Risolvere i problemi di configurazione remota del file system per gli appliance di analisi della rete sicure.

Sommario

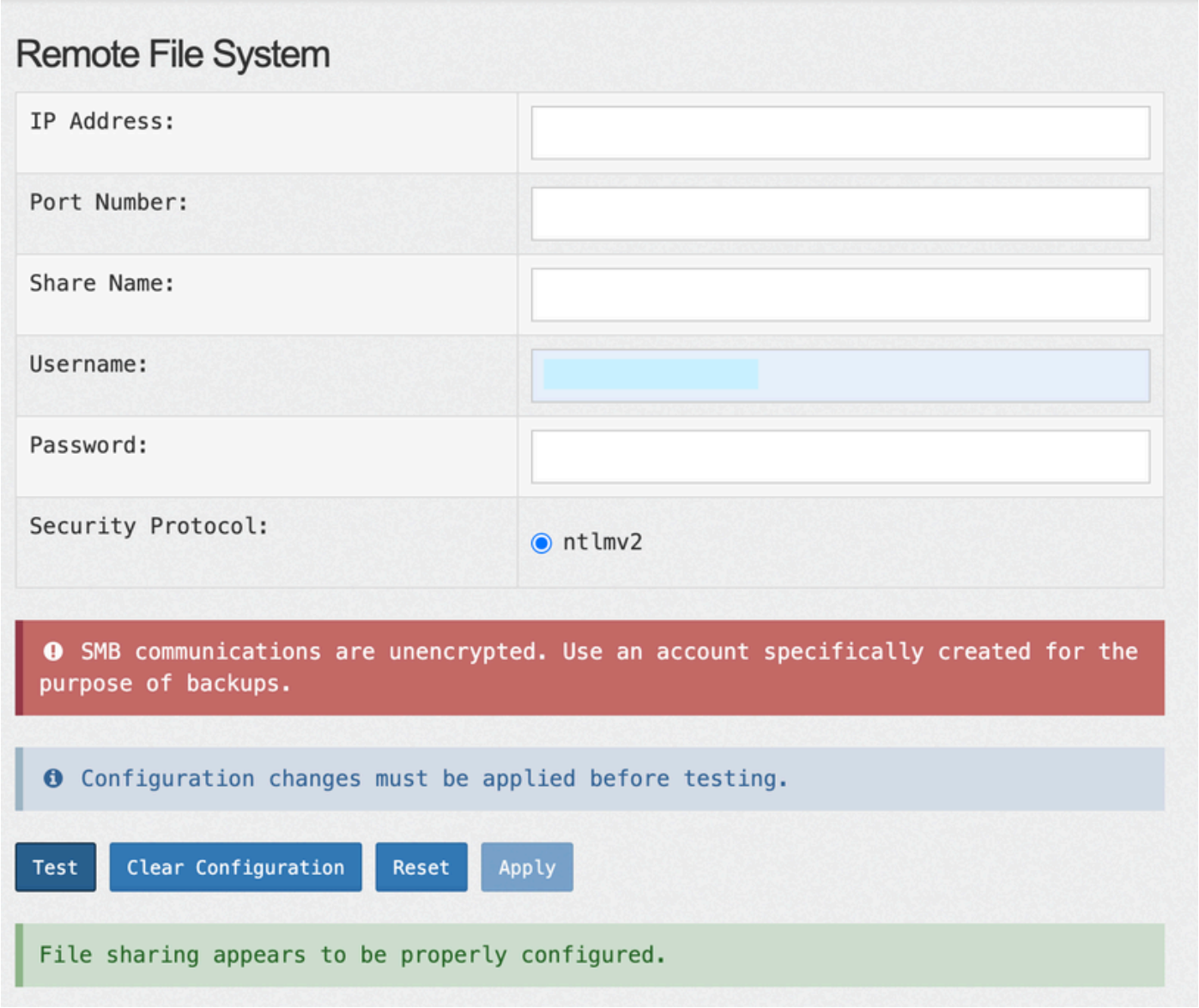
Introduzione

Questo documento descrive come risolvere i problemi di configurazione remota del file system per SNA (Secure Network Analytics) versione 7.5.2 e successive.

Configurazione remota del file system

La configurazione remota del file system è essenziale per la creazione di backup del database in ambiente DDS (Distributed Database System). Utilizza il protocollo CIFS (Common Internet File Share), noto anche come SMB (Server Message Block).

