Unable to Connect to Azure Files Over Reboot_Storage

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

Tags

cw.Azure-Files-All-Topics	cw.TSG	cw.Reviewed-03-2021

Contents

Symptoms

Customer observes that the mapped Azure Files drive shows a red "X" after a reboot, though Azure Files share credentials were added using cmdkey. After reboot, the customer needs to double-click on the Azure Files mapped drive to get connected and there is a 15-30 second delay in connecting to the mapped drive.

Cause

This issue can happen because of multiple reasons:

1. Name resolution issues: The client OS was not able to resolve the IP address of the Azure Files endpoint.
2. When a Windows machine is part of an Active Directory Domain, Windows Explorer is programmed to call the most secure authentication mechanism which is Kerberos. This results in the client contacting a key distribution center (KDC) to look for a ticket which is causing the delay. This behavior is a default design for Windows Explorer.
3. The customer might also see this issue if other elements of the command line have a forward slash, such as the Storage Account name or share name. The following wiki will help resolve that: https://supportability.visualstudio.com/AzureIaaSVM/_wiki/wikis/AzureIaaSVM/496191

Solution

1. Customer can create an Serice Principal Name in Active directory for the File share resource and add an AD user account using the Storage Account name and key.

2. Customer can create a File services server (Windows/Linux) and add it to the Active directory domain and use it.

Next Steps

Create a collaboration to the Windows Networking team using the following Support Area Path (SAP): Windows Servers/Windows Server <Windows Server Version>/<Windows Server Version>/Network Connectivity and File Sharing/Access to file shares (SMB)

Log collection

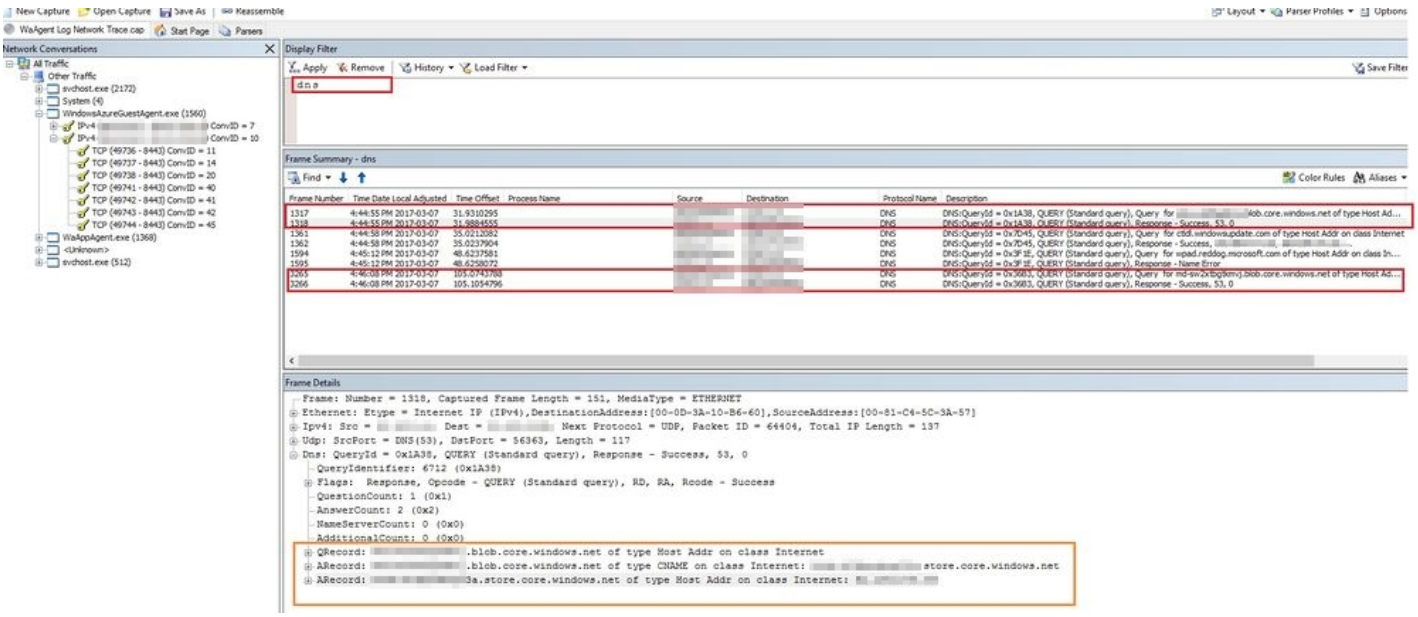
The purpose of this log collection is to help speed up the case by already having a network trace once the Windows team is engaged, so that they have logs to look at. It is **not** expected for VM engineers to troubleshoot the network trace themselves.

