Troubleshoot Remote File System Configuration Issues for Secure Network Analytics Appliances.

Contents

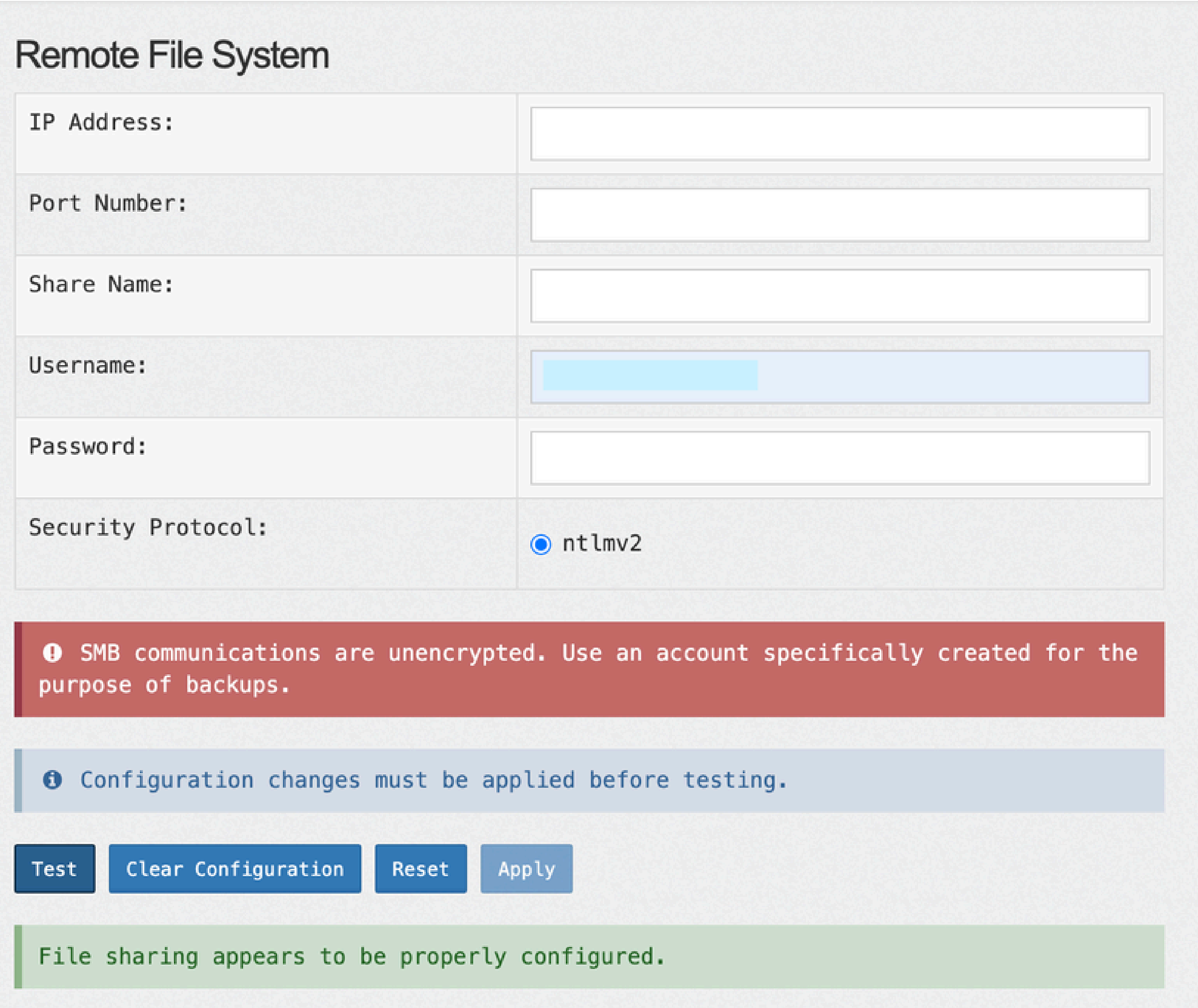
Introduction

This document describes how to troubleshoot remote file system configuration issues for SNA (Secure Network Analytics) version 7.5.2 onwards.

