

對Secure Network Analytics裝置的遠端檔案系統配置問題進行故障排除。

目錄

[簡介](#)

[遠端檔案系統配置](#)

[程式](#)

[啟動資料包捕獲](#)

[配置和測試遠端檔案系統](#)

[下載並檢視資料包捕獲](#)

[常見錯誤](#)

[TCP埠445塊](#)

[服務未運行](#)

[SMB版本1/2/3已禁用](#)

[SMB共用的密碼錯誤](#)

[許可權問題](#)

[不正常終止的會話](#)

簡介

本檔案介紹如何疑難排解SNA（安全網路分析）版本7.5.2及以上的遠端檔案系統組態問題。

遠端檔案系統配置

在DDS（分散式資料庫系統）環境中建立資料庫備份時，遠端檔案系統配置必不可少。它使用CIFS（通用網際網路檔案共用）協定，也稱為SMB（伺服器消息塊）。

當SNA裝置啟動與已配置的遠端檔案系統的測試連線時，它會執行一系列步驟，然後發出「檔案共用似乎已正確配置」消息。

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.

ℹ Configuration changes must be applied before testing.

Test

Clear Configuration

Reset

Apply

File sharing appears to be properly configured.

成功的SMB測試

- 客戶端通過埠445使用TCP/IP發起到伺服器（遠端檔案目錄）的連線。
- 當使用埠139時，CIFS協定利用NetBIOS進行名稱解析和會話建立；當使用埠445時，CIFS協定直接通過TCP進行解析。
- 客戶端和伺服器協商要使用的協定版本。這可確保客戶端和伺服器之間的相容性。
- 伺服器通過支援的協定方言清單進行響應，客戶端選擇最合適的方言。
- 客戶端傳送包含身份驗證憑證的會話設定請求。
- 身份驗證使用ntlmv2機制執行。
- 在身份驗證成功後，伺服器會建立會話並向客戶端分配唯一的會話ID。
- 客戶端傳送樹連線請求以訪問特定共用資源。
- 伺服器驗證該請求並提供樹ID，客戶端使用該樹ID對資源進行後續操作。
- 客戶端現在可以執行諸如讀取、寫入或修改共用資源上的檔案的操作。
- CIFS支援檔案鎖定和併發訪問等功能，以確保資料完整性。
- 客戶端完成操作後，會傳送註銷請求以終止會話。
- 伺服器釋放會話ID和相關資源。

程式

為SNA裝置配置遠端檔案系統時遇到的非常常見的問題是「Failed to mount」錯誤。

为了更好地瞭解導致問題的原因，請按照以下步驟操作：

啟動資料包捕獲

- 使用sysadmin憑據登入SNA設備CLI。
- 導覽至Advanced > Packet Capture
- 在Host IP Address(主機IP地址)下輸入遠端共用IP地址，445作為埠過濾器，至少60秒，100作為持續時間，100作為資料包輸入

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>

從CLI捕獲資料包

配置和測試遠端檔案系統

- 登入到SNA裝置UI並導航到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.

ℹ Configuration changes must be applied before testing.

Test

Clear Configuration

Reset

Apply

遠端共用配置

- 按一下「Apply」和「Test」。

下載並檢視資料包捕獲

- 等待資料包捕獲停止或使用CTRL-C手動中斷。
- 導航到SNA裝置UI >支援>瀏覽檔案> tcpdump。

常見錯誤

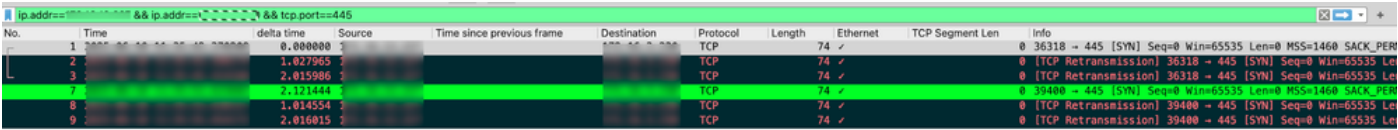
開啟資料包捕獲並應用過濾器ip.addr==ip_address_of_SNA &&
ip.addr==ip_address_of_remote_storage && tcp.port==445。



封包擷取過濾器

TCP埠445塊

SNA裝置發起的多個SYN數據包沒有響應，並且TCP重傳嘗試指向遠端檔案伺服器IP地址。



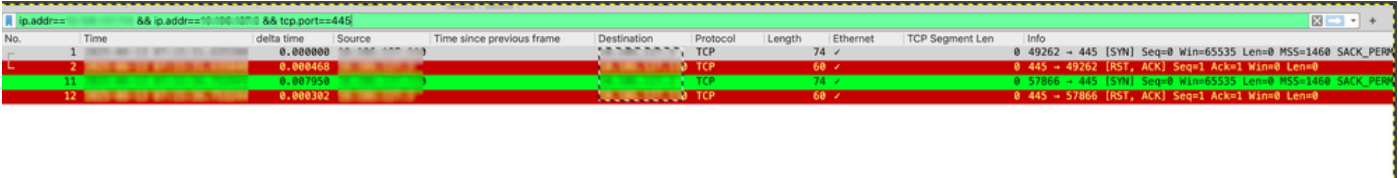
No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000		10.0.0.1		10.0.0.2	TCP	74	✓		0 36318 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
2	1.027965		10.0.0.1		10.0.0.2	TCP	74	✓		0 [TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Le
3	2.015986		10.0.0.1		10.0.0.2	TCP	74	✓		0 [TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Le
7	2.121444		10.0.0.1		10.0.0.2	TCP	74	✓		0 39400 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
8	1.014554		10.0.0.1		10.0.0.2	TCP	74	✓		0 [TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Le
9	2.016015		10.0.0.1		10.0.0.2	TCP	74	✓		0 [TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Le

