System Error when Connecting to Azure Files Share_Storage

Last updated by | Kevin Gregoire | Apr 14, 2022 at 9:20 AM PDT

Tags

cw.Azure-Files-All-Topics cw.TSG

Contents

Content replaced

**Content replaced with article: https://supportability.visualstudio.com/AzureIaaSVM/_wiki/wikis/AzureIaaSVM/496199

Symptoms

When the customer tries to connect to an Azure Files share from a Windows machine, they may experience one of the following symptoms:

1. `System Error 53` from 'net use,' or from New-SmbMapping
2. `System Error 67` from 'net use,' or from New-SmbMapping. **This is usually due to TCP Port 445 being blocked, so the LmCompatibilityLevel section does not apply. In some cases you will get error 67 even when Port 445 is opened. In such cases please check whether there are any Antimalware or Antivirus Software's installed on the VM. If yes, please uninstall the Antimalware or Antivirus Software's and try mounting the File share.**
3. `System Error 87` from 'net use,' or from New-SmbMapping. This error should appear when the **LmCompatibilityLevel** on the client is set to value other than 3.
4. `Error code: 0x80070035` when mapping a drive from Windows Explorer. (This is a translation of Error 53; it is an error mask (0x80070000) OR'd with 53 in hex (0x35).)
5. `System Error 86` from 'net use' . This error appears when the password provided along with the net use command is bad.

Cause

Error 53 is ERROR_BAD_NETPATH, which is "The network path was not found." It is a generic error message that is logged when the SMB client is not able to communicate with the Azure Files server.

To resolve the issue, you will need to investigate why the Windows client cannot communicate with Azure Files.

Resolution

Use Azure Files troubleshooter Script to identify the issue

The below link provides guidance to use Azure file troubleshooter to find /Fix common Azure files connectivity issues while using Windows /Linux Clients.

Azure/Storage/TSG/Azure Files connectivity troubleshooter:

```
https://supportability.visualstudio.com/AzureIaaSVM/_wiki/wikis/AzureIaaSVM/495826
```

Step by Step process to Isolate and fix the issue

Below are steps to troubleshoot and resolve Error 53 and similar issues on a Windows client machine.

1. Check the Client operating system used by customer to see if its compatible with Azure files requirements: Azure/Storage/Docs/OS Restrictions for Azure Files
    1. Accessing File shares over the network is done through a protocol called SMB (Server Message Block) and this protocol has a few versions supported by each client.
    2. The client must support SMB 2.1 to access the share from a VM in the same region as the share. It must support SMB 3.0 and SMB encryption to access the share from the Internet.
2. Check DNS name resolution.
    1. Ask the customer to ping the Files storage URL, and check that it resolves to an Azure IP address.
        1. Any network communication needs to start with name resolution. Making sure we can resolve the URL to a valid IP address is a good test to make sure name resolution is working.