Remote File System Configuration

Remote file system configuration is essential for creation of database backup in DDS (Distributed Database system) environment. It uses CIFS (Common Internet File Share) protocol also known as SMB (Server Message Block).

When SNA appliance initiates test connection with configured remote file system it performs series of steps before announcing "File sharing appears to be properly configured" message.



Remote File System

IP Address:	
Port Number:	
Share Name:	
Username:	
Password:	
Security Protocol:	● ntlmv2

SMB communications are unencrypted. Use an account specifically created for the purpose of backups.

Configuration changes must be applied before testing.

File sharing appears to be properly configured.

Successful SMB Test

- The client initiates a connection to the server (remote file directory) using TCP/IP over port 445.
- The CIFS protocol utilises NetBIOS for name resolution and session establishment when using port 139 or directly over TCP when using port 445.
- The client and server negotiate the protocol version to use. This ensures compatibility between the client and server.
- The server responds with a list of supported protocol dialects, and the client selects the most appropriate one.
- The client sends a session setup request, which includes authentication credentials.
- Authentication is performed using mechanisms ntlmv2.
- Upon successful authentication, the server establishes a session and assigns a unique session ID to the client.
- The client sends a tree connect request to access a specific shared resource.
- The server validates the request and provides a tree ID, which the client uses for subsequent operations on the resource.
- The client can now perform operations such as reading, writing, or modifying files on the shared resource.
- CIFS supports features like file locking and concurrent access to ensure data integrity.
- Once the client has completed its operations, it sends a log off request to terminate the session.
- The server releases the session ID and associated resources.

