SMB / CIFS TRANSACTIONS PERFORMANCE ANALYSIS

performance vision

Content

1. Product Features

2. SMB Overview & Use Cases

- 1. Connect and Browse Files
- 2. Login Authorization Failure
- 3. Put a File on a Remote Folder
- 4. Not Authorized to Delete a Remote File

3. Documentation + Q&A

© Performance Vision

Content

performance vision

1. **Product Features**

2. SMB Overview & Use Cases

- 1. Connect and Browse Files
- 2. Login Authorization Failure
- 3. Put a File on a Remote Folder
- 4. Not Authorized to Delete a Remote File

3. Documentation + Q&A

© Performance Vision

What is SMB Used for?

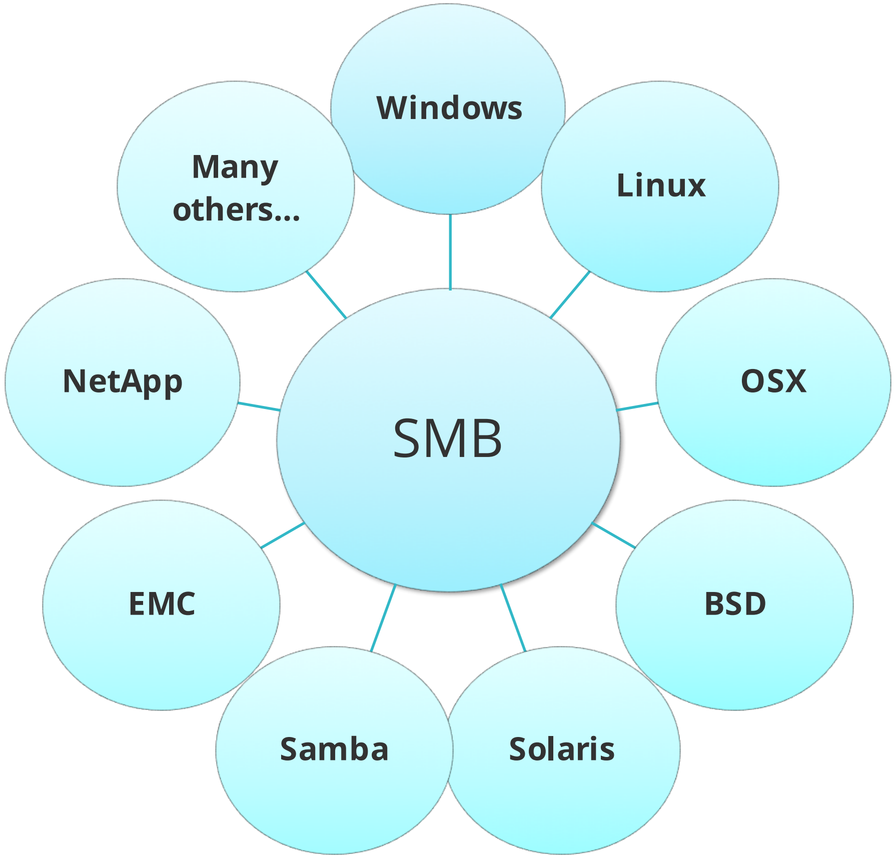
Remote Files Manipulation

- Open
- Close
- Read
- Write
- Rename
- Move
- …

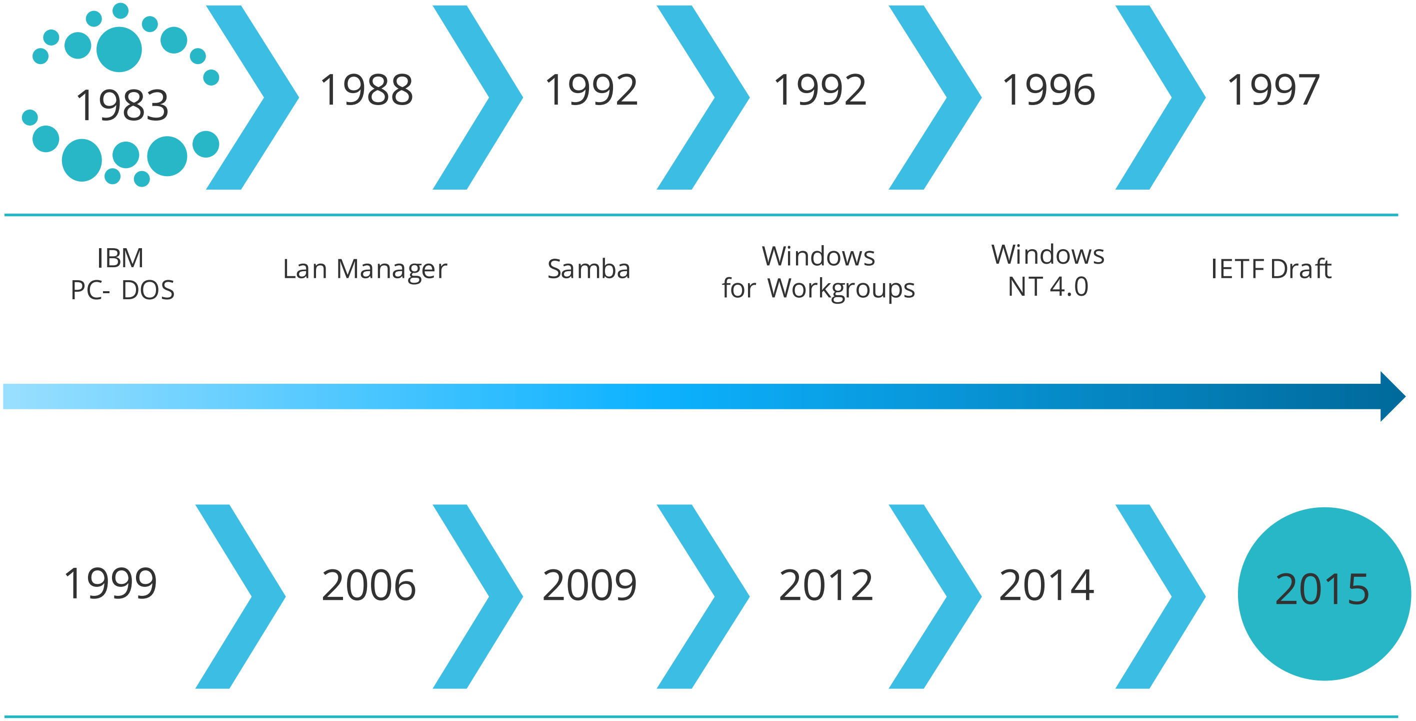
Inter-process Communication

- Through a Named Pipe mechanism