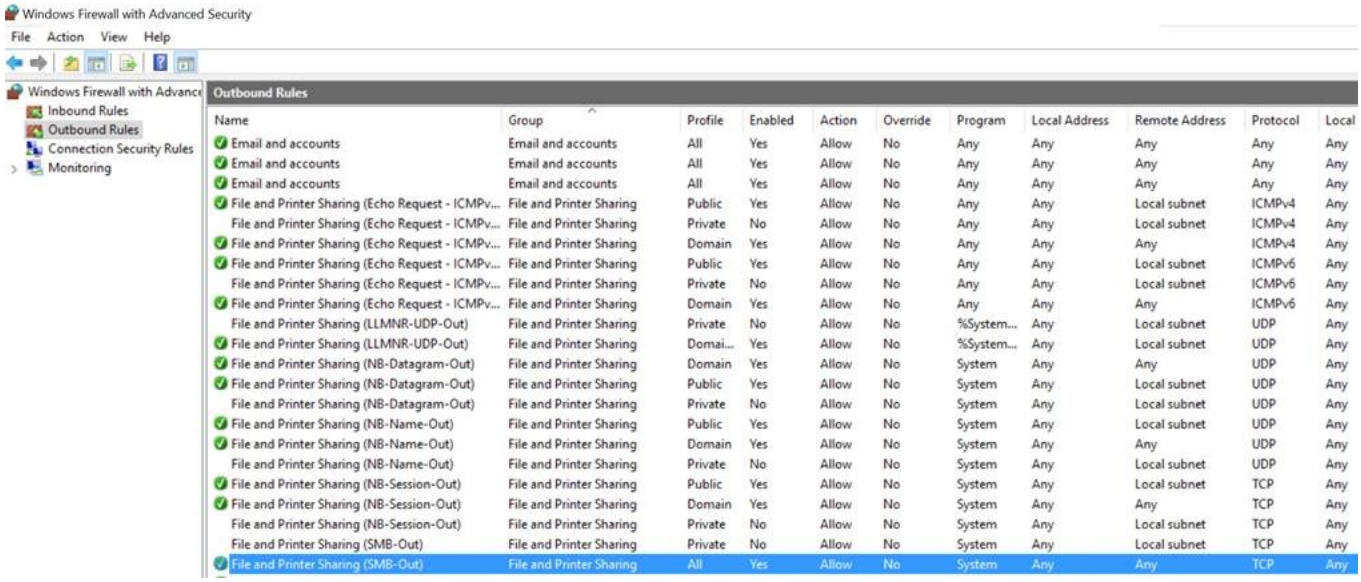
2. The IP address that is resolved for *.file.core.windows.net will be different than the IP address that is resolved for *.blob.core.windows.net, *.table.core.windows.net, or *.queue.core.windows.net.
3. SMB connectivity events will be logged under: Application and services logs > Microsoft > SMBClient > Connectivity You can get to this event log by running "%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx" For windows Client you will see an Event id 30800 for any Name resolution failures Log Name: Microsoft-Windows-SmbClient/Connectivity Source: Microsoft-Windows-SMBClient Date: 2016-10-05 10:01:07 AM Event ID: 30800 Task Category: None Level: Error Keywords: (64) User: SYSTEM Computer: XXXXXXX.domain.com Description: The server name cannot be resolved. Error: The object was not found. Server name: gnx001 Guidance: The client cannot resolve the server address in DNS or WINS. This issue often manifests immediately after joining a computer to the domain, when the client's DNS registration may not yet have propagated to all DNS servers. You should also expect this event at system startup on a DNS server (such as a domain controller) that points to itself for the primary DNS. You should validate the DNS client settings on this computer using IPCONFIG /ALL and NSLOOKUP.
4. You may use the below PsPing command to check on name resolution and port connectivity.

3. Check if communication can occur over TCP Port 445.
   1. "System Error 53" when mounting an Azure File share can occur if outbound traffic on TCP Port 445 is blocked before it reaches the Azure Files data center.
   2. Is this an an internal (Microsoft) customer?
      1. MSIT blocks outgoing traffic from CorpNet over port 445. You will not be able to connect to the Azure Files share from CorpNet.
   3. Use PsPing to verify the client can communicate on TCP Port 445
      1. PsPing is a Sysinternals tool which can be downloaded here: https://technet.microsoft.com/en-us/sysinternals/psping.aspx
         1. Usage: `psping <Storage Account Name>.file.core.windows.net 445`
      2. If the result is `Request timed out` it indicates communication cannot occur over TCP Port 445.
   4. Use PortQry to query the TCP:445 endpoint.
      1. PortQry can be downloaded from here: https://www.microsoft.com/en-us/download/details.aspx?id=17148
         1. Usage: `PortQry.exe -n [Storage Account name].file.core.windows.net -p TCP -e 445`
         2. For more information on using PortQry, see https://support.microsoft.com/kb/310099.
      2. If the result is `TCP port 445 (microsoft-ds service): FILTERED` it indicates TCP 445 being blocked by a rule along the network path.
   5. If the customer is trying to access this port over internet, it might be blocked by their Internet Service Provider (ISP).
      1. Comcast and some IT organizations block this port. Follow this article to get unblocked such situations: Azure/Storage/TSG/What to do when an ISP Blocks TCP port 445
      2. SMB connectivity events could be seen under: \Winevt\Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx
      3. You will see Event 30803 when the connection attempt to any file share fails from a Windows Clients Log Name: Microsoft-Windows-SmbClient/Connectivity Source: Microsoft-Windows-SMBClient Date: 2016-10-05 3:05:29 PM Event ID: 30803 Task Category: None Level: Error Keywords: (64) User: SYSTEM Computer: Compter.domain.com Description: Failed to establish a network connection. Error: {Device Timeout} The specified I/O operation on%hs was not completed before the time-out period expired. Server name: gn001 Server address: 150.59.9.220:445 Connection type: Wsk Guidance: This indicates a problem with the underlying network or transport, such as with TCP/IP, and not with SMB. A firewall that blocks TCP port 445, or TCP port 5445 when using an iWARP RDMA adapter, can also cause this issue.

