

Problemen met de configuratie van externe bestandssystemen oplossen voor Secure Network Analytics-apparaten.

Inhoud

[Inleiding](#)

[Configuratie extern bestandssysteem](#)

[Procedure](#)

[Pakketvastlegging starten](#)

[Bestandssysteem op afstand configureren en testen](#)

[Pakketvastlegging downloaden en beoordelen](#)

[Veelvoorkomende fout](#)

[TCP-poort 445-blok](#)

[Service wordt niet uitgevoerd](#)

[SMB versie 1/2/3 uitgeschakeld](#)

[Verkeerd wachtwoord voor SMB Share](#)

[machtigingskwestie](#)

[onelegant beëindigde sessie](#)

Inleiding

In dit document wordt beschreven hoe problemen met de configuratie van externe bestandssystemen voor SNA (Secure Network Analytics) versie 7.5.2 en volgende kunnen worden opgelost.

Configuratie extern bestandssysteem

Configuratie van bestandssysteem op afstand is essentieel voor het maken van databaseback-ups in een DDS-omgeving (Distributed Database System). Het maakt gebruik van het CIFS-protocol (Common Internet File Share), ook bekend als SMB (Server Message Block).

Wanneer het SNA-toestel een testverbinding start met een geconfigureerd extern bestandssysteem, voert het een reeks stappen uit voordat het bericht "Bestanden delen lijkt correct te zijn geconfigureerd" wordt aangekondigd.

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.

Test

Clear Configuration

Reset

Apply

File sharing appears to be properly configured.

Succesvolle SMB-test

- De client initieert een verbinding met de server (externe bestandsdirectory) via TCP/IP via poort 445.
- Het CIFS-protocol maakt gebruik van NetBIOS voor het oplossen van namen en het instellen van sessies wanneer poort 139 wordt gebruikt of rechtstreeks via TCP wanneer poort 445 wordt gebruikt.
- De client en server onderhandelen over de te gebruiken protocolversie. Dit zorgt voor compatibiliteit tussen de client en de server.
- De server reageert met een lijst met ondersteunde protocoldialecten en de client selecteert de meest geschikte dialecten.
- De client verzendt een sessie-installatieverzoek, dat verificatiereferenties bevat.
- Authenticatie wordt uitgevoerd met behulp van mechanismen ntlmv2.
- Na succesvolle verificatie stelt de server een sessie op en wijst een unieke sessie-ID toe aan de client.
- De client verzendt een boomverbindingsverzoek om toegang te krijgen tot een specifieke gedeelde bron.
- De server valideert het verzoek en biedt een structuur-ID die de client gebruikt voor

volgende bewerkingen op de resource.

- De client kan nu bewerkingen uitvoeren zoals lezen, schrijven of wijzigen van bestanden op de gedeelde bron.
- CIFS ondersteunt functies zoals bestandsvergrendeling en gelijktijdige toegang om de gegevensintegriteit te waarborgen.
- Zodra de client zijn bewerkingen heeft voltooid, verzendt deze een afmeldingsverzoek om de sessie te beëindigen.
- De server geeft de sessie-ID en bijbehorende bronnen vrij.

Procedure

Een veel voorkomend probleem bij het configureren van een extern bestandssysteem voor SNA-apparaten is de fout "Failed to mount".

Om beter te begrijpen wat de oorzaak van het probleem is, gaat u als volgt te werk:

Pakketvastlegging starten

- Meld u aan bij de CLI van het SNA-toestel met sysadmin-referenties.
- Navigeer naar Geavanceerd > Pakketvastlegging
- Voer het IP-adres voor delen op afstand in onder Host IP Address, 445 als Port Filter, Minimum 60 sec, 100 als duur en pakket respectievelijk

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):	

<Start > <Cancel>

Pakketvastlegging vanuit CLI

Bestandssysteem op afstand configureren en testen

- Meld u aan bij de gebruikersinterface van het SNA-toestel en navigeer naar Configuratie > Extern bestandssysteem

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.