- For custom Application Level Protocols

SMB is Widely Supported



SMB: a Long History



1983 IBM PC- DOS

1988 Lan Manager

1992 Samba

1992 Windows for Workgroups

1996 Windows NT 4.0

1997 IETF Draft

1999

2006

2009

2012

2014

2015

SMB/CIFS: Business Critical Elements

Today the SMB Protocol

Is widely used by both Users & Applications

Is a key component when accessing to remote resources

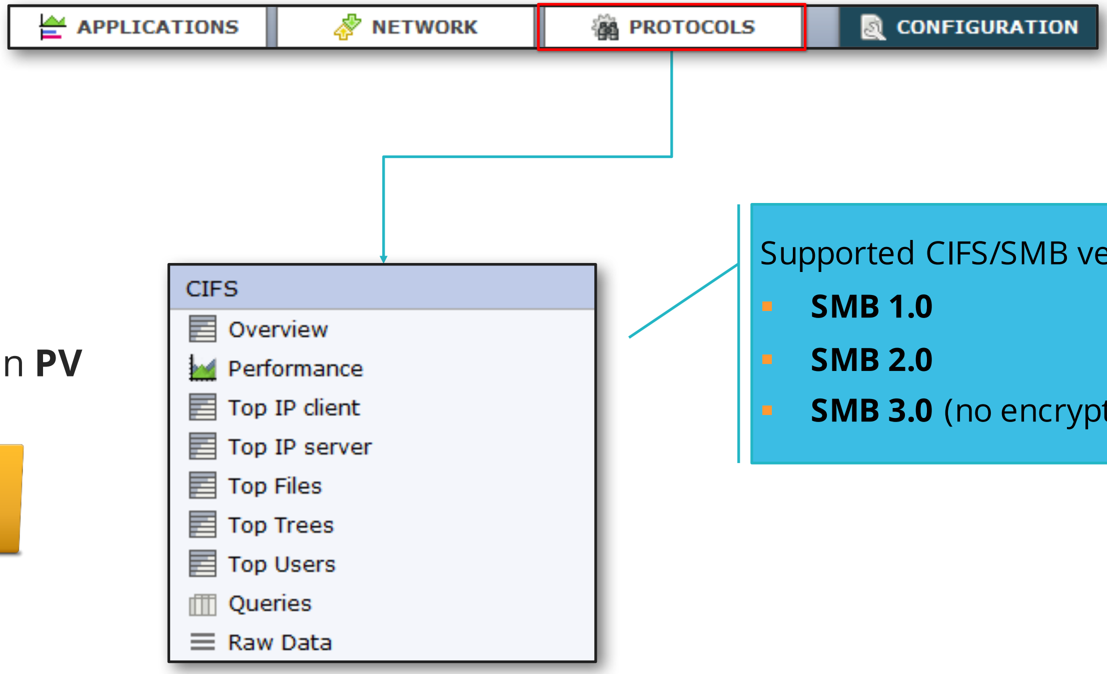
Performances are extremely variable due to the heterogeneity of use cases

SMB/CIFS Analysis: User Benefits

- **Monitor** SMB/CIFS Performance
- **Identify** Slow Transactions
- **Troubleshoot** File Sharing Issues
  - Access Rights
  - Deleted or Corrupted Files
  - Insufficient Resources
  - All Errors and Warnings
- **Correlate** *File Sharing* Problems with *Network* Performance Issues