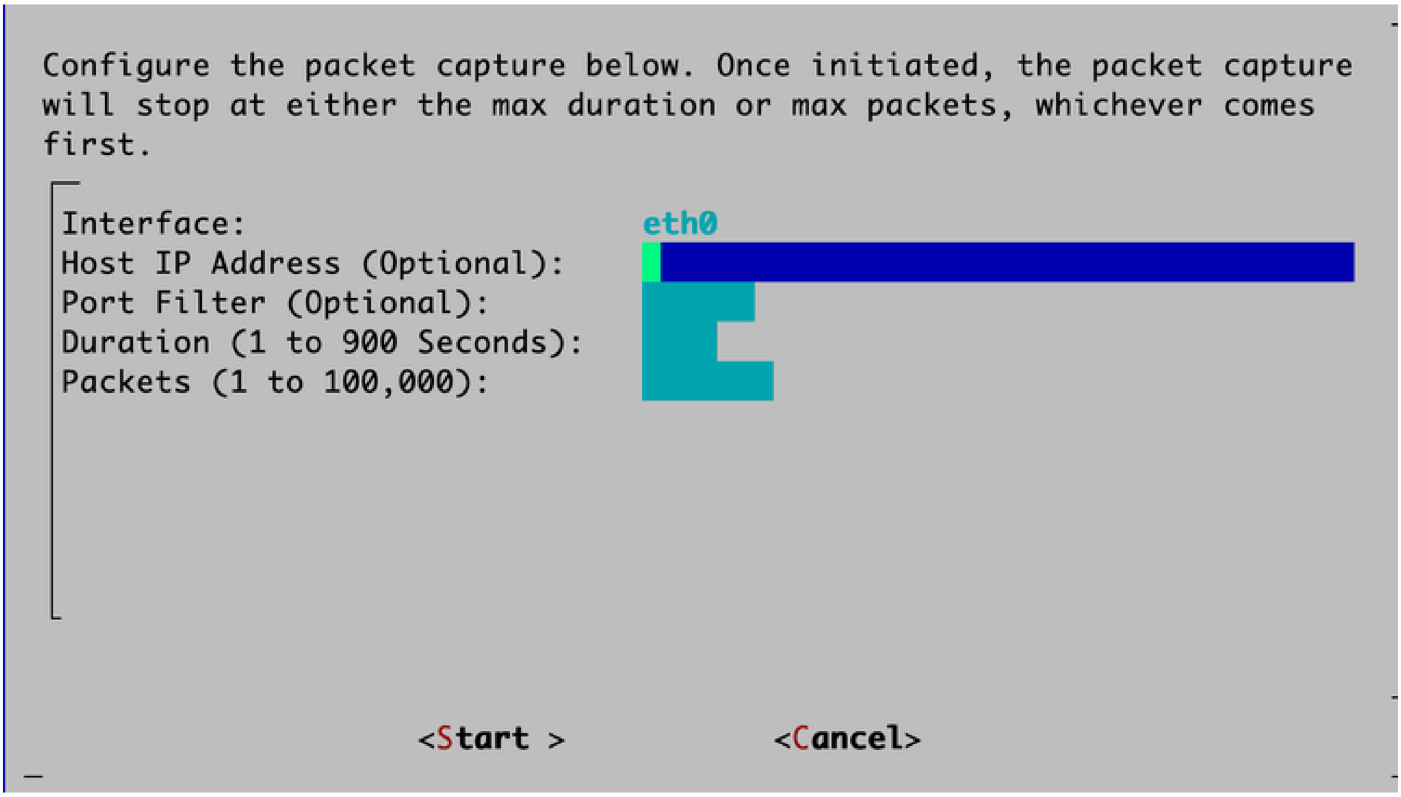
Procedure

A very common issue encounter while configuring remote file system for SNA devices is "Failed to mount" error.

To better understand what caused the issue, please proceed as follows:

Initiate Packet Capture

- Log in to SNA appliance CLI using **sysadmin** credentials.
- Navigate to **Advanced** > **Packet Capture**
- Enter remote share **IP address under Host IP Address**, **445 as Port Filter, Minimum 60 sec, 100 as duration and packet** respectively



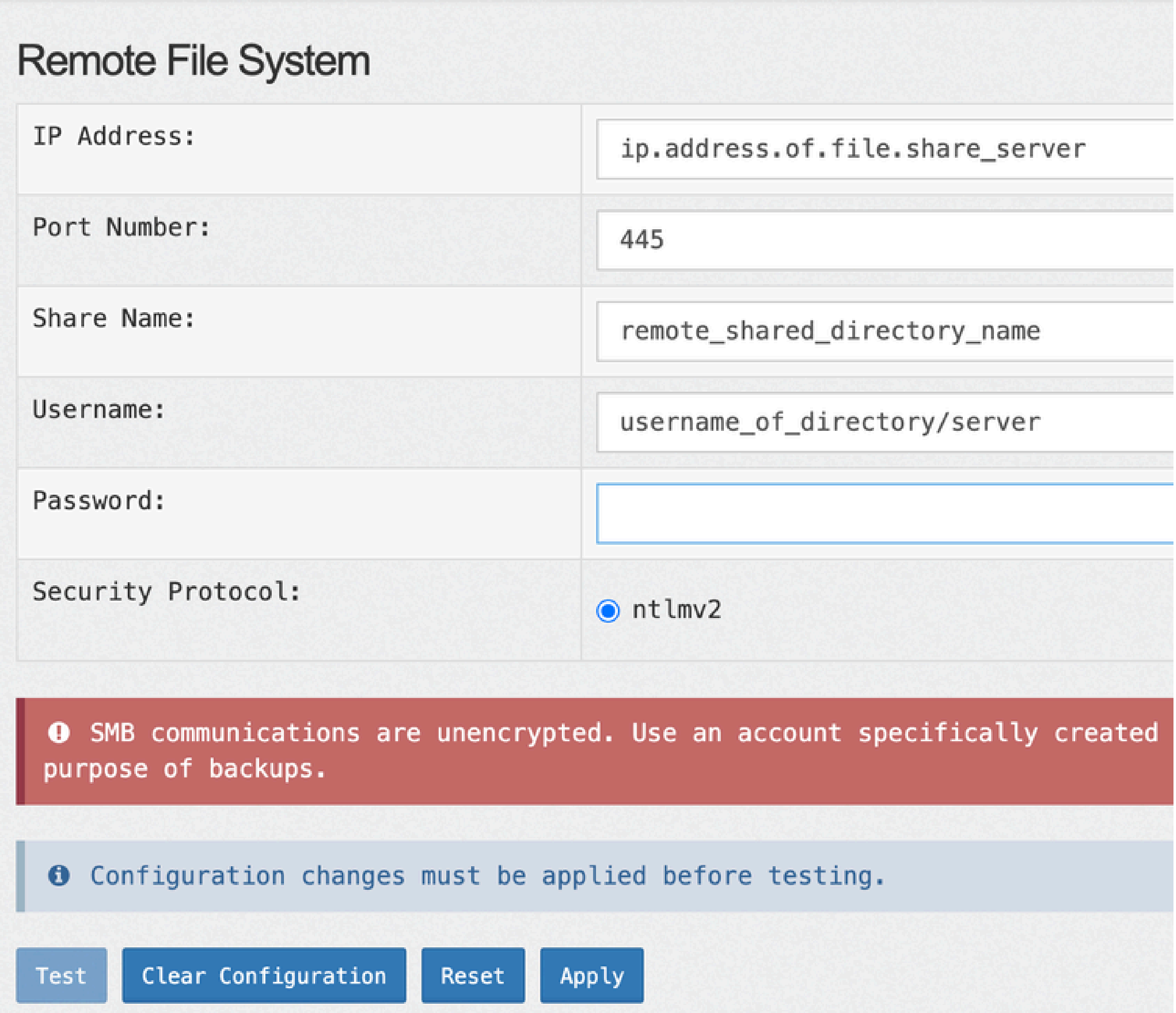
```
Configure the packet capture below. Once initiated, the packet capture
will stop at either the max duration or max packets, whichever comes
first.

 Interface:                     eth0
 Host IP Address (Optional):
 Port Filter (Optional):
 Duration (1 to 900 Seconds):
 Packets (1 to 100,000):
```

