

# 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](#)
- [Cause](#)
- [Solution](#)
- [Next Steps](#)
- [Log collection](#)
  - [What to lookout for in the traces](#)
- [Need additional help or have feedback?](#)

## 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](https://supportability.visualstudio.com/AzureIaaSVM/_wiki/wikis/AzureIaaSVM/496191)

## Solution

1. Customer can create an Service 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 c:\ion`
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 clloff` 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:

Wireshark network capture showing DNS traffic. The display filter is 'dns'. The frame summary shows a DNS query from the client to the server. The frame details show the query and response details, including the query ID, flags, and the query type.

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1317	4:44:55 PM 2017-03-07	31.9310295				DNS	DNS-QueryId = 0x1A3B, QUERY (Standard query), Query for blob.core.windows.net of type Host Ad...
1318	4:44:55 PM 2017-03-07	31.9884555				DNS	DNS-QueryId = 0x1A3B, QUERY (Standard query), Response - Success, 53, 0
1361	4:44:58 PM 2017-03-07	35.0212382				DNS	DNS-QueryId = 0x2414, QUERY (Standard query), Query for cdk.windowsupdate.com of type Host Addr on class Internet
1362	4:44:58 PM 2017-03-07	35.0237904				DNS	DNS-QueryId = 0x2414, QUERY (Standard query), Response - Success, 53, 0
1394	4:45:12 PM 2017-03-07	48.0217581				DNS	DNS-QueryId = 0x2414, QUERY (Standard query), Query for wpa2.redtop.microsoft.com of type Host Addr on class In...
1395	4:45:12 PM 2017-03-07	48.0268072				DNS	DNS-QueryId = 0x2414, QUERY (Standard query), Response - Name Error
1505	4:46:08 PM 2017-03-07	105.0743768				DNS	DNS-QueryId = 0x3063, QUERY (Standard query), Query for ms-smb2blob.core.windows.net of type Host Ad...
1506	4:46:08 PM 2017-03-07	105.1074796				DNS	DNS-QueryId = 0x3063, QUERY (Standard query), Response - Success, 53, 0

Frame Details

Frame: Number = 1318, Captured Frame Length = 151, MediaType = ETHERNET

Ethernet II Type = Internet IP (IPv4), Destination Address: [00-0D-3A-10-B6-60], Source Address: [00-01-C4-5C-3A-57]

IPv4: Src = [192.168.1.100], Dest = [192.168.1.1], Next Protocol = UDP, Packet ID = 64408, Total IP Length = 137

UDP: SrcPort = DNS(53), DestPort = 54363, Length = 117

Dns: QueryId = 0x1A3B, QUERY (Standard query), Response - Success, 53, 0

QueryIdentifier: 6712 (0x1A3B)

Flags: Response, Opcode = QUERY (Standard query), RD, RA, Recode = Success

QuestionCount: 1 (0x1)

AnswerCount: 2 (0x2)

NameServerCount: 0 (0x0)

AdditionalCount: 0 (0x0)

QRecord: [192.168.1.100].blob.core.windows.net of type Host Addr on class Internet

ARecord: [192.168.1.100].blob.core.windows.net of type CHAME on class Internet: [192.168.1.100].store.core.windows.net

ARecord: [192.168.1.100].3a.store.core.windows.net of type Host Addr on class Internet: [192.168.1.100].

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:

Wireshark network capture showing a Kerberos authentication attempt. The display filter is 'ipv4.address == 192.168.1.100'. The frame summary shows a Kerberos authentication attempt. The frame details show the authentication attempt details, including the client name, target name, and the authentication data.

