

Solucionar problemas de configuração do sistema de arquivos remoto para dispositivos de análise de rede segura.

Contents

[Introdução](#)

[Configuração do Sistema de Arquivos Remoto](#)

[Procedimento](#)

[Iniciar captura de pacote](#)

[Configurar e testar o sistema de arquivos remoto](#)

[Fazer download e revisar a captura de pacotes](#)

[Erro comum](#)

[Bloco de Porta TCP 445](#)

[O serviço não está em execução](#)

[SMB Versão 1/2/3 Desabilitada](#)

[Senha incorreta para compartilhamento SMB](#)

[Problema de Permissão](#)

[Sessão terminada sem graça](#)

Introdução

Este documento descreve como solucionar problemas de configuração do sistema de arquivos remoto para o SNA (Secure Network Analytics) versão 7.5.2 em diante.

Configuração do Sistema de Arquivos Remoto

A configuração do sistema de arquivos remoto é essencial para a criação do backup do banco de dados no ambiente DDS (Distributed Database System). Ele usa o protocolo CIFS (Common Internet File Share, compartilhamento comum de arquivos da Internet), também conhecido como SMB (Server Message Block, bloco de mensagens do servidor).

Quando o dispositivo SNA inicia a conexão de teste com o sistema de arquivos remoto configurado, ele executa uma série de etapas antes de anunciar a mensagem "O compartilhamento de arquivos parece estar configurado corretamente".

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.

Teste de SMB Bem-sucedido

- O cliente inicia uma conexão com o servidor (diretório de arquivos remotos) usando TCP/IP pela porta 445.
- O protocolo CIFS utiliza NetBIOS para resolução de nomes e estabelecimento de sessão ao usar a porta 139 ou diretamente sobre TCP ao usar a porta 445.
- O cliente e o servidor negociam a versão do protocolo a ser usada. Isso garante a compatibilidade entre o cliente e o servidor.
- O servidor responde com uma lista de dialetos de protocolo suportados e o cliente seleciona o mais apropriado.
- O cliente envia uma solicitação de configuração de sessão, que inclui credenciais de autenticação.
- A autenticação é realizada usando os mecanismos ntlmv2.
- Após a autenticação bem-sucedida, o servidor estabelece uma sessão e atribui um ID de sessão exclusivo ao cliente.
- O cliente envia uma solicitação de conexão em árvore para acessar um recurso compartilhado específico.
- O servidor valida a solicitação e fornece uma ID de árvore, que o cliente usa para operações

subsequentes no recurso.

- O cliente agora pode executar operações como ler, gravar ou modificar arquivos no recurso compartilhado.
- O CIFS suporta recursos como bloqueio de arquivos e acesso simultâneo para garantir a integridade dos dados.
- Quando o cliente tiver concluído suas operações, ele enviará uma solicitação de logoff para encerrar a sessão.
- O servidor libera a ID da sessão e os recursos associados.

Procedimento

Um problema muito comum ao configurar o sistema de arquivos remoto para dispositivos SNA é o erro "Falha ao montar".

Para entender melhor o que causou o problema, faça o seguinte:

Iniciar captura de pacote

- Faça login na CLI do dispositivo SNA usando as credenciais de sysadmin.
- Navegue até Avançado > Captura de pacotes
- Insira o endereço IP de compartilhamento remoto em Endereço IP do host, 45 como Filtro de porta, Mínimo de 60 segundos, 100 como duração e pacote respectivamente

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>

Captura de pacotes do CLI

Configurar e testar o sistema de arquivos remoto

- Faça login na interface do usuário do dispositivo SNA e navegue para 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.

Configurações de compartilhamento remoto

- Clique em Aplicar e Testar.

Fazer download e revisar a captura de pacotes

- Aguarde até que a captura de pacotes pare ou interrompa manualmente usando CTRL-C.
- Navegue até SNA appliance UI > Support > Browse Files > tcpdump.

Erro comum

Abra a captura de pacotes e aplique o filtro `ip.addr==ip_address_of_SNA && ip.addr==ip_address_of_remote_storage && tcp.port==445`.



Filtro de captura de pacote

Bloco de Porta TCP 445

Nenhuma resposta para vários pacotes SYN iniciados pelo dispositivo SNA junto com as tentativas de retransmissão TCP para o endereço IP do servidor de arquivos remoto.

No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000	0.000000	192.168.1.100		192.168.1.101	TCP	74	✓	0	36318 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	1.027965	1.027965	192.168.1.100		192.168.1.101	TCP	74	✓	0	[TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
3	2.015986	2.015986	192.168.1.100		192.168.1.101	TCP	74	✓	0	[TCP Retransmission] 36318 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
7	2.121444	2.121444	192.168.1.100		192.168.1.101	TCP	74	✓	0	39400 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
8	16.014554	16.014554	192.168.1.100		192.168.1.101	TCP	74	✓	0	[TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
9	2.016015	2.016015	192.168.1.100		192.168.1.101	TCP	74	✓	0	[TCP Retransmission] 39400 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

Bloco de porta

Solução: Permita a comunicação de porta TCP/445 entre o dispositivo SNA e o diretório/local de Compartilhamento de Arquivo Remoto do firewall.