Quando l'accessorio SNA avvia la connessione di prova con il file system remoto configurato, esegue una serie di passaggi prima di annunciare il messaggio "La condivisione del file sembra essere configurata correttamente".



Test SMB riuscito

- Il client avvia una connessione al server (directory file remota) utilizzando TCP/IP sulla porta 445.
- Il protocollo CIFS utilizza NetBIOS per la risoluzione dei nomi e la definizione delle sessioni quando utilizza la porta 139 o direttamente su TCP quando utilizza la porta 445.
- Il client e il server negoziano la versione del protocollo da utilizzare. Ciò garantisce la compatibilità tra client e server.
- Il server risponde con un elenco di dialetti di protocollo supportati e il client seleziona quello più appropriato.
- Il client invia una richiesta di impostazione della sessione, che include le credenziali di autenticazione.
- L'autenticazione viene eseguita utilizzando i meccanismi ntlmv2.
- Una volta completata l'autenticazione, il server stabilisce una sessione e assegna un ID sessione univoco al client.
- Il client invia una richiesta di connessione struttura per accedere a una risorsa condivisa specifica.
- Il server convalida la richiesta e fornisce un ID di struttura che il client utilizza per le

operazioni successive sulla risorsa.
- Il client può ora eseguire operazioni quali la lettura, la scrittura o la modifica dei file nella risorsa condivisa.
- CIFS supporta funzionalità quali il blocco dei file e l'accesso simultaneo per garantire l'integrità dei dati.
- Una volta completate le operazioni, il client invia una richiesta di disconnessione per terminare la sessione.
- Il server rilascia l'ID sessione e le risorse associate.

