Secure Network Analytics Appliance의 원격 파일 시스템 컨피그레이션 문제를 해결합니다.

목차

- 소개
- 원격 파일 시스템 컨피그레이션
- 절차
  - 패킷 캡처 시작
  - 원격 파일 시스템 구성 및 테스트
  - 패킷 캡처 다운로드 및 검토
  - 일반 오류
    - TCP 포트 445 블록
    - 서비스가 실행되고 있지 않음
    - SMB 버전 1/2/3 사용 안 함
    - SMB 공유에 대한 잘못된 비밀번호
    - 권한 문제
    - 세션이 잘못 종료되었습니다.

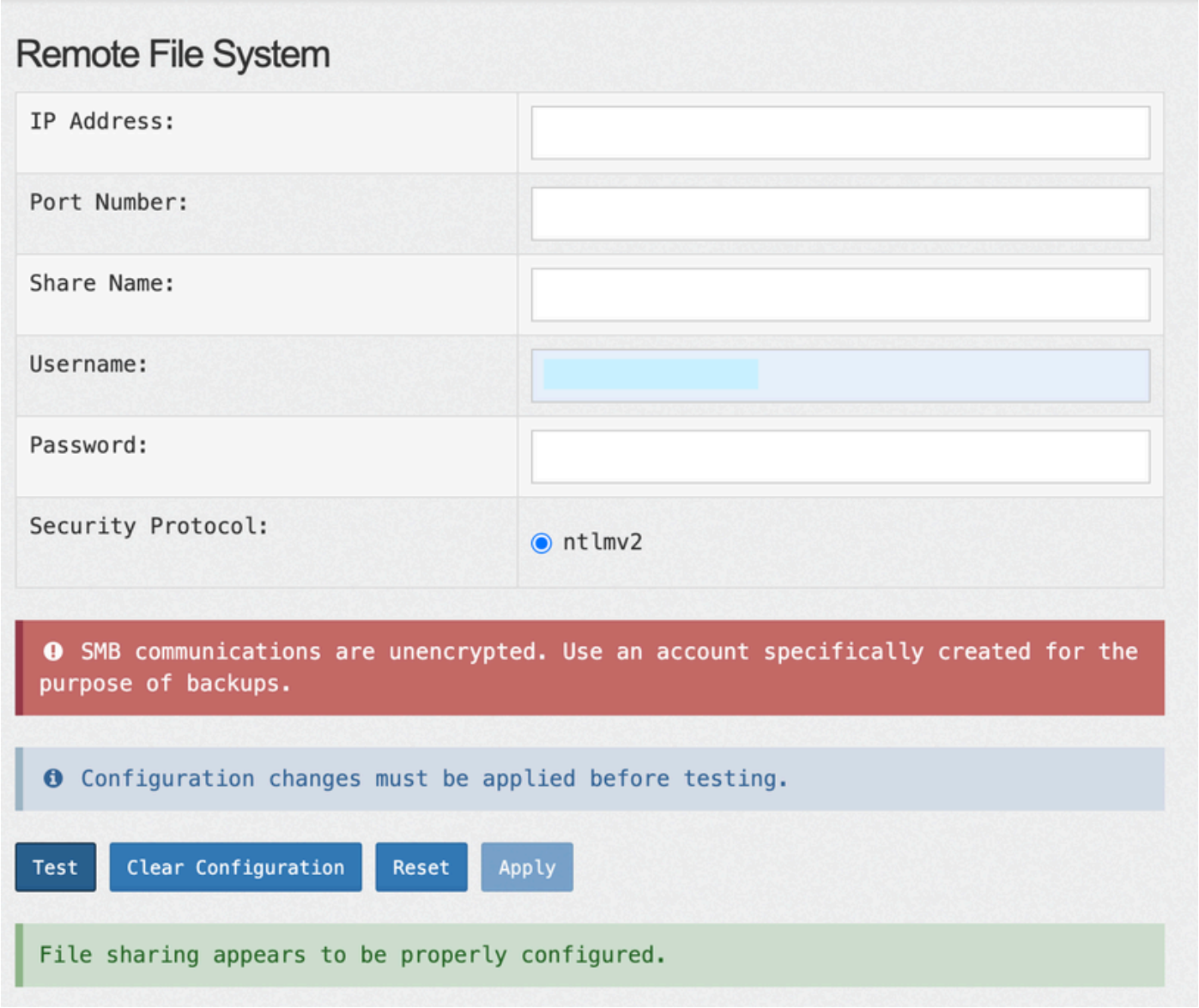
소개

이 문서에서는 SNA(Secure Network Analytics) 버전 7.5.2 이상에서 원격 파일 시스템 컨피그레이션 문제를 해결하는 방법에 대해 설명합니다.

원격 파일 시스템 컨피그레이션

DDS(분산 데이터베이스 시스템) 환경에서 데이터베이스 백업을 만들려면 원격 파일 시스템 컨피그레이션이 필수적입니다. 또한 SMB(Server Message Block)라고도 하는 CIFS(Common Internet File Share) 프로토콜을 사용합니다.

SNA 어플라이언스는 구성된 원격 파일 시스템과의 테스트 연결을 시작할 때 "파일 공유가 올바르게 구성된 것 같습니다."라는 메시지를 알리기 전에 일련의 단계를 수행합니다.