Packet Capture from CLI

Configure and Test Remote File System

- Log in to SNA appliance UI and navigate to **Configuration** > **Remote File System**



Remote File System

IP Address:	ip.address.of.file.share_server
Port Number:	445
Share Name:	remote_shared_directory_name
Username:	username_of_directory/server
Password:	
Security Protocol:	● ntlmv2

SMB communications are unencrypted. Use an account specifically created
purpose of backups.

Configuration changes must be applied before testing.

Remote Share Configurations

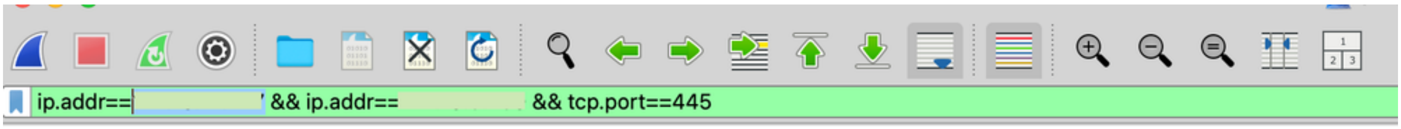
- Click **Apply** and **Test**.

Download and Review Packet capture

- Wait for packet capture to stop or manually interrupt using **CTRL-C**.
- Navigate to **SNA appliance UI** > **Support** > **Browse Files** > **tcpdump**.

Common Error

Open the packet capture and apply filter **ip.addr==ip_address_of_SNA && ip.addr==ip_address_of_remote_storage && tcp.port==445**.

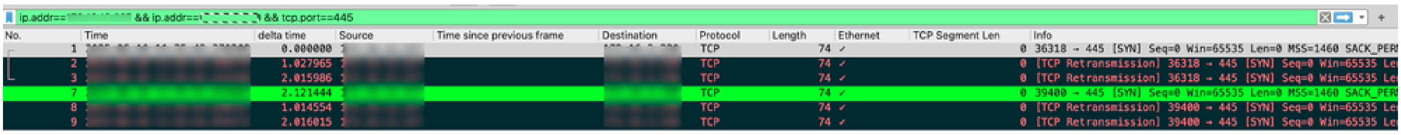


ip.addr==[redacted] && ip.addr==[redacted] && tcp.port==445

Packet Capture Filter

TCP Port 445 Block

No response for multiple **SYN** packet initiated by SNA appliance along with **TCP** retransmission attempts towards remote file server IP address.