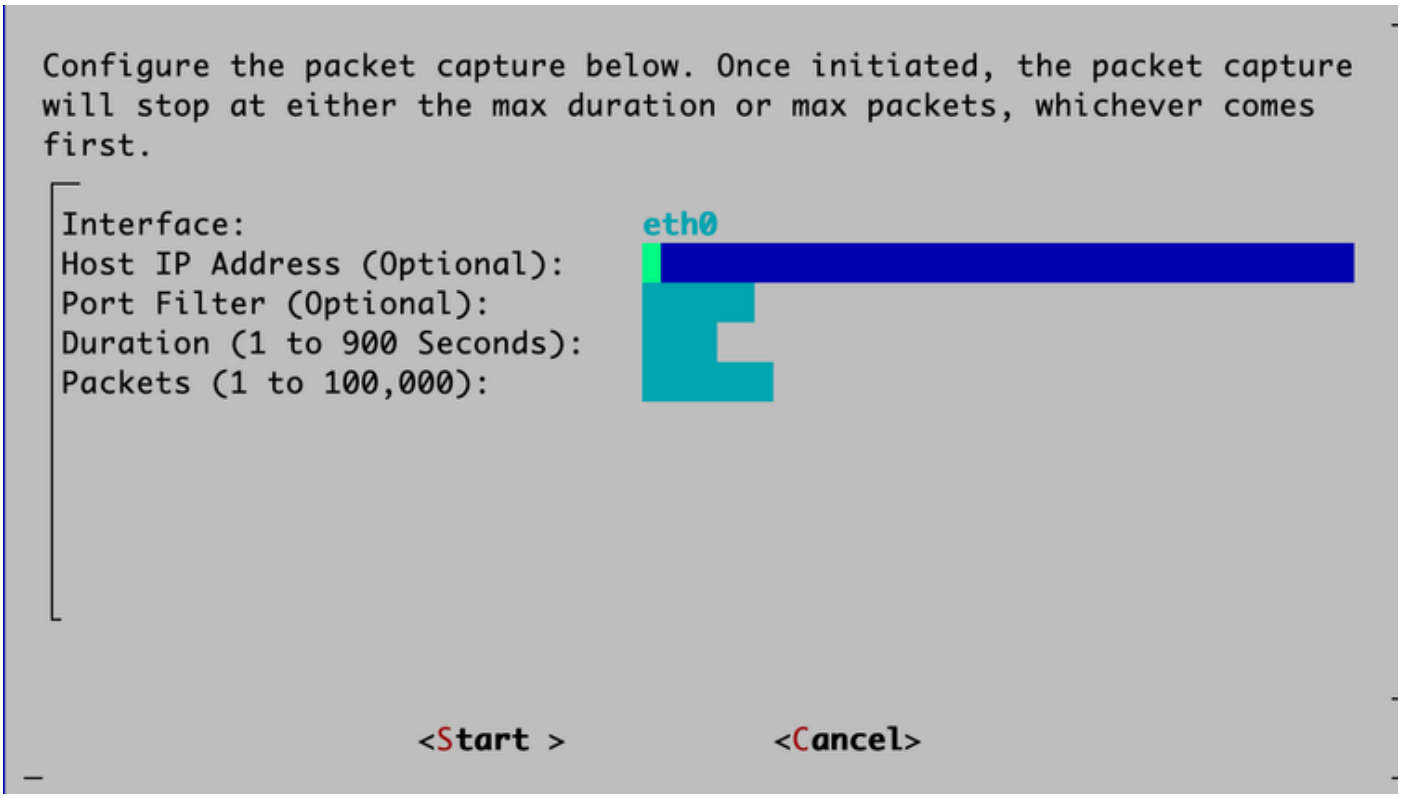
Procedura

Un problema molto comune riscontrato durante la configurazione del file system remoto per i dispositivi SNA è l'errore "Failed to mount" (Impossibile montare).

Per comprendere meglio la causa del problema, procedere come segue:

Avvia acquisizione pacchetto

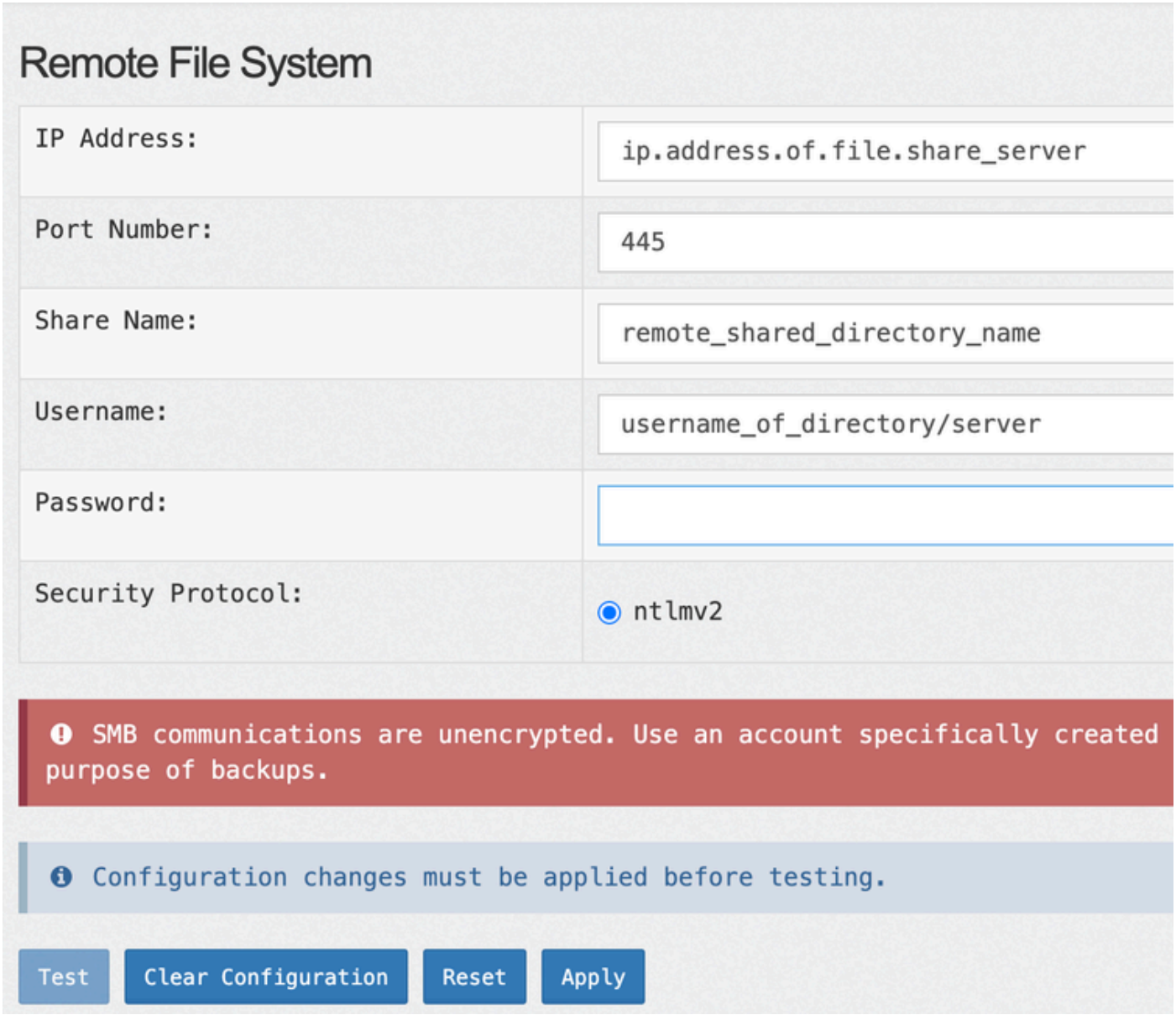
- Accedere alla CLI dell'appliance SNA utilizzando le credenziali sysadmin.
- Selezionare Avanzate > Acquisizione pacchetti
- Immettere l'indirizzo IP della condivisione remota in Indirizzo IP host, 445 come Filtro porta, Minimo 60 sec, 100 come durata e pacchetto, rispettivamente