성공적인 SMB 테스트

- 클라이언트는 포트 445를 통해 TCP/IP를 사용하여 서버(원격 파일 디렉토리)에 대한 연결을 시작합니다.
- CIFS 프로토콜은 포트 139를 사용할 때 이름 확인 및 세션 설정에 NetBIOS를 활용하거나 포트 445를 사용할 때 TCP를 통해 직접 사용합니다.
- 클라이언트와 서버는 사용할 프로토콜 버전을 협상합니다. 이렇게 하면 클라이언트와 서버 간의 호환성이 보장됩니다.
- 서버는 지원되는 프로토콜 언어 목록으로 응답하며, 클라이언트는 가장 적합한 프로토콜 언어를 선택합니다.
- 클라이언트는 인증 자격 증명을 포함하는 세션 설정 요청을 보냅니다.
- 인증은 메커니즘 ntlmv2를 사용하여 수행됩니다.
- 인증에 성공하면 서버는 세션을 설정하고 클라이언트에 고유한 세션 ID를 할당합니다.
- 클라이언트는 특정 공유 리소스에 액세스하기 위해 트리 연결 요청을 보냅니다.
- 서버는 요청을 검증하고 트리 ID를 제공하며, 클라이언트는 이 ID를 사용하여 리소스의 후속 작업을 수행합니다.
- 이제 클라이언트는 공유 리소스에서 파일을 읽거나 쓰거나 수정하는 등의 작업을 수행할 수 있습니다.

- CIFS는 파일 잠금 및 동시 액세스와 같은 기능을 지원하여 데이터 무결성을 보장합니다.
- 클라이언트가 작업을 완료하면 로그 오프 요청을 전송하여 세션을 종료합니다.
- 서버는 세션 ID 및 관련 리소스를 릴리스합니다.