In-Depth SMB/CIFS Performance Analysis

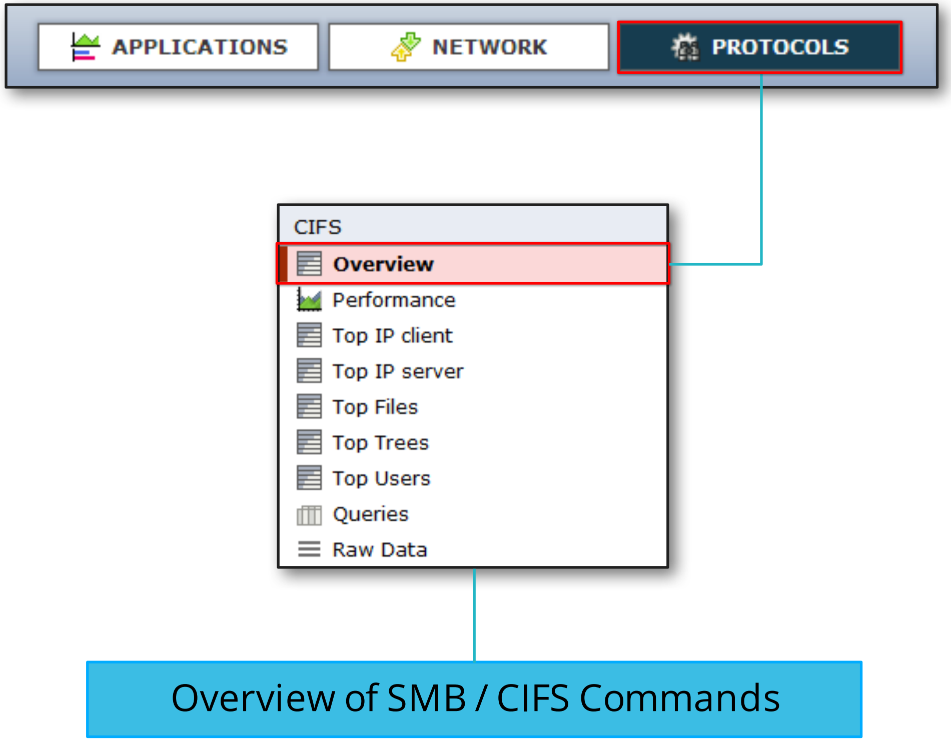
CIFS/SMB in **PV**



Supported CIFS/SMB versions

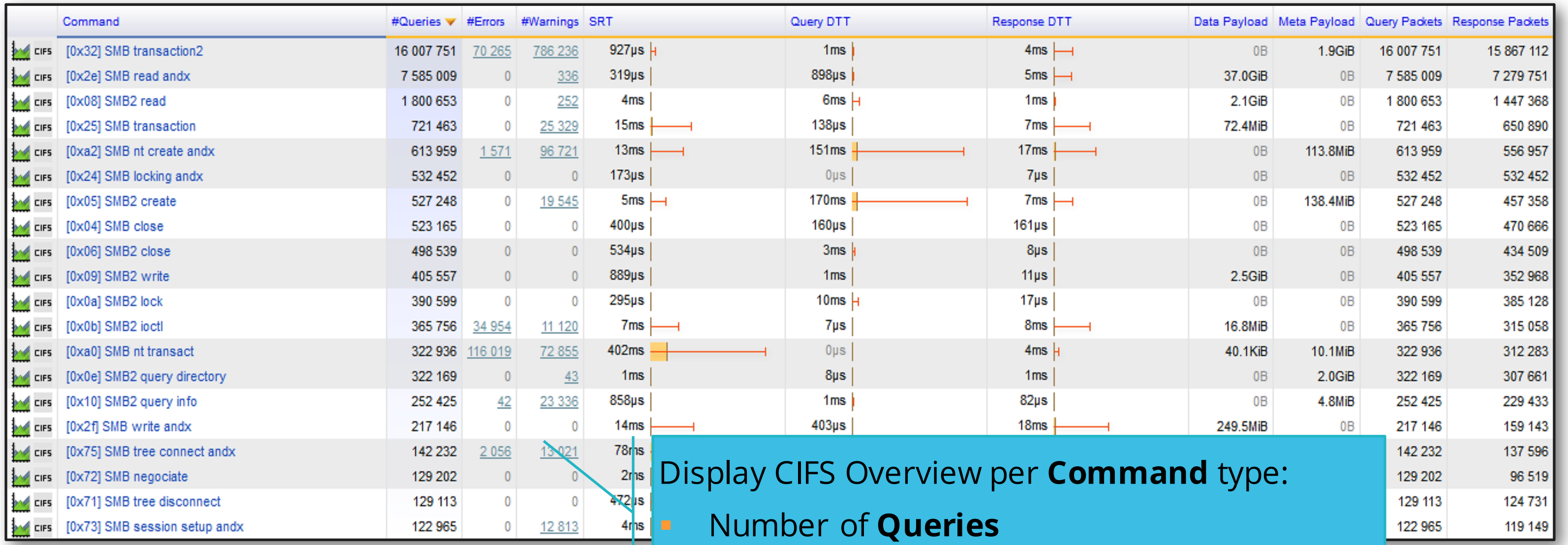
- **SMB 1.0**
- **SMB 2.0**
- **SMB 3.0** (no encryption)