4. Check if the Virtual Machine is part of an Corporate domain.
   1. If the Virtual Machine is part of a domain, check if Windows Firewall settings are implemented via Group Policy Object (GPO).
      1. Most times when firewall policies are applied by organizations, the ability to add rules would be blocked at this point ask customer to work with their domain admins to add firewall rules to allow outbound SMB communication.

      2. Furthermore check if the Customer had assigned any Network security group to the Virtual machines as a part of Security compliance which could be Blocking traffic to the Azure file Storage services. If such is the case you would see the State of the Virtual machines would show up as failed as Agent service needs to communicate to the storage account to update the Status: https://blogs.msdn.microsoft.com/mast/2016/04/27/vm-stuck-in-updating-when-nsg-rule-restricts-outbound-internet-connectivity

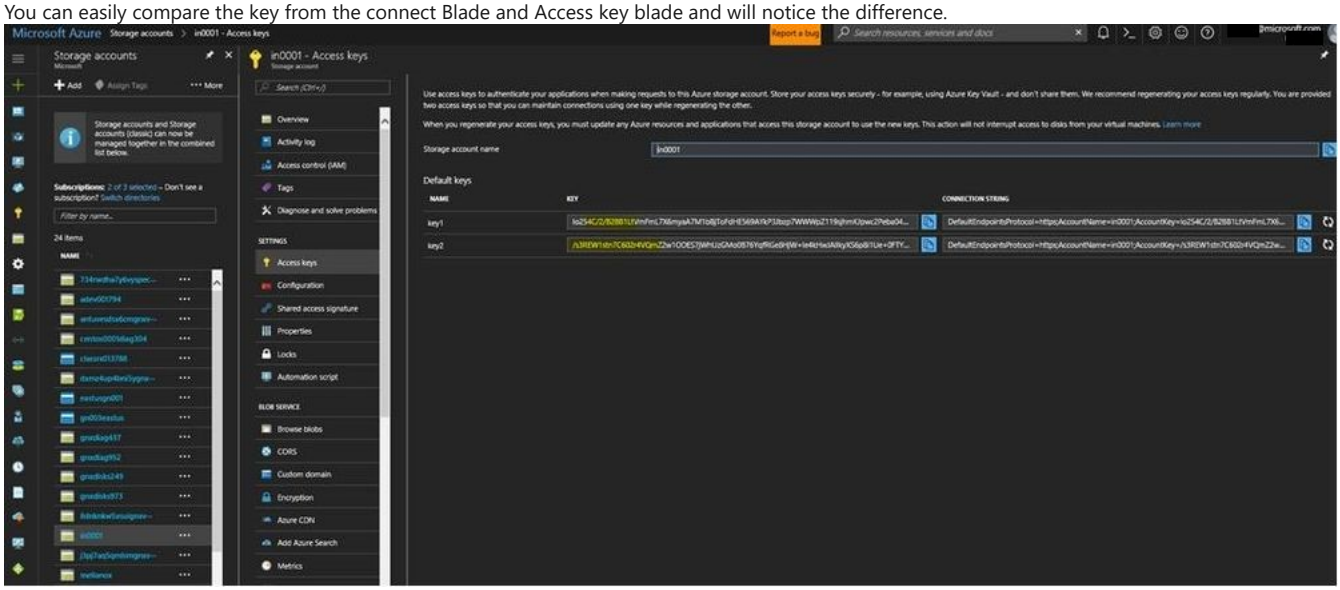
      3. Immediate Mitigation would be to suggest customer to create Network Security Group (NSG) rules to allow traffic from Virtual Machine to the Azure Storage (blobs/Files/Tables/Queues) IP address. This should restore connectivity to the storage.

