Failed to Configure Bitlocker as Expected_Encryption

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

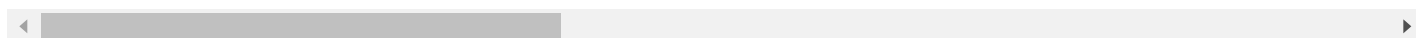| Tags |
|------|
| cw.Azure-Encryption   cw.TSG |

Contents

Symptom

1. When you try to encrypt your disk, you get the following error

```
Encryption fails with Error::Failed to configure bitlocker as expected. System.Net.WebException Excep
```



```
PS C:\Users\PSolanki> Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName 'RG-VM-Dev' -VMName $vmName -AadClientID $aadClientID -AadClientSecret $aadClientSecret -DiskEncrypti
Set-AzureRmVMDiskEncryptionExtension : Long running operation failed with status 'Failed'.
ErrorCode: VMExtensionProvisioningError
ErrorMessage: VM has reported a failure when processing extension 'AzureDiskEncryption'. Error message: "Failed to configure bitlocker as expected. Exception: An error occurred
while sending the request., InnerException: System.Net.WebException: The underlying connection was closed: An unexpected error occurred on a receive. --->
System.ComponentModel.Win32Exception: The client and server cannot communicate, because they do not possess a common algorithm
   at System.Net.SSPIWrapper.AcquireCredentialsHandle(SSPIInterface SecModule, String package, CredentialUse intent, SecureCredential scc)
   at System.Net.Security.SecureChannel.AcquireCredentialsHandle(CredentialUse credUsage, SecureCredential& secureCredential)
   at System.Net.Security.SecureChannel.AcquireClientCredentials(Byte[]& thumbPrint)
   at System.Net.Security.SecureChannel.GenerateToken(Byte[] input, Int32 offset, Int32 count, Byte[]& output)
   at System.Net.Security.SecureChannel.NextMessage(Byte[] incoming, Int32 offset, Int32 count)
   at System.Net.Security.SslState.StartSendBlob(Byte[] incoming, Int32 count, AsyncProtocolRequest asyncRequest)
   at System.Net.Security.SslState.ForceAuthentication(Boolean receiveFirst, Byte[] buffer, AsyncProtocolRequest asyncRequest)
   at System.Net.Security.SslState.ProcessAuthentication(LazyAsyncResult lazyResult)
   at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
   at System.Net.TlsStream.ProcessAuthentication(LazyAsyncResult result)
   at System.Net.TlsStream.BeginWrite(Byte[] buffer, Int32 offset, Int32 size, AsyncCallback asyncCallback, Object asyncState)
   at System.Net.ConnectStream.WriteHeaders(Boolean async)
   --- End of inner exception stack trace ---
   at System.Net.HttpWebRequest.EndGetResponse(IAsyncResult asyncResult)
   at System.Net.Http.HttpClientHandler.GetResponseCallback(IAsyncResult ar), stack trace:    at
Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.UploadBekToKeyVault(EncryptableVolume vol, String protectorId, Boolean saveKeyToBekVolume)
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateAndUploadProtectorForVolume(EncryptableVolume vol, Boolean saveKeyToBekVolume)
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateAndUploadOsVolumeProtector()
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.EnableEncryption()
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.HandleEncryptionOperations()
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.OnEnable()".
StartTime: 8/29/2017 6:01:09 PM
EndTime: 8/29/2017 6:02:09 PM
OperationID: 508dd30d-3d78-4354-afa7-cedbe891dd98
Status: Failed
At line:1 char:1
+ Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName 'RG-VM-Dev' - ...
+
    + CategoryInfo          : CloseError: (:) [Set-AzureRmVMDiskEncryptionExtension], ComputeCloudException
    + FullyQualifiedErrorId : Microsoft.Azure.Commands.Compute.Extension.AzureDiskEncryption.SetAzureDiskEncryptionExtensionCommand
```
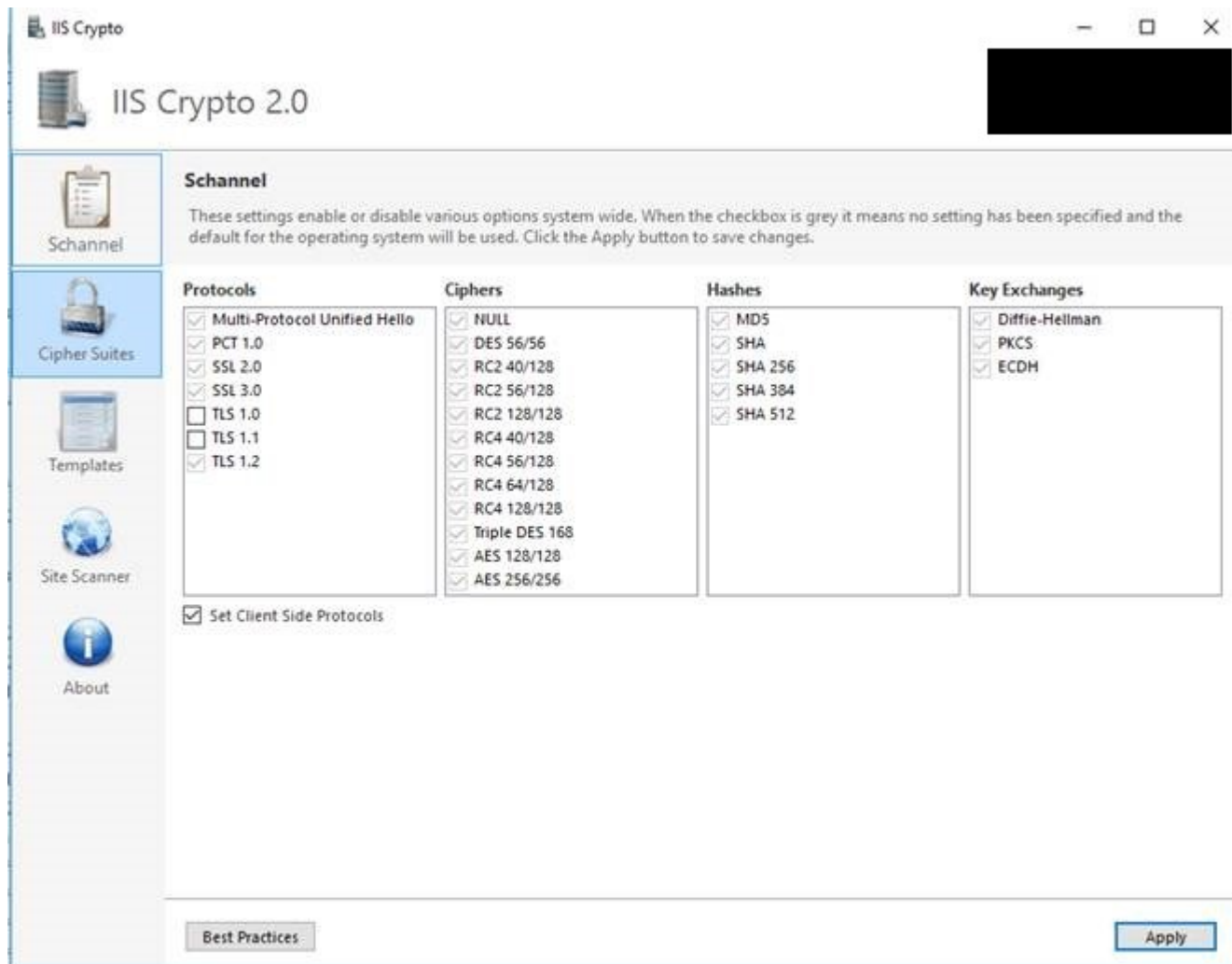
Data Collection