SMB / CIFS Overview



Overview of SMB / CIFS Commands

Overview of SMB / CIFS Commands



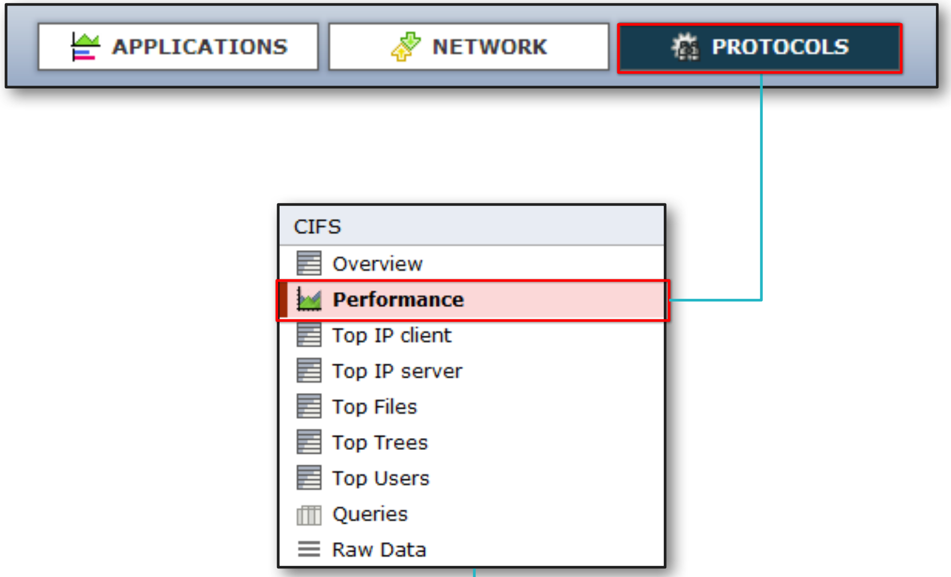
	Command	#Queries	#Errors	#Warnings	SRT	Query DTT	Response DTT	Data Payload	Meta Payload	Query Packets	Response Packets
CIFS	[0x32] SMB transaction2	16 007 751	70 265	786 236	927µs	1ms	4ms	0B	1.9GiB	16 007 751	15 867 112
CIFS	[0x2e] SMB read andx	7 585 009	0	336	319µs	898µs	5ms	37.0GiB	0B	7 585 009	7 279 751
CIFS	[0x08] SMB2 read	1 800 653	0	252	4ms	6ms	1ms	2.1GiB	0B	1 800 653	1 447 368
CIFS	[0x25] SMB transaction	721 463	0	25 329	15ms	138µs	7ms	72.4MiB	0B	721 463	650 890
CIFS	[0xa2] SMB nt create andx	613 959	1 571	96 721	13ms	151ms	17ms	0B	113.8MiB	613 959	556 957
CIFS	[0x24] SMB locking andx	532 452	0	0	173µs	0µs	7µs	0B	0B	532 452	532 452
CIFS	[0x05] SMB2 create	527 248	0	19 545	5ms	170ms	7ms	0B	138.4MiB	527 248	457 358
CIFS	[0x04] SMB close	523 165	0	0	400µs	160µs	161µs	0B	0B	523 165	470 666
CIFS	[0x06] SMB2 close	498 539	0	0	534µs	3ms	8µs	0B	0B	498 539	434 509
CIFS	[0x09] SMB2 write	405 557	0	0	889µs	1ms	11µs	2.5GiB	0B	405 557	352 968
CIFS	[0x0a] SMB2 lock	390 599	0	0	295µs	10ms	17µs	0B	0B	390 599	385 128
CIFS	[0x0b] SMB2 ioctl	365 756	34 954	11 120	7ms	7µs	8ms	16.8MiB	0B	365 756	315 058
CIFS	[0xa0] SMB nt transact	322 936	116 019	72 855	402ms	0µs	4ms	40.1KiB	10.1MiB	322 936	312 283
CIFS	[0x0e] SMB2 query directory	322 169	0	43	1ms	8µs	1ms	0B	2.0GiB	322 169	307 661
CIFS	[0x10] SMB2 query info	252 425	42	23 336	858µs	1ms	82µs	0B	4.8MiB	252 425	229 433
CIFS	[0x2f] SMB write andx	217 146	0	0	14ms	403µs	18ms	249.5MiB	0B	217 146	159 143
CIFS	[0x75] SMB tree connect andx	142 232	2 056	13 021	78ms					142 232	137 596
CIFS	[0x72] SMB negociate	129 202	0	0	2ms					129 202	96 519
CIFS	[0x71] SMB tree disconnect	129 113	0	0	472µs					129 113	124 731
CIFS	[0x73] SMB session setup andx	122 965	0	12 813	4ms					122 965	119 149

Display CIFS Overview per **Command** type:

- Number of **Queries**
- Number of **Errors** and **Warnings**
- **Performance** Metrics (SRT, DTT)
- **Payload** and Number of **Packets** (PDUs)