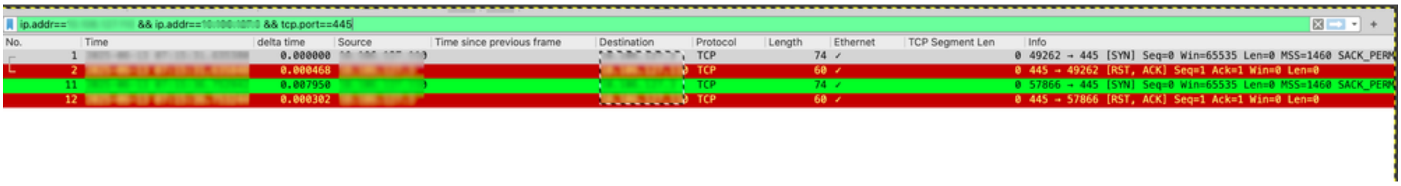
```
ip.addr==[redacted] && ip.addr==[redacted] && tcp.port==445
No.  Time        delta time  Source      Time since previous frame  Destination  Protocol  Length  Ethernet  TCP Segment Len  Info
  1  [redacted]  0.000000    [redacted]                             [redacted]   TCP           74  ✓                        0  36318 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
  2  [redacted]  1.027965    [redacted]                             [redacted]   TCP           74  ✓                        0  [TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Le
  3  [redacted]  2.015986    [redacted]                             [redacted]   TCP           74  ✓                        0  [TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Le
  7  [redacted]  2.121444    [redacted]                             [redacted]   TCP           74  ✓                        0  39400 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
  8  [redacted]  1.014554    [redacted]                             [redacted]   TCP           74  ✓                        0  [TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Le
  9  [redacted]  2.016015    [redacted]                             [redacted]   TCP           74  ✓                        0  [TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Le
```

Port Block

Solution: Allow **TCP/445** port communication between **SNA appliance** and **Remote File Share directory/location** from firewall.

Service Not Running

SNA device initiated **SYN** packet over **TCP port 445** however SMB server respond with **RST,ACK**.



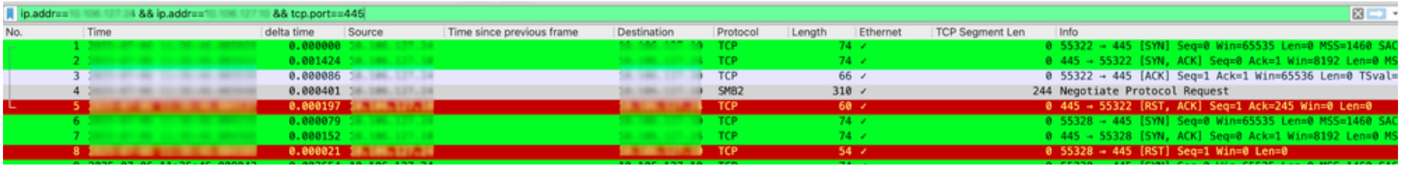
```
ip.addr==[redacted] && ip.addr==[redacted] && tcp.port==445
No.  Time        delta time  Source      Time since previous frame  Destination  Protocol  Length  Ethernet  TCP Segment Len  Info
  1  [redacted]  0.000000    [redacted]                             [redacted]   TCP           74  ✓                        0  49262 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
  2  [redacted]  0.000468    [redacted]                             [redacted]   TCP           60  ✓                        0  445 → 49262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 11  [redacted]  0.007950    [redacted]                             [redacted]   TCP           74  ✓                        0  57866 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
 12  [redacted]  0.000302    [redacted]                             [redacted]   TCP           60  ✓                        0  445 → 57866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

SMB service Not Running

Solution: Initialise SMB File Share on respective server

SMB Version 1/2/3 Disabled

TCP handshake completes successfully however **SMB** negotiation fails due to **SMB version** being disabled.