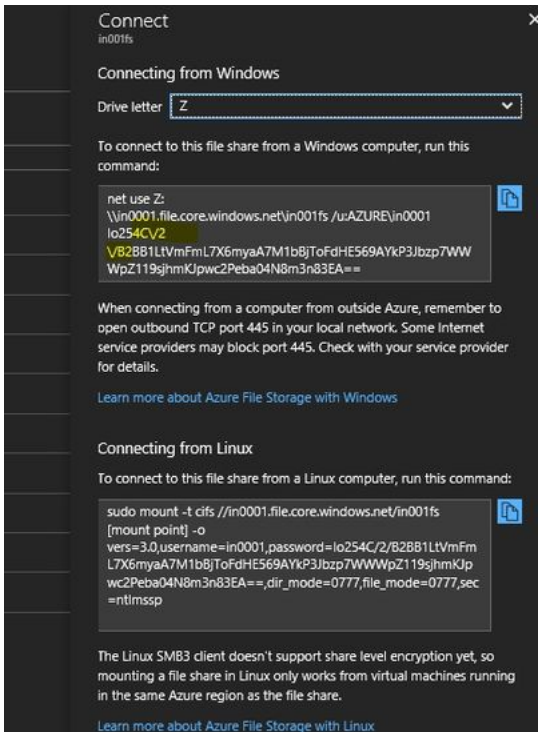


Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local
Email and accounts	Email and accounts	All	Yes	Allow	No	Any	Any	Any	Any	Any
Email and accounts	Email and accounts	All	Yes	Allow	No	Any	Any	Any	Any	Any
Email and accounts	Email and accounts	All	Yes	Allow	No	Any	Any	Any	Any	Any
File and Printer Sharing (Echo Request - ICMPv...	File and Printer Sharing	Public	Yes	Allow	No	Any	Any	Local subnet	ICMPv4	Any
File and Printer Sharing (Echo Request - ICMPv...	File and Printer Sharing	Private	No	Allow	No	Any	Any	Local subnet	ICMPv4	Any
File and Printer Sharing (Echo Request - ICMPv...	File and Printer Sharing	Domain	Yes	Allow	No	Any	Any	Any	ICMPv4	Any
File and Printer Sharing (Echo Request - ICMPv...	File and Printer Sharing	Public	Yes	Allow	No	Any	Any	Local subnet	ICMPv6	Any
File and Printer Sharing (Echo Request - ICMPv...	File and Printer Sharing	Private	No	Allow	No	Any	Any	Local subnet	ICMPv6	Any
File and Printer Sharing (Echo Request - ICMPv...	File and Printer Sharing	Domain	Yes	Allow	No	Any	Any	Any	ICMPv6	Any
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	Private	No	Allow	No	%System...	Any	Local subnet	UDP	Any
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	Domai...	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any	Any	UDP	Any
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Public	Yes	Allow	No	System	Any	Local subnet	UDP	Any
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Private	No	Allow	No	System	Any	Local subnet	UDP	Any
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Public	Yes	Allow	No	System	Any	Local subnet	UDP	Any
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any	Any	UDP	Any
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Private	No	Allow	No	System	Any	Local subnet	UDP	Any
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Public	Yes	Allow	No	System	Any	Local subnet	TCP	Any
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any	Any	TCP	Any
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Private	No	Allow	No	System	Any	Local subnet	TCP	Any
File and Printer Sharing (SMB-Out)	File and Printer Sharing	Private	No	Allow	No	System	Any	Local subnet	TCP	Any
File and Printer Sharing (SMB-Out)	File and Printer Sharing	All	Yes	Allow	No	System	Any	Any	TCP	Any