O serviço não está em execução

O dispositivo SNA iniciou o pacote SYN pela porta TCP 445, no entanto o servidor SMB responde com RST,ACK.

No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000	0.000000	192.168.1.100		192.168.1.101	TCP	74	✓	0	49262 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	0.000468	0.000468	192.168.1.101		192.168.1.100	TCP	60	✓	0	445 → 49262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	8.007958	8.007958	192.168.1.100		192.168.1.101	TCP	74	✓	0	57866 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
12	0.000302	0.000302	192.168.1.101		192.168.1.100	TCP	60	✓	0	445 → 57866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

O serviço SMB não está em execução

Solução: Inicializar Compartilhamento de Arquivo SMB no respectivo servidor

SMB Versão 1/2/3 Desabilitada

O handshake TCP é concluído com êxito, mas a negociação SMB falha porque a versão SMB está sendo desabilitada.

No.	Time	delta time	Source	Time since previous frame	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000	0.000000	192.168.1.100		192.168.1.101	TCP	74	✓	0	55322 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	0.001424	0.001424	192.168.1.101		192.168.1.100	TCP	74	✓	0	445 → 55322 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
3	0.000086	0.000086	192.168.1.100		192.168.1.101	TCP	66	✓	0	55322 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=0
4	0.000401	0.000401	192.168.1.100		192.168.1.101	SMB2	310	✓	244	Negotiate Protocol Request
5	0.000197	0.000197	192.168.1.101		192.168.1.100	TCP	60	✓	0	445 → 55322 [RST, ACK] Seq=1 Ack=245 Win=0 Len=0
6	0.000079	0.000079	192.168.1.100		192.168.1.101	TCP	74	✓	0	55328 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
7	0.000152	0.000152	192.168.1.100		192.168.1.101	TCP	74	✓	0	445 → 55328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8	0.000021	0.000021	192.168.1.101		192.168.1.100	TCP	54	✓	0	55328 → 445 [RST] Seq=1 Win=0 Len=0

Versões SMB Desabilitadas

Solução: Ative a versão SMB apropriada no respectivo servidor.

Senha incorreta para compartilhamento SMB

O handshake TCP é concluído com êxito junto com a negociação SMB.

Resposta STATUS_LOGIN_FAILURE do servidor de compartilhamento de arquivos SMB.

No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
1	0.000000	0.000000	10.0.0.0	10.0.0.0	TCP	74	✓	0	53396 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=679743950 TSecr=0
2	0.000785	0.000785	10.0.0.0	10.0.0.0	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	0.000060	10.0.0.0	10.0.0.0	TCP	66	✓	0	53396 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=679743951 TSecr=323876616
4	0.000373	0.000468	10.0.0.0	10.0.0.0	SMB2	310	✓	244	Negotiate Protocol Request
5	0.000697	0.000324	10.0.0.0	10.0.0.0	SMB2	378	✓	312	Negotiate Protocol Response
6	0.000849	0.000152	10.0.0.0	10.0.0.0	TCP	66	✓	0	53396 → 445 [ACK] Seq=245 Ack=313 Win=67072 Len=0 TSval=679743952 TSecr=323876618
7	0.000852	0.000003	10.0.0.0	10.0.0.0	SMB2	202	✓	136	Session Setup Request, NTLMSSP_NEGOTIATE
8	0.000391	0.000439	10.0.0.0	10.0.0.0	SMB2	350	✓	284	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
9	0.000238	0.000153	10.0.0.0	10.0.0.0	SMB2	466	✓	400	Session Setup Request, NTLMSSP_AUTH, User: administrator
10	0.001390	0.001152	10.0.0.0	10.0.0.0	SMB2	143	✓	77	Session Setup Response, Error: STATUS_LOGIN_FAILURE

Solução: Digite a senha correta do usuário de login.

Problema de Permissão

O handshake TCP é concluído com êxito junto com a negociação SMB.

O logon no servidor de Compartilhamento de Arquivo foi bem-sucedido.

Resposta de STATUS_BAD_NETWORK_NAME do servidor de compartilhamento de arquivos SMB.