1. Open up an elevated command line, and run `ipconfig /flushdns`
2. Put t.cmd.2008.txt on the C: drive of the problem server, and rename it to "T.cmd"
3. From an elevated Command Prompt, type `t.cmd clion`
4. Type `netsh trace start scenario=filesharing capture=yes report=yes tracefile=c:\Fileshareerror.etl`
5. Reproduce the Azure Files access issue.
6. From the command line, type `t.cmd clioff` and `netsh trace stop`
7. On the root of the C: drive, you will find three files: "T.cab, "Fileshareerror.etl," "Fileshareerror.cab>" Save these files for analysis.

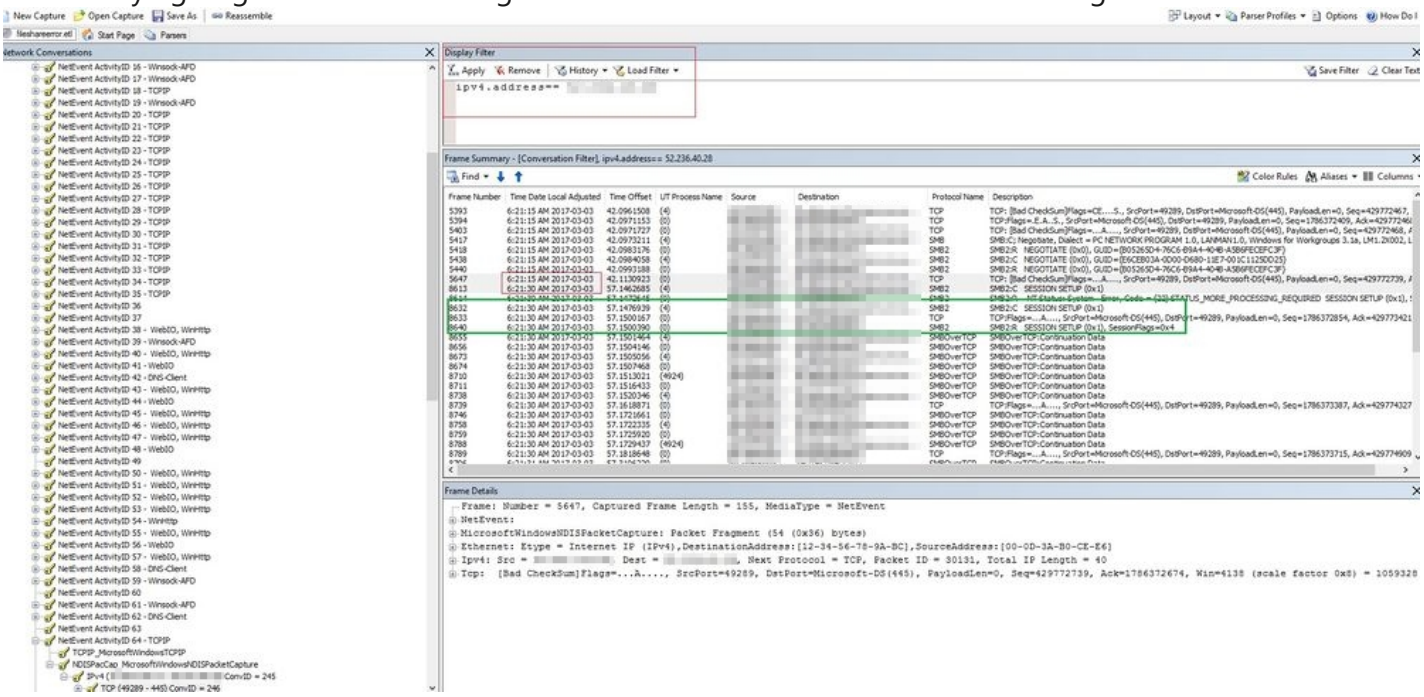
What to lookout for in the traces

It is not expected for Azure VM POD Engineers to look at this logging, and this information is purely to help your own understanding, and help the Windows Networking and Directory Services teams to provide a faster mitigation.