Configuraties voor externe delen

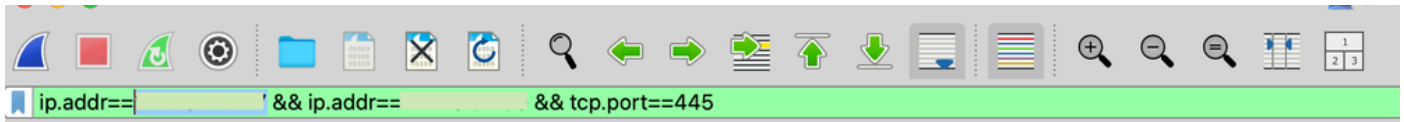
- Klik op Toepassen en testen.

Pakketvastlegging downloaden en beoordelen

- Wacht tot pakketopname stopt of handmatig wordt onderbroken met CTRL-C.
- Navigeer naar SNA toestel UI > Ondersteuning > Bladeren door bestanden > tcpdump.

Veelvoorkomende fout

Open de pakketopname en pas het filter `ip.addr==ip_address_of_SNA && ip.addr==ip_address_of_remote_storage && tcp.port==445` toe.



pakketopnamefilter

TCP-poort 445-blok

Geen respons voor meerdere SYN-pakketten die door het SNA-apparaat zijn geïnitieerd, samen met TCP-hertransmissie pogingen naar het IP-adres van de externe bestandsserver.

No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000					TCP	74	✓		0 36318 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
2	1.027965					TCP	74	✓		0 [TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Le
3	2.015986					TCP	74	✓		0 [TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Le
7	2.121444					TCP	74	✓		0 39400 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
8	1.014554					TCP	74	✓		0 [TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Le
9	2.016815					TCP	74	✓		0 [TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Le

havenblok

Oplossing: Sta TCP/445-poortcommunicatie toe tussen SNA-toestel en Remote File Share-directory/locatie vanuit firewall.

Service wordt niet uitgevoerd

SNA-apparaat startte SYN-pakket via TCP-poort 445, maar SMB-server reageert met RST, ACK.

No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000					TCP	74	✓		0 49262 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
2	0.000468					TCP	60	✓		0 445 → 49262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.007958					TCP	74	✓		0 57866 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
12	0.008382					TCP	60	✓		0 445 → 57866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

SMB-service wordt niet uitgevoerd

Oplossing: SMB File Share initialiseren op de betreffende server

SMB versie 1/2/3 uitgeschakeld

TCP-handshake is voltooid, maar SMB-onderhandeling mislukt omdat de SMB-versie is uitgeschakeld.

No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000					TCP	74	✓		0 55322 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
2	0.001424					TCP	74	✓		0 445 → 55322 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
3	0.000086					TCP	66	✓		0 55322 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=
4	0.000401					SMB2	310	✓		244 Negotiate Protocol Request
5	0.000197					TCP	60	✓		0 445 → 55322 [RST, ACK] Seq=1 Ack=245 Win=0 Len=0
6	0.000070					TCP	74	✓		0 55328 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
7	0.000152					TCP	74	✓		0 445 → 55328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
8	0.000921					TCP	54	✓		0 55328 → 445 [RST] Seq=1 Win=0 Len=0

SMB-versies uitgeschakeld

Oplossing: schakel de juiste SMB-versie in op de betreffende server.

Verkeerd wachtwoord voor SMB Share

TCP-handshake wordt succesvol afgerond, samen met SMB-onderhandelingen.

STATUS_LOGIN_FAILURE-reactie van SMB File Share Server.