Acquisizione pacchetti dalla CLI

Configurazione e test del file system remoto

- Accedere all'interfaccia utente dell'accessorio SNA e selezionare Configurazione > File system remoto



Configurazioni di condivisione remota

- Fare clic su Apply and Test.

Download e controllo dell'acquisizione dei pacchetti

- Attendere l'interruzione dell'acquisizione dei pacchetti o interrompere manualmente l'operazione utilizzando CTRL-C.
- Selezionare Interfaccia utente accessorio SNA > Supporto > Sfoglia file > tcpdump.

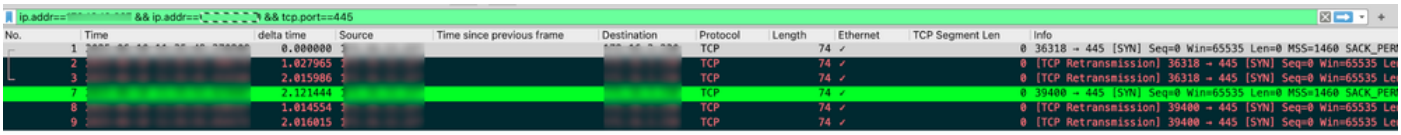
Errore comune

Aprire l'acquisizione pacchetti e applicare il filtro ip.addr==ip_address_of_SNA && ip.addr==ip_address_of_remote_storage && tcp.port==445.

Filtro acquisizione pacchetti

Blocco porta TCP 445

Nessuna risposta per più pacchetti SYN inizializzati dall'appliance SNA insieme ai tentativi di ritrasmissione TCP verso l'indirizzo IP remoto del file server.



Blocco porta

Soluzione: Consente la comunicazione della porta TCP/445 tra l'accessorio SNA e la directory/posizione di condivisione file remota dal firewall.

Servizio non in esecuzione

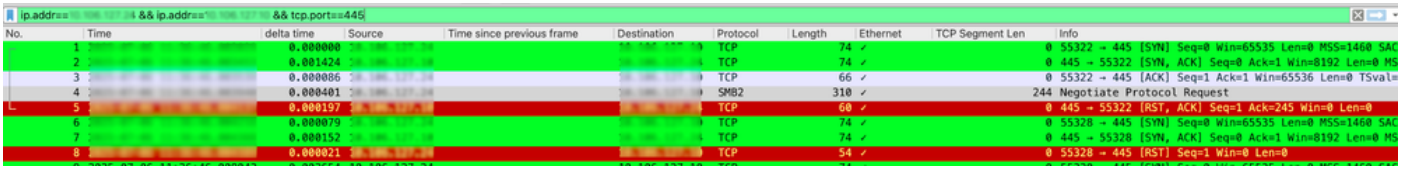
Il dispositivo SNA ha avviato il pacchetto SYN sulla porta TCP 445. Tuttavia, il server SMB risponde con RST,ACK.

Servizio SMB non in esecuzione

Soluzione: Inizializza condivisione file SMB nel server corrispondente

SMB versione 1/2/3 disabilitato

L'handshake TCP viene completato correttamente, ma la negoziazione SMB non riesce a causa della versione SMB disabilitata.



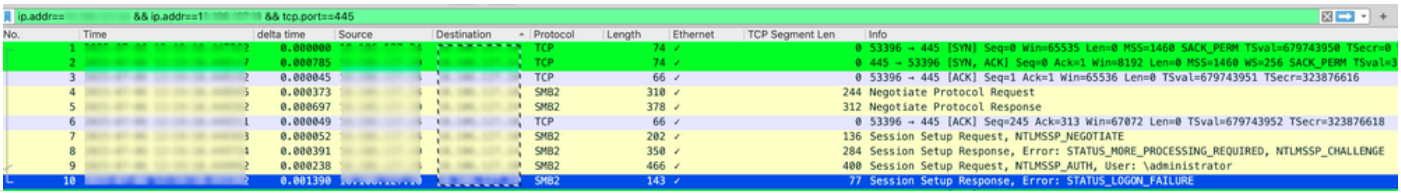
Versioni SMB disabilitate

Soluzione: Abilitare la versione SMB appropriata sul server corrispondente.