```
ip.addr==[redacted] && ip.addr==[redacted] && tcp.port==445
No.  Time        delta time  Source      Time since previous frame  Destination  Protocol  Length  Ethernet  TCP Segment Len  Info
  1  [redacted]  0.000000    [redacted]                             [redacted]   TCP           74  ✓                        0  55322 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SAC
  2  [redacted]  0.001424    [redacted]                             [redacted]   TCP           74  ✓                        0  445 → 55322 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
  3  [redacted]  0.000086    [redacted]                             [redacted]   TCP           66  ✓                        0  55322 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=
  4  [redacted]  0.000401    [redacted]                             [redacted]   SMB2         310  ✓                      244  Negotiate Protocol Request
  5  [redacted]  0.000197    [redacted]                             [redacted]   TCP           60  ✓                        0  445 → 55322 [RST, ACK] Seq=1 Ack=245 Win=0 Len=0
  6  [redacted]  0.000079    [redacted]                             [redacted]   TCP           74  ✓                        0  55328 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SAC
  7  [redacted]  0.000152    [redacted]                             [redacted]   TCP           74  ✓                        0  445 → 55328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
  8  [redacted]  0.000021    [redacted]                             [redacted]   TCP           54  ✓                        0  55328 → 445 [RST] Seq=1 Win=0 Len=0
```

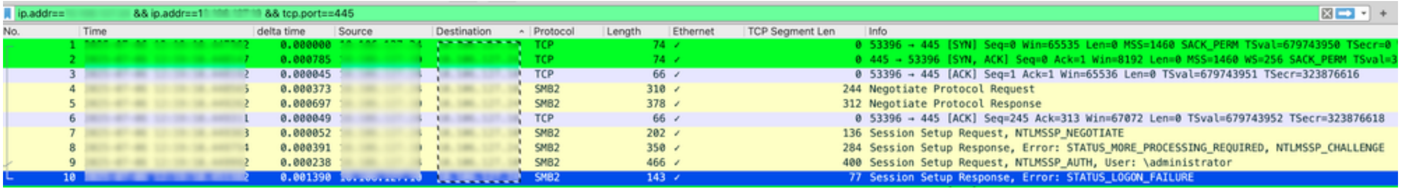
SMB Versions Disabled

Solution: Enable the appropriate SMB version on respective server.

Wrong Password for SMB Share

TCP handshake completes successfully along with **SMB** negotiation.

STATUS_LOGIN_FAILURE response from SMB File share server.