No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	74	✓	0	53396 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=679743950 TSecr=0
2	0.000785		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	74	✓	0	445 → 53396 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=0 TSecr=679743950
3	0.000845		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	✓	0	53396 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=679743951 TSecr=323876616
4	0.000373		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	310	✓		244 Negotiate Protocol Request
5	0.000697		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	378	✓		312 Negotiate Protocol Response
6	0.000849		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	✓	0	53396 → 445 [ACK] Seq=245 Ack=313 Win=67072 Len=0 TSval=679743952 TSecr=323876618
7	0.000852		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	202	✓		136 Session Setup Request, NTLMSSP_NEGOTIATE
8	0.000391		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	350	✓		284 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
9	0.000238		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	466	✓		400 Session Setup Request, NTLMSSP_AUTH, User: \administrator
10	0.001390		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	143	✓		77 Session Setup Response, Error: STATUS_LOGIN_FAILURE

Oplossing: Voer het juiste wachtwoord van de aanmeldingsgebruiker in.

machtingiskwestie

TCP-handshake wordt succesvol afgerond, samen met SMB-onderhandelingen.

Aanmelden bij de bestandsdelende server is gelukt.

STATUS_BAD_NETWORK_NAME reactie van SMB file share server.

No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
9	0.014775		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	74	✓	0	53018 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=681143321 TSecr=0
10	0.000830		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	74	✓	0	445 → 53018 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=0 TSecr=681143321
11	0.000800		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	✓	0	53018 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=681143322 TSecr=3252760
12	0.000159		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	310	✓		244 Negotiate Protocol Request
13	0.000642		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	378	✓		312 Negotiate Protocol Response
14	0.000026		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	✓	0	53018 → 445 [ACK] Seq=245 Ack=313 Win=67072 Len=0 TSval=681143323 TSecr=325
15	0.000040		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	202	✓		136 Session Setup Request, NTLMSSP_NEGOTIATE
16	0.000333		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	350	✓		284 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHA
17	0.000047		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	466	✓		400 Session Setup Request, NTLMSSP_AUTH, User: \administrator
18	0.001066		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	142	✓		76 Session Setup Response
19	0.000059		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	184	✓		118 Tree Connect Request Tree: \\.\IPC\$
20	0.000295		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	150	✓		84 Tree Connect Response
21	0.000034		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	184	✓		118 Tree Connect Request Tree: \\.\test
22	0.000183		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	143	✓		77 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
23	0.001127		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	232	✓		166 Ioctl Request FSCTL_DFSC_GET_REFERRALS, File: \\.\test
24	0.002042		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	143	✓		77 Ioctl Response, Error: STATUS_PENDING
25	0.001391		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	143	✓		77 Ioctl Response, Error: STATUS_NOT_FOUND

Oplossing: lees-/schrijfrechten toewijzen aan aanmeldingsgebruiker.

onelegant beëindigde sessie

De back-upbewerking van de database kan worden onderbroken als de externe bestandsdirectory/opslaglocatie leeg raakt.

SMB-sessie is een lus van Close Request en Close Response.

No.	Time	delta time	Source	Destination	Protocol	Length	Info
184	0.000033		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	49556 → 445 [ACK] Seq=17627 Ack=23655 Win=1025 Len=0 TSval=1097637759 TSecr=1329621664
183	0.001254		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
182	0.998491		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
181	0.000039		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	49556 → 445 [ACK] Seq=17279 Ack=23211 Win=1025 Len=0 TSval=1097636759 TSecr=1329620665
180	0.001059		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
179	0.999102		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
178	0.000035		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	49556 → 445 [ACK] Seq=16931 Ack=22767 Win=1025 Len=0 TSval=1097635759 TSecr=1329619664
177	0.000854		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
176	0.999512		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
175	0.000023		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	49556 → 445 [ACK] Seq=16583 Ack=22323 Win=1025 Len=0 TSval=1097634758 TSecr=1329618664
174	0.000865		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
173	0.998652		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
172	0.000035		10.0.0.0.0.0.0	10.0.0.0.0.0.0	TCP	66	49556 → 445 [ACK] Seq=16235 Ack=21879 Win=1025 Len=0 TSval=1097633759 TSecr=1329617664
171	0.001120		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
170	0.039882		10.0.0.0.0.0.0	10.0.0.0.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request

Ongracieuze afbraak van SMB-sessie

Oplossing: Start het SNA-apparaat opnieuw op.

Als verdere hulp nodig is om de kwestie te onderzoeken, moedigen we aan om een TAC-geval te

creëren [athttps://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html](https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.