Password errata per la condivisione SMB

Handshake TCP completato correttamente insieme alla negoziazione SMB.

Risposta STATUS_LOGIN_FAILURE dal server di condivisione file SMB.



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

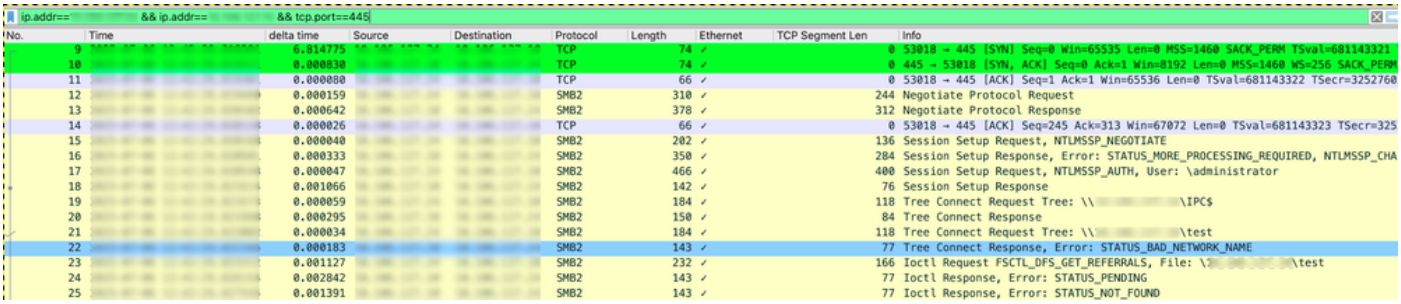
Soluzione: Immettere la password corretta dell'utente di accesso.

Problema di autorizzazione

Handshake TCP completato correttamente insieme alla negoziazione SMB.

Accesso al server di condivisione file completato.

RISPOSTA STATUS_BAD_NETWORK_NAME dal server di condivisione file SMB.



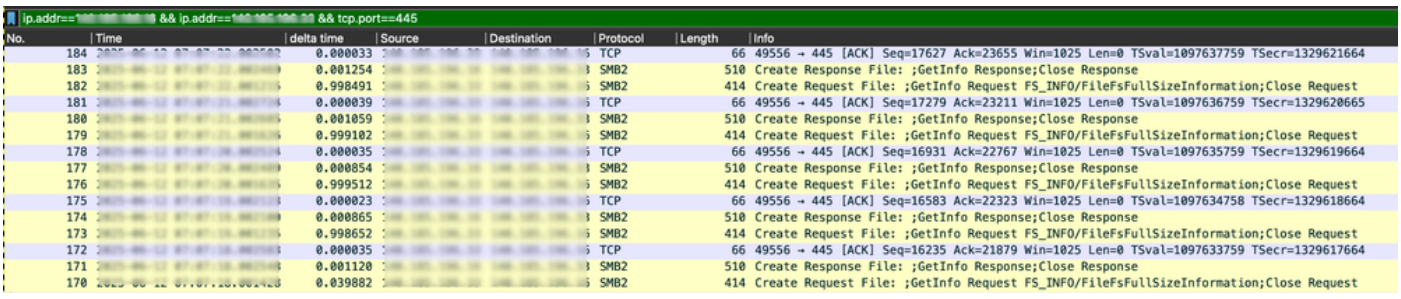
No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
9		6.814775			TCP	74	✓	0	53018 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=681143321
10		0.000830			TCP	74	✓	0	445 → 53018 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
11		0.000080	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

Soluzione: Assegnare l'autorizzazione di lettura/scrittura all'utente di accesso.

Sessione terminata in modo anomalo

L'operazione di backup del database può essere interrotta se si esaurisce lo storage remoto di directory/percorsi di file.

La sessione SMB è un ciclo di Close Request e Close Response.



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

Annullamento inappropriato della sessione SMB

Soluzione: Riavviare l'accessorio SNA.

Se è necessaria ulteriore assistenza nell'investigazione del problema, si consiglia di creare un

caso TAC athttps://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).