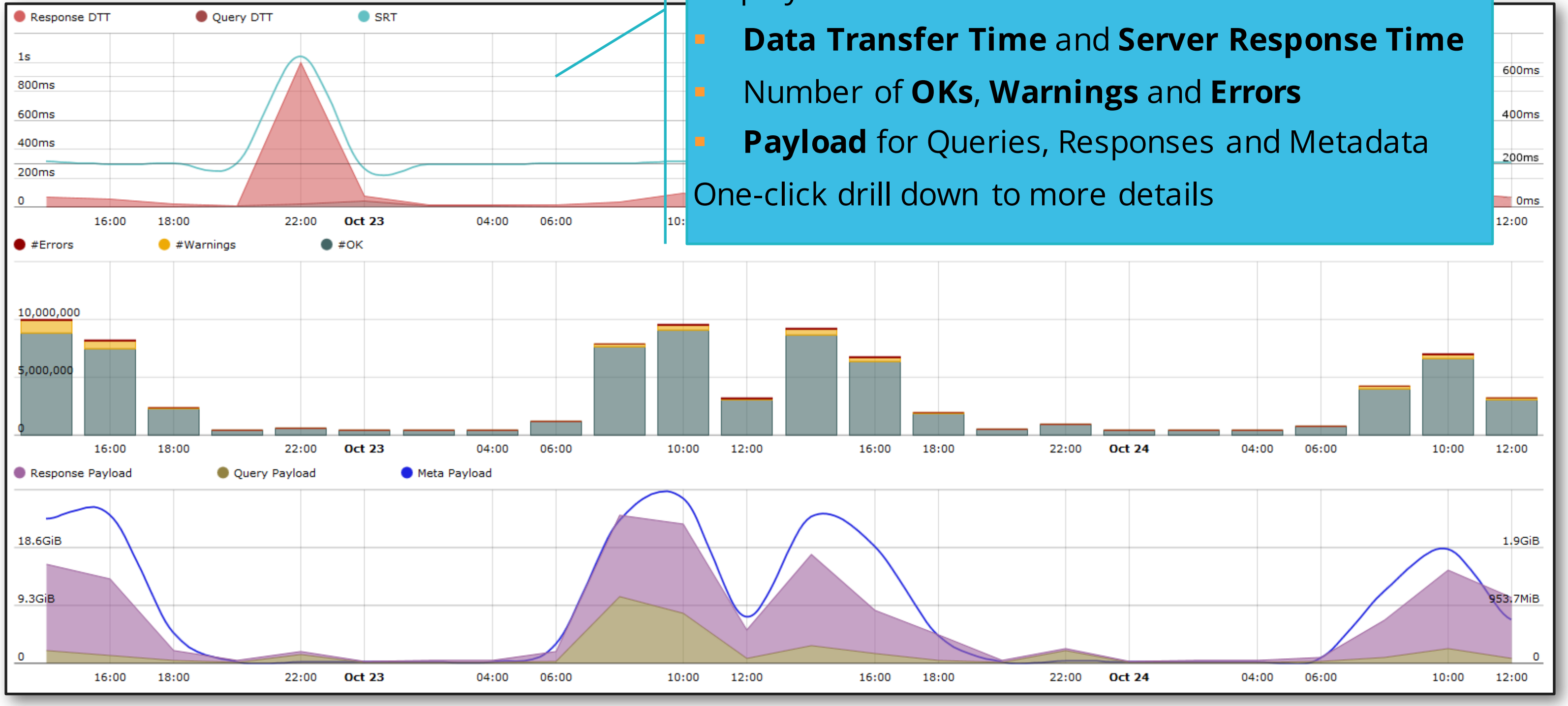
One-click drill down to more details

SMB / CIFS Performance



Performance of SMB / CIFS Queries over Time

Performance of SMB / CIFS Queries over Time

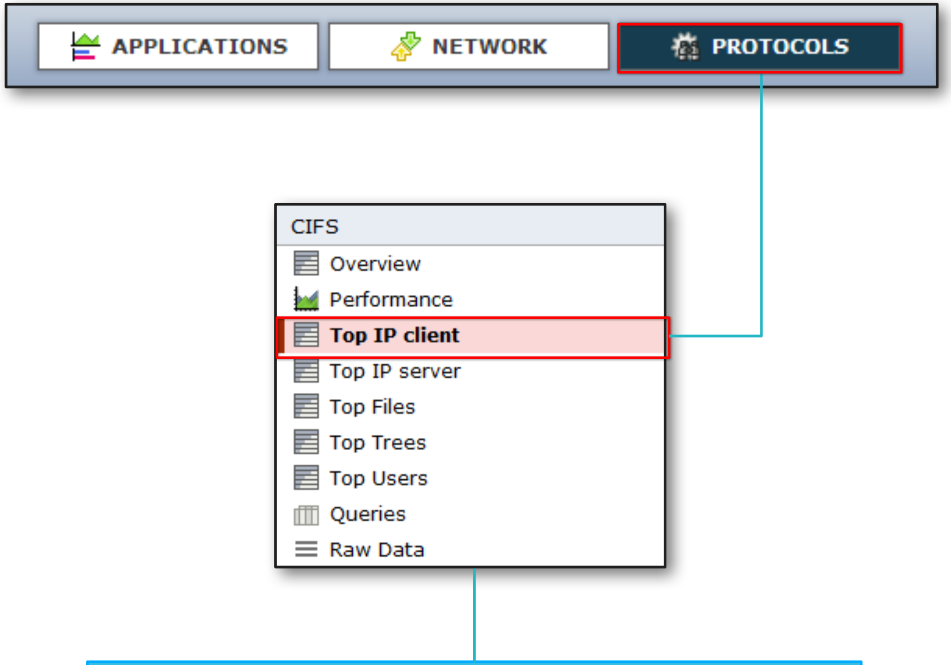


Display SMB / CIFS **Performance** metrics over time:

- **Data Transfer Time** and **Server Response Time**
- Number of **OKs**, **Warnings** and **Errors**
- **Payload** for Queries, Responses and Metadata