```
ip.addr==[redacted] && ip.addr==[redacted] && tcp.port==445
No.  Time        delta time  Source      Destination  Protocol  Length  Ethernet  TCP Segment Len  Info
  1  [redacted]  0.000000    [redacted]  [redacted]   TCP           74  ✓                        0  53396 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=679743950 TSecr=0
  2  [redacted]  0.000785    [redacted]  [redacted]   TCP           74  ✓                        0  445 → 53396 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=3
  3  [redacted]  0.000045    [redacted]  [redacted]   TCP           66  ✓                        0  53396 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=679743951 TSecr=323876616
  4  [redacted]  0.000373    [redacted]  [redacted]   SMB2         310  ✓                      244  Negotiate Protocol Request
  5  [redacted]  0.000697    [redacted]  [redacted]   SMB2         378  ✓                      312  Negotiate Protocol Response
  6  [redacted]  0.000049    [redacted]  [redacted]   TCP           66  ✓                        0  53396 → 445 [ACK] Seq=245 Ack=313 Win=67072 Len=0 TSval=679743952 TSecr=323876618
  7  [redacted]  0.000052    [redacted]  [redacted]   SMB2         202  ✓                      136  Session Setup Request, NTLMSSP_NEGOTIATE
  8  [redacted]  0.000391    [redacted]  [redacted]   SMB2         350  ✓                      284  Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
  9  [redacted]  0.000238    [redacted]  [redacted]   SMB2         466  ✓                      400  Session Setup Request, NTLMSSP_AUTH, User: \administrator
 10  [redacted]  0.001390    [redacted]  [redacted]   SMB2         143  ✓                       77  Session Setup Response, Error: STATUS_LOGON_FAILURE
```

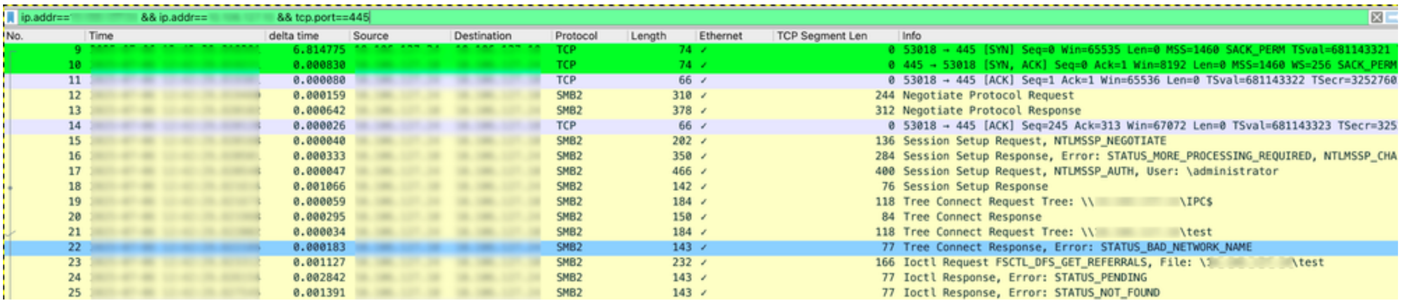
Solution: Enter correct password of login user.

Permission Issue

TCP handshake completes successfully along with **SMB** negotiation.

Login to File Share server succeeds successfully.

STATUS_BAD_NETWORK_NAME response from SMB file share server.



ip.addr==[redacted] && ip.addr==[redacted] && tcp.port==445

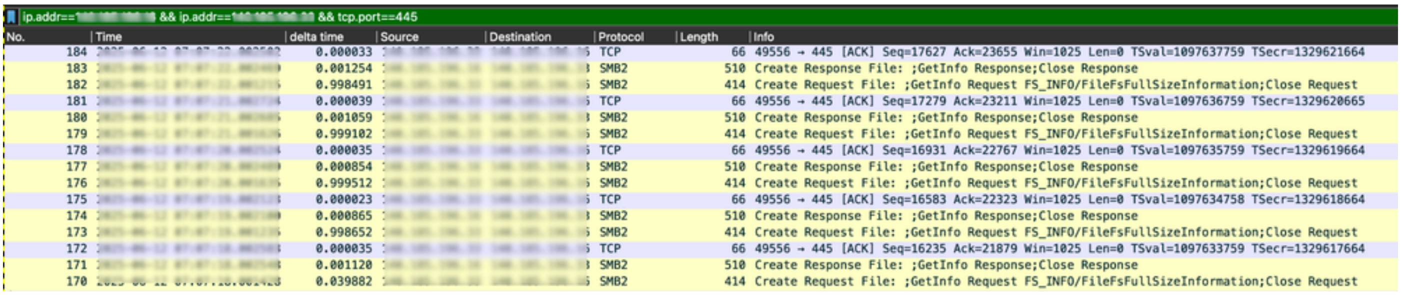
No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
9	[redacted]	6.814775	[redacted]	[redacted]	TCP	74	✓	0	53018 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=681143321
10	[redacted]	0.000830	[redacted]	[redacted]	TCP	74	✓	0	445 → 53018 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
11	[redacted]	0.000080	[redacted]	[redacted]	TCP	66	✓	0	53018 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=681143322 TSecr=3252760
12	[redacted]	0.000159	[redacted]	[redacted]	SMB2	310	✓	244	Negotiate Protocol Request
13	[redacted]	0.000642	[redacted]	[redacted]	SMB2	378	✓	312	Negotiate Protocol Response
14	[redacted]	0.000026	[redacted]	[redacted]	TCP	66	✓	0	53018 → 445 [ACK] Seq=245 Ack=313 Win=67072 Len=0 TSval=681143323 TSecr=325
15	[redacted]	0.000040	[redacted]	[redacted]	SMB2	202	✓	136	Session Setup Request, NTLMSSP_NEGOTIATE
16	[redacted]	0.000333	[redacted]	[redacted]	SMB2	350	✓	284	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHA
17	[redacted]	0.000047	[redacted]	[redacted]	SMB2	466	✓	400	Session Setup Request, NTLMSSP_AUTH, User: \administrator