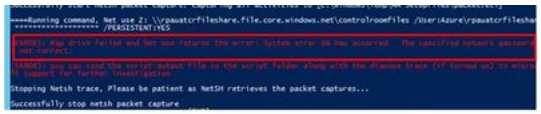
This screenshot is an example of an outbound firewall rule which allows TCP port 445 to any destination, and applies to all Firewall profiles.

5. Confirm that NTLMv2 authentication is enabled on the Windows client.
    1. Having NTLMv1 enabled creates a less secure client, and therefore communication will be blocked for Azure Files.
    2. If you try accessing the same file share from a VM or on-premise machine that is not domain joined, does it work as expected?
        1. NTLMv1 authentication is usually enforced through Group Policy. For example, on domain-joined machines. Therefore, a non-domain-joined machine likely has the default NTLMv2 authentication enabled.
    3. To confirm the customer is using NTLMv2, verify the following registry value is set to **3** in the registry:
    `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\LmCompatibilityLevel`
        1. On **multiple machines or in a domain**, it is recommended to apply this setting via Group Policy. The relevant Group Policy setting is "Send NTLMv2 response only." Ensuring this policy is applied to the clients will prevent this error from occurring, and is also considered a security best practice.
            1. The following article describes how to configure clients to use NTLMv2 using Group Policy: https://technet.microsoft.com/en-us/library/jj852207(v=ws.11).aspx
            2. Make sure to run `gpupdate /force` from an elevated Command Prompt after applying this policy, and restart the machine that is having trouble connecting.
        2. On a **single machine**, if the above registry value is set to a value other than 3, change it back to the default (3) and restart.
6. If the customer gets `System error 86 has occurred. The specified network password is not correct` , the User ID or password used to connect to the Azure Files share is wrong.
7. There is a recent portal issue were the access key included in the net use command through the connect blade is encoded. If the original access key had "/" then the portal encodes and includes character "\" , this end up with extra characters in the access key. Using the password along with the net use command in connect blade thus will end up in `System error 86 has occurred.The specified network password is not correct` , the Fix is being worked on ICM: 49162433 . The work around to this issue would be to get the password from the Storage account's access Key blade and use it along with the net use command.
    1. You can easily compare the key from the connect Blade and Access key blade and will notice the difference.





For Scenario 5 at Symptoms section
Customer unable to mount Azure files on VMs. They were getting the following error message
[Error]: Map Drive failed and Net use returns the error: **System error 86 has occurred**. The specified network password is not correct.



Cause : All the VMs were part of on premise AD and the custom DNS failed to resolve the storage account.

Resolution : Customer followed the below resolution,

1. Need to create external Microsoft DNS VIP (168.63.129.16) on the VM NIC level or Subnet level (or)
2. Need to create conditional forwarder in internal DNS to query external DNS name resolution to resolve Microsoft DNS name (Windows.net)

Case Coding

Please use one of the following Root Cause buckets when closing a case that was resolved by this TSG:

Root Cause - Windows Azure\Storage\Files\Connectivity or

Root Cause - Windows Azure\Storage\Files\Connectivity\Authentication Errors

More Information

To troubleshoot a similar error message on a Linux machine, please see: Azure/Storage/TSG/Errors when trying to mount an Azure Files share on Linux

The following public article describes how to use Azure Files with Windows: https://azure.microsoft.com/en-us/documentation/articles/storage-dotnet-how-to-use-files/

Need additional help or have feedback?

To engage the Azure Files All Topics SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **Azure Files All Topics SMEs** AVA channel via Teams. Make sure to use the **Ava process** for faster assistance.	Use the **Azure Files All Topics Feedback** form to submit detailed feedback on improvements or new content ideas for Azure Files All Topics. ***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 Files All Topics 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!