No.	Time	delta time	Source	Destination	Protocol	Length	Ethernet	TCP Segment Len	Info
9	0.014775	0.014775	10.0.0.0	10.0.0.0	TCP	74	✓	0	53018 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=681143321 TSecr=0
10	0.000030	0.000030	10.0.0.0	10.0.0.0	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	0.000080	0.000050	10.0.0.0	10.0.0.0	TCP	66	✓	0	53018 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=681143322 TSecr=3252760
12	0.000159	0.000079	10.0.0.0	10.0.0.0	SMB2	310	✓	244	Negotiate Protocol Request
13	0.000642	0.000483	10.0.0.0	10.0.0.0	SMB2	378	✓	312	Negotiate Protocol Response
14	0.000026	0.000016	10.0.0.0	10.0.0.0	TCP	66	✓	0	53018 → 445 [ACK] Seq=245 Ack=313 Win=67072 Len=0 TSval=681143323 TSecr=325
15	0.000040	0.000014	10.0.0.0	10.0.0.0	SMB2	202	✓	136	Session Setup Request, NTLMSSP_NEGOTIATE
16	0.000333	0.000293	10.0.0.0	10.0.0.0	SMB2	350	✓	284	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHA
17	0.000047	0.000014	10.0.0.0	10.0.0.0	SMB2	466	✓	400	Session Setup Request, NTLMSSP_AUTH, User: administrator
18	0.001066	0.001019	10.0.0.0	10.0.0.0	SMB2	142	✓	76	Session Setup Response
19	0.000059	0.000013	10.0.0.0	10.0.0.0	SMB2	184	✓	118	Tree Connect Request Tree: \\10.0.0.0\IPC\$
20	0.000295	0.000236	10.0.0.0	10.0.0.0	SMB2	150	✓	84	Tree Connect Response
21	0.000034	0.000014	10.0.0.0	10.0.0.0	SMB2	184	✓	118	Tree Connect Request Tree: \\10.0.0.0\test
22	0.000183	0.000149	10.0.0.0	10.0.0.0	SMB2	143	✓	77	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
23	0.001127	0.001044	10.0.0.0	10.0.0.0	SMB2	232	✓	166	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \\10.0.0.0\test
24	0.002842	0.001715	10.0.0.0	10.0.0.0	SMB2	143	✓	77	Ioctl Response, Error: STATUS_PENDING
25	0.001391	0.001149	10.0.0.0	10.0.0.0	SMB2	143	✓	77	Ioctl Response, Error: STATUS_NOT_FOUND

Solução: Atribuir permissão de leitura/gravação ao usuário de logon.

Sessão terminada sem graça

A operação de backup do banco de dados pode ser interrompida se o armazenamento do diretório/local de arquivos remotos se esgotar.

A sessão SMB é um loop de Close Request e Close Response.

No.	Time	delta time	Source	Destination	Protocol	Length	Info
184	0.000000	0.000000	10.0.0.0	10.0.0.0	TCP	66	49556 → 445 [ACK] Seq=17627 Ack=23655 Win=1025 Len=0 TSval=1097637759 TSecr=1329621664
183	0.001254	0.001254	10.0.0.0	10.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
182	0.998491	0.998491	10.0.0.0	10.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
181	0.000039	0.000039	10.0.0.0	10.0.0.0	TCP	66	49556 → 445 [ACK] Seq=17279 Ack=23211 Win=1025 Len=0 TSval=1097636759 TSecr=1329620665
180	0.001059	0.001020	10.0.0.0	10.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
179	0.999102	0.999102	10.0.0.0	10.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
178	0.000035	0.000035	10.0.0.0	10.0.0.0	TCP	66	49556 → 445 [ACK] Seq=16931 Ack=22767 Win=1025 Len=0 TSval=1097635759 TSecr=1329619664
177	0.000054	0.000019	10.0.0.0	10.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
176	0.999512	0.999512	10.0.0.0	10.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
175	0.000023	0.000023	10.0.0.0	10.0.0.0	TCP	66	49556 → 445 [ACK] Seq=16583 Ack=22323 Win=1025 Len=0 TSval=1097634758 TSecr=1329618664
174	0.000065	0.000042	10.0.0.0	10.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
173	0.998652	0.998652	10.0.0.0	10.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request
172	0.000035	0.000035	10.0.0.0	10.0.0.0	TCP	66	49556 → 445 [ACK] Seq=16235 Ack=21879 Win=1025 Len=0 TSval=1097633759 TSecr=1329617664
171	0.001120	0.001085	10.0.0.0	10.0.0.0	SMB2	510	Create Response File: ;GetInfo Response;Close Response
170	0.039882	0.039882	10.0.0.0	10.0.0.0	SMB2	414	Create Request File: ;GetInfo Request FS_INFO/FileFsFullSizeInformation;Close Request

Descarte de Sessão SMB Ingraciosa

Solução: Reinicie o dispositivo SNA.

Se for necessária assistência adicional para investigar o problema , recomendamos criar um caso de TAC [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)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.