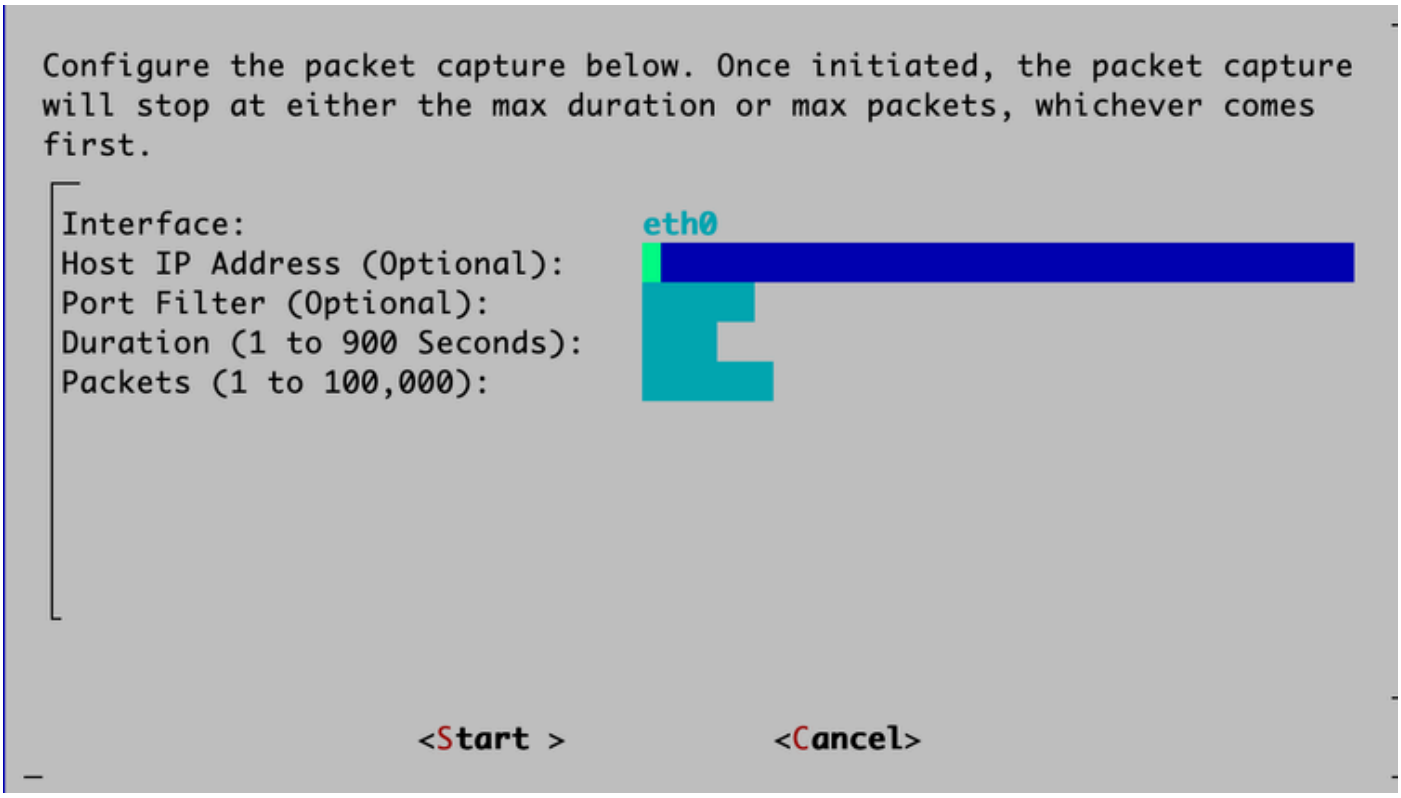
절차

SNA 장치에 대한 원격 파일 시스템을 구성하는 동안 발생하는 매우 일반적인 문제는 "마운트 실패" 오류입니다.

문제의 원인을 더 정확하게 파악하려면 다음과 같이 진행하십시오.