埠塊

解決方案：允許SNA裝置與來自防火牆的遠端文件共用目錄/位置之間進行TCP/445端口通訊。

服務未運行

SNA裝置透過TCP連接埠445啟動SYN封包，但SMB伺服器會使用RST，ACK回應。



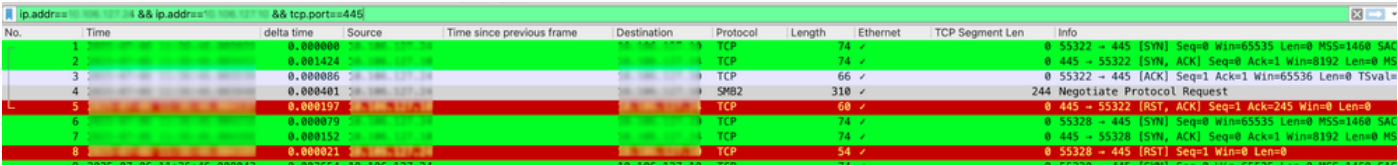
No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000		10.0.0.1		10.0.0.2	TCP	74	✓		0 49262 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
2	0.000458		10.0.0.2		10.0.0.1	TCP	60	✓		0 445 → 49262 [RST, ACK] Seq=1 Ack=3 Win=0 Len=0
11	0.007755		10.0.0.1		10.0.0.2	TCP	74	✓		0 37265 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
12	0.008302		10.0.0.2		10.0.0.1	TCP	60	✓		0 445 → 37265 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

SMB服務未運行

解決方案：在相應的伺服器上初始化SMB檔案共用

SMB版本1/2/3已禁用

TCP握手成功完成，但由於禁用了SMB版本,SMB協商失敗。



No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000		10.0.0.1		10.0.0.2	TCP	74	✓		0 55322 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SAC
2	0.001424		10.0.0.2		10.0.0.1	TCP	74	✓		0 445 → 55322 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
3	0.000086		10.0.0.1		10.0.0.2	TCP	66	✓		0 55322 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=
4	0.000401		10.0.0.2		10.0.0.1	SMB2	310	✓		244 Negotiate Protocol Request
5	0.000197		10.0.0.1		10.0.0.2	TCP	60	✓		0 445 → 55322 [RST, ACK] Seq=1 Ack=245 Win=0 Len=0
6	0.000078		10.0.0.2		10.0.0.1	TCP	74	✓		0 55328 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SAC
7	0.000152		10.0.0.1		10.0.0.2	TCP	74	✓		0 445 → 55328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
8	0.000021		10.0.0.2		10.0.0.1	TCP	54	✓		0 55328 → 445 [RST] Seq=1 Win=0 Len=0

SMB版本已禁用

解決方案：在相應的伺服器上啟用適當的SMB版本。

SMB共用的密碼錯誤

TCP握手成功與SMB協商一起完成。

來自SMB檔案共用服務器的STATUS_LOGIN_FAILURE響應。

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=0
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		0.000230			SMB2	466	✓		400 Session Setup Request, NTLMSSP_AUTH, User: \administrator
10		0.001390			SMB2	143	✓		77 Session Setup Response, Error: STATUS_LOGON_FAILURE

解決方案：輸入登入使用者的正確密碼。

許可權問題

TCP握手成功與SMB協商一起完成。

已成功登入到檔案共用伺服器。

SMB檔案共用伺服器的STATUS_BAD_NETWORK_NAME響應。

No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
9		0.014775			TCP	74	✓		0 53018 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=681143321
10		0.000030			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_DFSC_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

解決方案：為登入使用者分配讀/寫許可權。

不正常終止的會話

如果遠端檔案目錄/位置儲存用完，資料庫備份操作可能會中斷。

SMB會話是Close Request和Close Response的循環。

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/FilesFsFullSizeInformation;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/FilesFsFullSizeInformation;Close Request
178		0.000035			TCP	66	49556 → 445 [ACK] Seq=16931 Ack=22767 Win=1025 Len=0 TSval=1097635759 TSecr=1329619664
177		0.000054			SMB2	510	Create Response File: ;GetInfo Response;Close Response
176		0.999512			SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FilesFsFullSizeInformation;Close Request
175		0.000023			TCP	66	49556 → 445 [ACK] Seq=16583 Ack=22323 Win=1025 Len=0 TSval=1097634758 TSecr=1329618664
174		0.000065			SMB2	510	Create Response File: ;GetInfo Response;Close Response
173		0.998652			SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FilesFsFullSizeInformation;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/FilesFsFullSizeInformation;Close Request

不正常的SMB會話拆除

解決方案：重新啟動SNA裝置。

如果調查問題需要進一步協助，我們鼓勵建立TAC案例

[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)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。