1. Collect the logs from the extension on

   `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.Security.AzureDiskEncryption\<VERSION>`
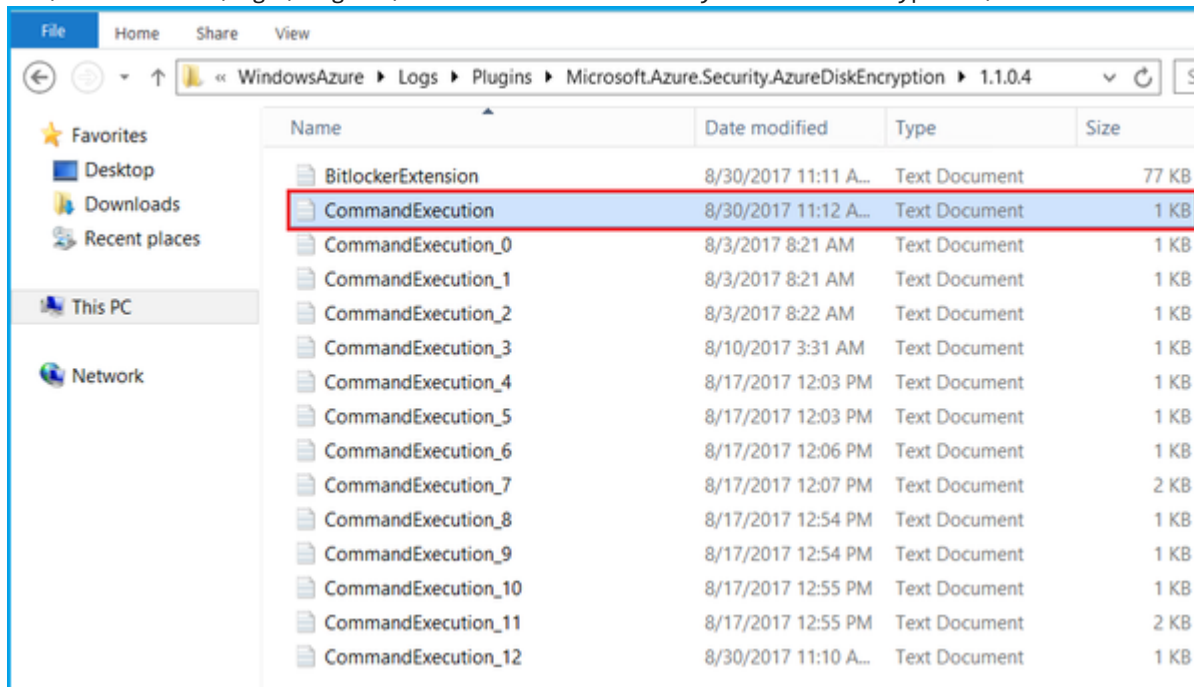
Root Cause Analysis

This may happen if the customer is using TLS 1.2 and the .NET Framework is still pointed to use TLS 2.0 or higher.

Mitigation

1. Deselect TLS 1.0 & 1.1

2. Apply

3. Ensure to add below registry keys so that .Net uses TLS 1.2 only

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
  "SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
  "SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
  "SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
  "SchUseStrongCrypto"=dword:00000001
```

4. Reboot the VM

5. Run the encryption again

Root Cause Closing Code - Service Desk

> ### *Root Cause - Windows Azure\Compute\Virtual Machine\OS Hardening*

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. 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. **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.	Use the **Azure Encryption Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! **Please note** the link to the page is required when submitting kudos!