패킷 캡처 시작

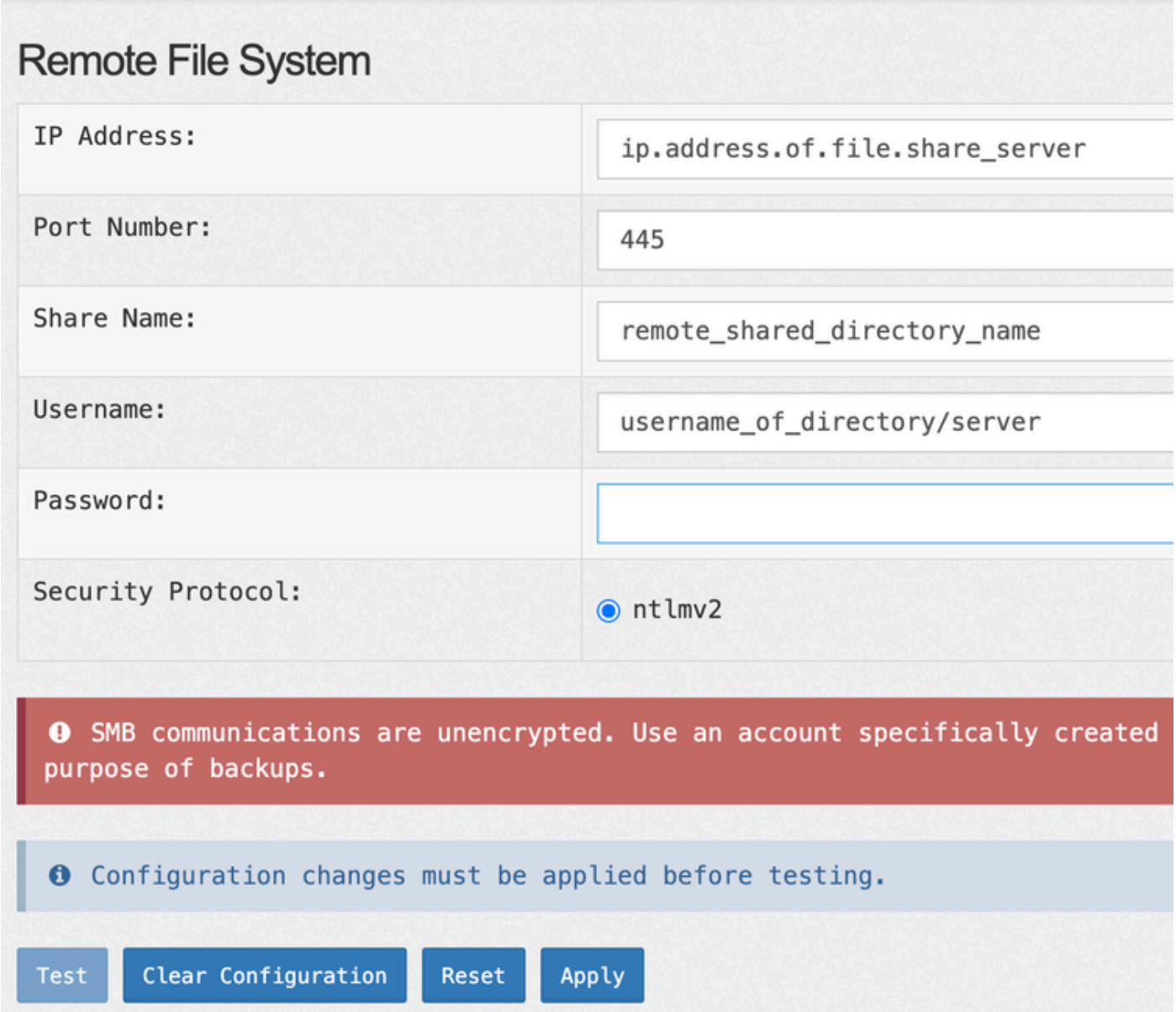
- sysadmin 자격 증명을 사용하여 SNA 어플라이언스 CLI에 로그인합니다.
- Advanced(고급) > Packet Capture(패킷 캡처)로 이동합니다.
- Host IP Address(호스트 IP 주소) 아래에 원격 공유 IP 주소, 445 as Port Filter(포트 필터로 445), Minimum 60 sec(최소 60초), 100 as duration(기간)과 packet(패킷)으로 각각 입력합니다.



CLI에서 패킷 캡처

원격 파일 시스템 구성 및 테스트

- SNA 어플라이언스 UI에 로그인하고 Configuration(컨피그레이션) > Remote File System(원격 파일 시스템)으로 이동합니다.



원격 공유 구성

- Apply(적용) 및 Test(테스트)를 클릭합니다.

패킷 캡처 다운로드 및 검토

- 패킷 캡처가 중지될 때까지 기다리거나 CTRL-C를 사용하여 수동으로 중단합니다.
- SNA Appliance UI(SNA 어플라이언스 UI) > Support(지원) > Browse Files(파일 찾아보기) > tcpdump로 이동합니다.