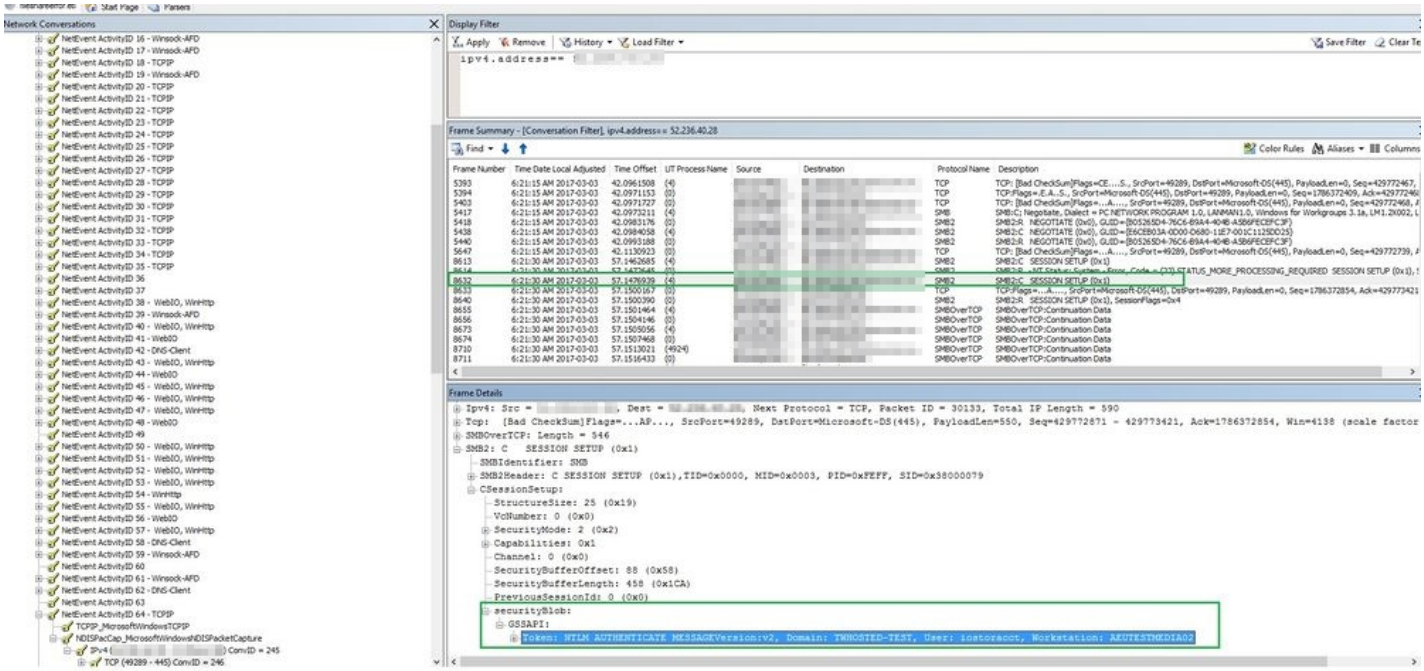
1. Install Network Monitor 3.4: https://www.microsoft.com/en-us/download/details.aspx?id=4865
2. Launch NetMon in Administrator mode.
3. Click on the "New Capture" button, and then the "Start" Button to start the capture.
4. From an elevated Command Prompt, type `ipconfig /flushdns`
5. Allow the capture to run for a minute or two, then stop and save the capture.
6. Under Display Filters, type "DNS" and click on Apply to filter out only DNS traffic. Use the frame details to get the name of the Storage Account, and the ipaddress of the stamp:



