
| ***Mitigation 1*** | ***Root Cause - Windows Azure\Compute\Virtual Machine\OS Hardening*** | |
| ***Mitigation 2*** | Product: ***Azure Virtual Networks*** | Cause: ***Root Cause - Azure Virtual Networks\Virtual Network\Configuration\How to\Lack of documentation*** |

To know how to flag a bug on a case please refer to How to do Proper Case Coding

## 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>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>***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>***Please note*** the link to the page is required when submitting kudos! |