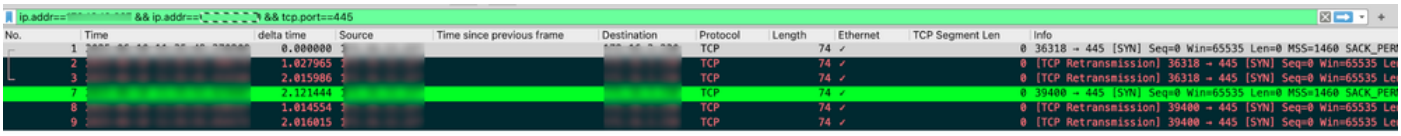
일반 오류

패킷 캡처를 열고 필터 ip.addr==ip_address_of_SNA && ip.addr==ip_address_of_remote_storage && tcp.port==445를 적용합니다.

패킷 캡처 필터

TCP 포트 445 블록

원격 파일 서버 IP 주소에 대한 TCP 재전송 시도와 함께 SNA 어플라이언스에서 시작된 다중 SYN 패킷에 대한 응답이 없습니다.



포트 블록

해결책: 방화벽에서 SNA 장치와 원격 파일 공유 디렉토리/위치 간 TCP/445 포트 통신 허용

서비스가 실행되고 있지 않음

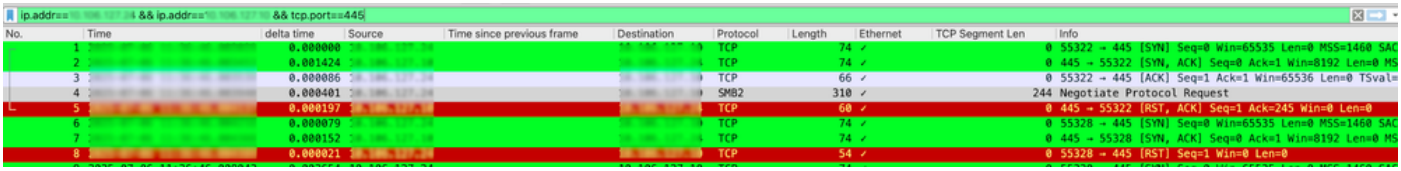
SNA 장치가 TCP 포트 445를 통해 SYN 패킷을 시작했지만 SMB 서버가 RST,ACK로 응답했습니다.

SMB 서비스가 실행되고 있지 않음

해결책: 각 서버에서 SMB 파일 공유 초기화

SMB 버전 1/2/3 사용 안 함

TCP 핸드셰이크가 성공적으로 완료되지만 SMB 버전이 비활성화되어 SMB 협상이 실패합니다.



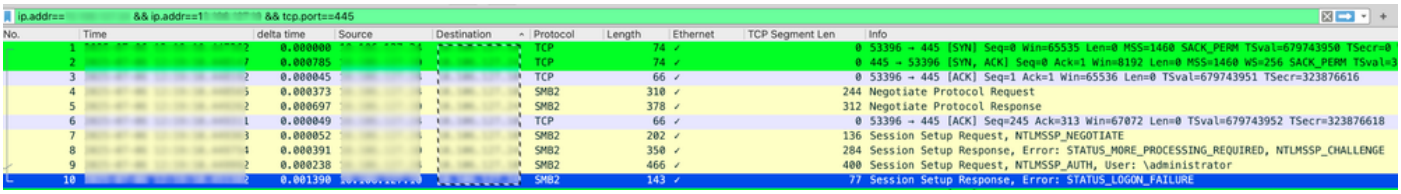
SMB 버전 사용 안 함

해결책: 각 서버에서 적절한 SMB 버전을 활성화합니다.

SMB 공유에 대한 잘못된 비밀번호

TCP 핸드셰이크가 SMB 협상과 함께 성공적으로 완료됩니다.