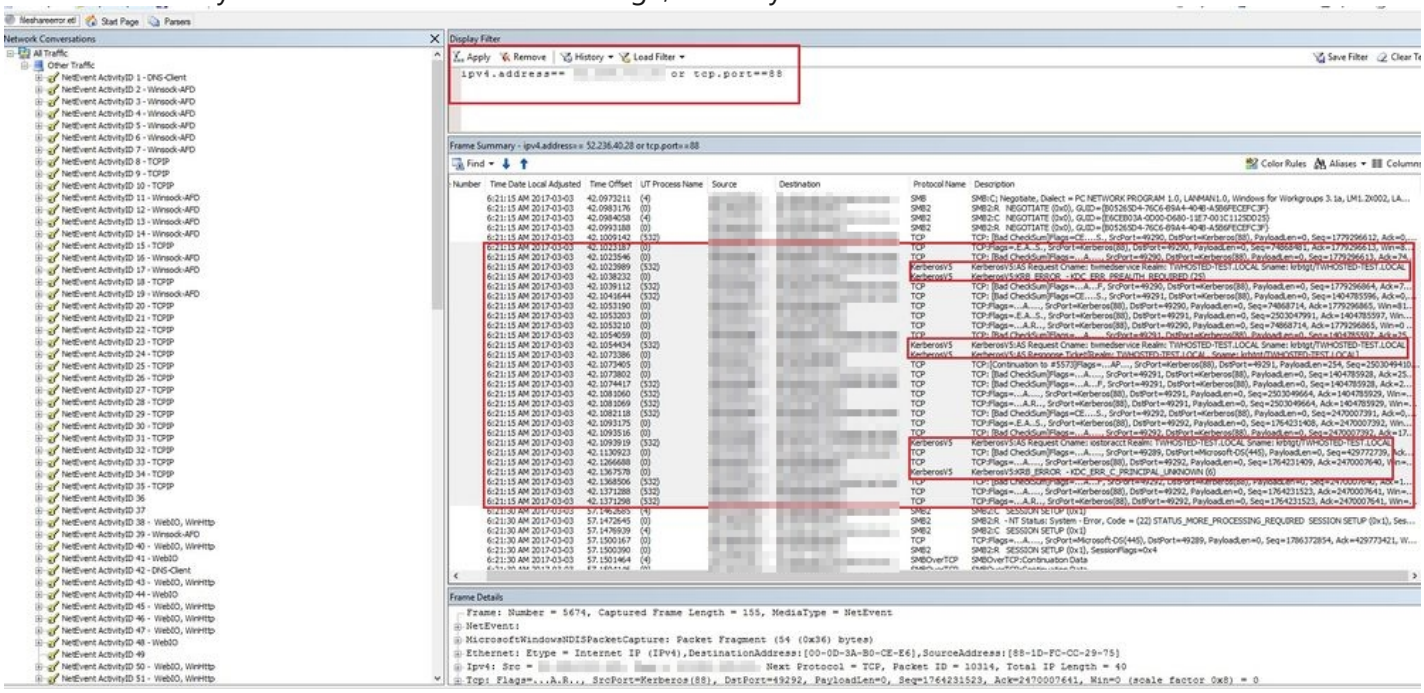
7. Look through the response, and you will see the ipaddress of the stamp hosting the File share.
8. Now, under Display Filter, type `ipv4.address == <ipaddress of the resolved Azure Files service>` and click on Apply on the display filter to filter traffic to the Azure Files service.
9. As shown below, if you see a delay in the client sending the right credentials, there is a good chance the client is trying to get to a local DC to get a Kerberos ticket for the Azure Files storage service:



10. You can also observe that after the 15 secs delay, the client did send the right credentials; that's recorded in frame 8632, for which we get a positive response from the server (Frame 8640).
11. If we look into the frame details of 8632 under the "securityBlob" section, we can see the user account being tried. Frame 8640 is a response from Files server that the authentication was a success:



12. Using the display filter `ipv4.address== <IP address of the resolved Azure file service> or tcp.port==88` we can now see only SMB traffic to Azure File storage, and any Kerberos traffic to a local Domain Controller:



13. This information could be used to cut a Problem to "Windows Directory Services T2" and "Windows Networking T2."

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!