18	[redacted]	0.001066	[redacted]	[redacted]	SMB2	142	✓	76	Session Setup Response
19	[redacted]	0.000059	[redacted]	[redacted]	SMB2	184	✓	118	Tree Connect Request Tree: \\[redacted]\IPC$
20	[redacted]	0.000295	[redacted]	[redacted]	SMB2	150	✓	84	Tree Connect Response
21	[redacted]	0.000034	[redacted]	[redacted]	SMB2	184	✓	118	Tree Connect Request Tree: \\[redacted]\test
22	[redacted]	0.000183	[redacted]	[redacted]	SMB2	143	✓	77	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
23	[redacted]	0.001127	[redacted]	[redacted]	SMB2	232	✓	166	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \[redacted]\test
24	[redacted]	0.002842	[redacted]	[redacted]	SMB2	143	✓	77	Ioctl Response, Error: STATUS_PENDING
25	[redacted]	0.001391	[redacted]	[redacted]	SMB2	143	✓	77	Ioctl Response, Error: STATUS_NOT_FOUND

Solution: Assign read/write permission to login user.

Ungracefully Terminated Session

Database backup operation can be interrupted if remote file directory/location storage runs out.

SMB session is a loop of **Close Request** and **Close Response**.



ip.addr==[redacted] && ip.addr==[redacted] && tcp.port==445

No.	Time	delta time	Source	Destination	Protocol	Length	Info
184	[redacted]	0.000033	[redacted]	[redacted]	TCP	66	49556 → 445 [ACK] Seq=17627 Ack=23655 Win=1025 Len=0 TSval=1097637759 TSecr=1329621664
183	[redacted]	0.001254	[redacted]	[redacted]	SMB2	510	Create Response File: ;GetInfo Response;Close Response
182	[redacted]	0.998491	[redacted]	[redacted]	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
181	[redacted]	0.000039	[redacted]	[redacted]	TCP	66	49556 → 445 [ACK] Seq=17279 Ack=23211 Win=1025 Len=0 TSval=1097636759 TSecr=1329620665
180	[redacted]	0.001059	[redacted]	[redacted]	SMB2	510	Create Response File: ;GetInfo Response;Close Response
179	[redacted]	0.999102	[redacted]	[redacted]	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
178	[redacted]	0.000035	[redacted]	[redacted]	TCP	66	49556 → 445 [ACK] Seq=16931 Ack=22767 Win=1025 Len=0 TSval=1097635759 TSecr=1329619664
177	[redacted]	0.000854	[redacted]	[redacted]	SMB2	510	Create Response File: ;GetInfo Response;Close Response
176	[redacted]	0.999512	[redacted]	[redacted]	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
175	[redacted]	0.000023	[redacted]	[redacted]	TCP	66	49556 → 445 [ACK] Seq=16583 Ack=22323 Win=1025 Len=0 TSval=1097634758 TSecr=1329618664
174	[redacted]	0.000865	[redacted]	[redacted]	SMB2	510	Create Response File: ;GetInfo Response;Close Response
173	[redacted]	0.998652	[redacted]	[redacted]	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
172	[redacted]	0.000035	[redacted]	[redacted]	TCP	66	49556 → 445 [ACK] Seq=16235 Ack=21879 Win=1025 Len=0 TSval=1097633759 TSecr=1329617664
171	[redacted]	0.001120	[redacted]	[redacted]	SMB2	510	Create Response File: ;GetInfo Response;Close Response
170	[redacted]	0.039882	[redacted]	[redacted]	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request

Ungraceful SMB Session Teardown

Solution: Restart the SNA appliance.

If Further assistance is required investigating the issue , we encourage to create TAC case athttps://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html