SMB 파일 공유 서버의 STATUS_LOGIN_FAILURE 응답



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

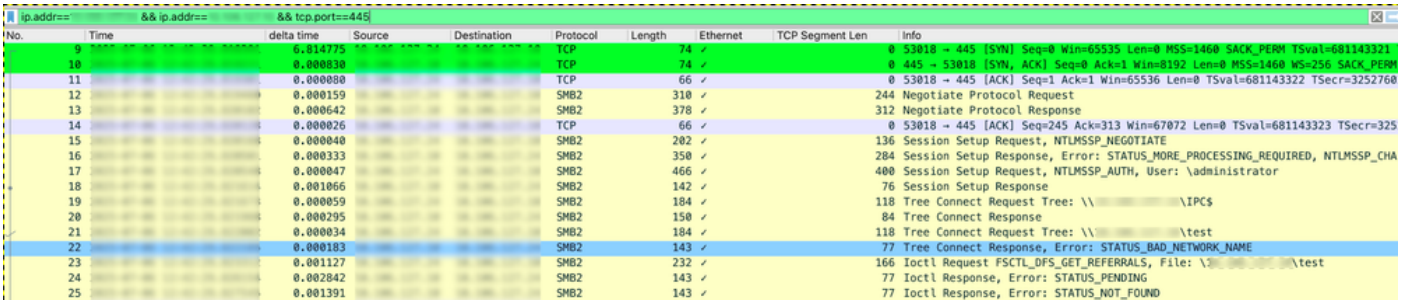
해결책: 로그인 사용자의 올바른 비밀번호를 입력합니다.

권한 문제

TCP 핸드셰이크가 SMB 협상과 함께 성공적으로 완료됩니다.

파일 공유 서버에 로그인했습니다.

SMB 파일 공유 서버의 STATUS_BAD_NETWORK_NAME 응답



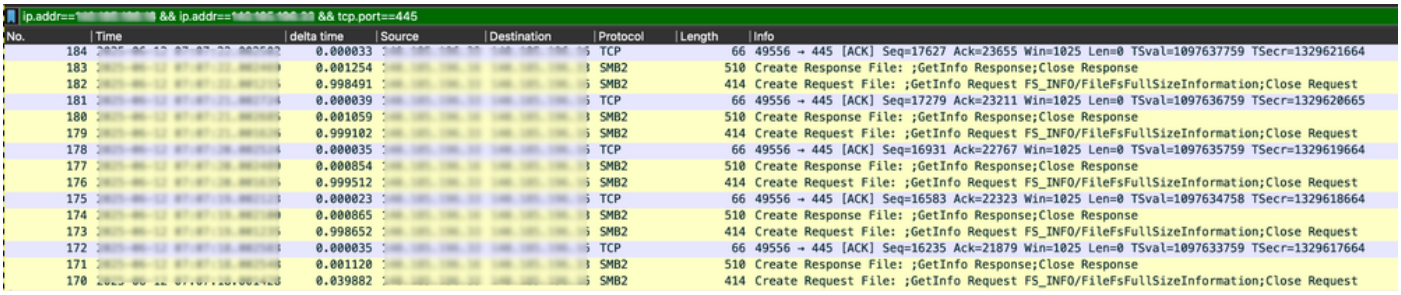
No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
9	[redacted]	6.814775	[redacted]	[redacted]	TCP	74	✓	0	53018 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=681143321
10	[redacted]	0.000830	[redacted]	[redacted]	TCP	74	✓	0	445 → 53018 [SYN, ACK] Seq=0 Ack=1 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

해결책: 로그인 사용자에게 읽기/쓰기 권한을 할당합니다.

세션이 잘못 종료되었습니다.

원격 파일 디렉토리/위치 저장소가 부족하면 데이터베이스 백업 작업이 중단될 수 있습니다.

SMB 세션은 Close Request 및 Close Response의 루프입니다.



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 세션 해체

해결책: SNA 어플라이언스를 다시 시작합니다.

문제를 조사하는 데 추가 지원이 필요한 경우, TAC 케이스를 생성하는 것이 좋습니다.
athttps://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

이 번역에 관하여
Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.