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
5393	6:21:15 AM 2017-03-07	42.0961508				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=429772467, TCPFlags=E.A.S., SrcPort=Microsoft-DG(445), DestPort=49289, PayloadLen=0, Seq=1786372495, Ack=429772467
5394	6:21:15 AM 2017-03-07	42.0971153				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786372495, Ack=429772467
5403	6:21:15 AM 2017-03-07	42.0973727				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786372495, Ack=429772467
5417	6:21:15 AM 2017-03-07	42.0973211				SMB	SMB2: Negotiate, dialect = PC NETWORK PROGRAM 1.0, LANMAN1.0, Windows for Workgroups 3.1a, LM1.2K002.1
5418	6:21:15 AM 2017-03-07	42.0983176				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5438	6:21:15 AM 2017-03-07	42.0984958				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5440	6:21:15 AM 2017-03-07	42.0991388				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=429772739, Ack=429772467
5447	6:21:15 AM 2017-03-07	42.1130923				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=429772739, Ack=429772467
5647	6:21:30 AM 2017-03-07	57.1462685				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5648	6:21:30 AM 2017-03-07	57.1462685				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5649	6:21:30 AM 2017-03-07	57.1462685				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5650	6:21:30 AM 2017-03-07	57.1462685				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5651	6:21:30 AM 2017-03-07	57.1462685				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5652	6:21:30 AM 2017-03-07	57.1462685				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5653	6:21:30 AM 2017-03-07	57.1500857				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786372854, Ack=429772421
5654	6:21:30 AM 2017-03-07	57.1500857				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786372854, Ack=429772421
5655	6:21:30 AM 2017-03-07	57.1500857				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786372854, Ack=429772421
5656	6:21:30 AM 2017-03-07	57.1504146				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5657	6:21:30 AM 2017-03-07	57.1505056				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5658	6:21:30 AM 2017-03-07	57.1507468				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5659	6:21:30 AM 2017-03-07	57.1507468				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5660	6:21:30 AM 2017-03-07	57.1513021				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5661	6:21:30 AM 2017-03-07	57.1514433				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5662	6:21:30 AM 2017-03-07	57.1520346				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5663	6:21:30 AM 2017-03-07	57.1520346				SMB2	SMB2: NEGOTIATE (0x0), GUID=00526504-76C5-68A4-404B-436FECFC3F
5664	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5665	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5666	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5667	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5668	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5669	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5670	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5671	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5672	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5673	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5674	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5675	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5676	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5677	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5678	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5679	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5680	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5681	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5682	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5683	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5684	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5685	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5686	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5687	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5688	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5689	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5690	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5691	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5692	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5693	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5694	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5695	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5696	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5697	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5698	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5699	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5700	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5701	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5702	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5703	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5704	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5705	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5706	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5707	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5708	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort=49289, DestPort=Microsoft-DG(445), PayloadLen=0, Seq=1786373287, Ack=429774327
5709	6:21:30 AM 2017-03-07	57.1568871				TCP	TCP: Bad CheckSum/Flags=CE...S, SrcPort

Display Filter: `ip4.address==`

Frame Summary: [Conversation Filter] ip4.address==52.236.40.28

Frame Details:

- IP: Src = ..., Dest = ..., Next Protocol = TCP, Packet ID = 30133, Total IP Length = 590
- TCP: [Bad Checksum] Flags... .AP... , SrcPort=49289, DestPort=Microsoft-DS(445), PayloadLen=550, Seq=429772781 - 429773421, Ack=1786372854, Win=4138 (scale factor ...)
- SMBOverTCP: Length = 546
- SMB2: C SESSION SETUP (0x1)
  - SMBIdentifier: SMB
  - SMBHeader: C SESSION SETUP (0x1), TID=0x0000, MID=0x0000, PID=0xFFFE, SID=0x80000079
  - CSessionSetup:
    - StructureSize: 25 (0x19)
    - Volume: 0 (0x0)
    - VolumeMode: 2 (0x2)
    - Capabilities: 0x1
    - Channel: 0 (0x0)
    - SecurityBufferOffset: 88 (0x58)
    - SecurityBufferLength: 458 (0x1CA)
    - PreviousSessionId: 0 (0x0)
    - SecurityBlob:
      - GSASAPI:
        - Token: WIN AUTHENTICATE MESSAGEVersion: v2, Domain: TWOHOSTED-TEST, User: Administrator, Workstation: ASUTESTMEDIAD2

12. Using the display filter `ip4.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:

Display Filter: `ip4.address== 52.236.40.28 or tcp.port==88`

Frame Summary: ip4.address== 52.236.40.28 or tcp.port==88


Frame Details:

- Frame Number = 5674, Captured Frame Length = 155, Media Type = NetEvent
- NetEvent:
  - MicrosoftWindowsDefenderSecurity: Packet Fragment (54 (0x36) bytes)
  - Ethernet II Type = Internet IP (IPv4), Destination Address: [00-0D-3A-B0-CE-F6], Source Address: [88-1D-FC-0D-29-75]
  - IP: Src = ..., Next Protocol = TCP, Packet ID = 10314, Total IP Length = 40
  - TCP: Flags = ...A.R... , SrcPort=Kerberos(88), DestPort=Kerberos(88), Seq=247007641, Win=0 (scale factor 0x8) = 0

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?



<i>To engage the Azure Files All Topics 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 Files All Topics SMEs</a>  AVA channel via Teams.</p> <p>Make sure to use the <a href="#">Ava process</a> for faster assistance.</p>	<p>Use the <a href="#">Azure Files All Topics Feedback</a> form to submit detailed feedback on improvements or new content ideas for Azure Files All Topics.</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 Files All Topics 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>