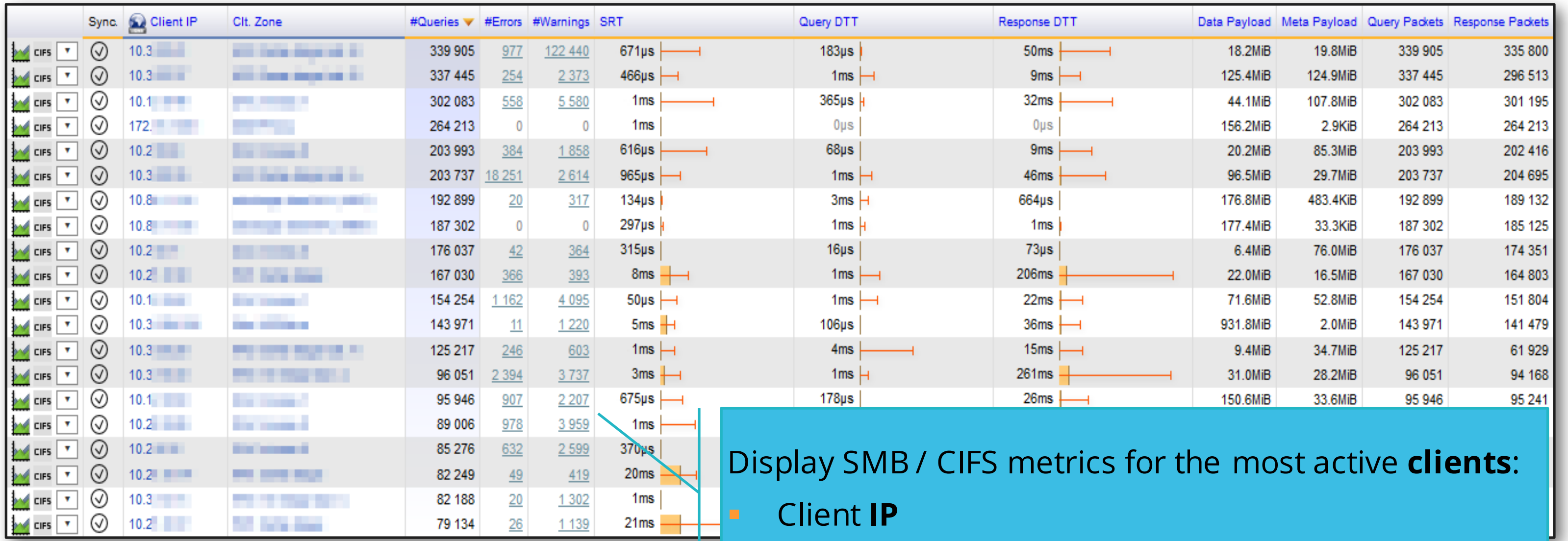
One-click drill down to more details

SMB / CIFS Clients



SMB / CIFS Most Active Clients

SMB / CIFS Most Active **Clients**



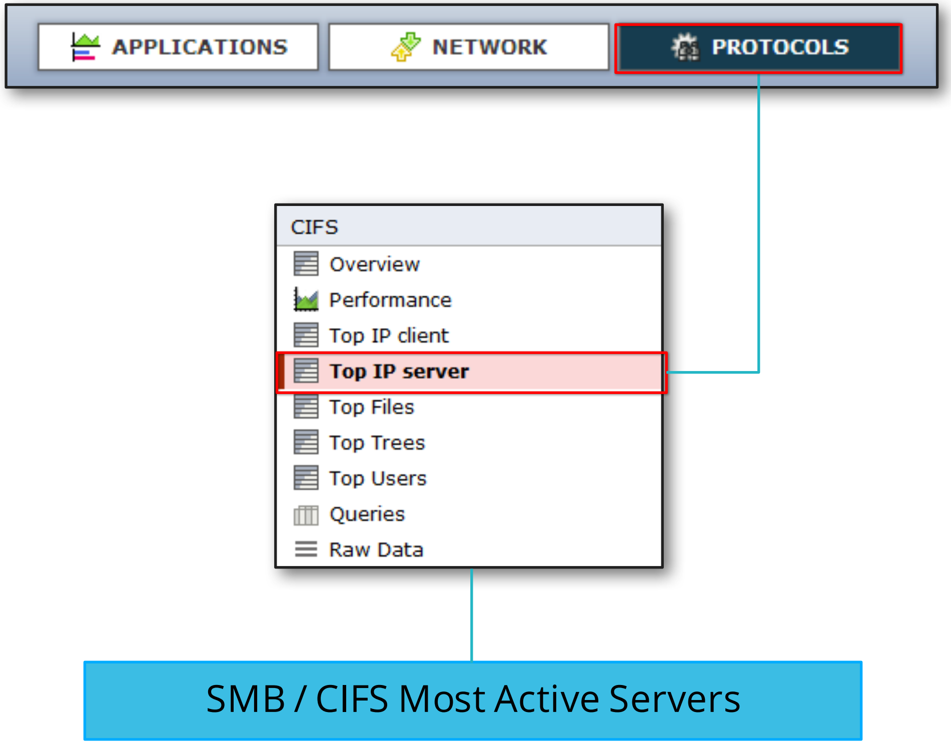
	Sync.	Client IP	Clt. Zone	#Queries ▼	#Errors	#Warnings	SRT	Query DTT	Response DTT	Data Payload	Meta Payload	Query Packets	Response Packets
CIFS ▾	✓	10.3 [redacted]	[redacted]	339 905	977	122 440	671µs	183µs	50ms	18.2MiB	19.8MiB	339 905	335 800
CIFS ▾	✓	10.3 [redacted]	[redacted]	337 445	254	2 373	466µs	1ms	9ms	125.4MiB	124.9MiB	337 445	296 513
CIFS ▾	✓	10.1 [redacted]	[redacted]	302 083	558	5 580	1ms	365µs	32ms	44.1MiB	107.8MiB	302 083	301 195
CIFS ▾	✓	172. [redacted]	[redacted]	264 213	0	0	1ms	0µs	0µs	156.2MiB	2.9KiB	264 213	264 213
CIFS ▾	✓	10.2 [redacted]	[redacted]	203 993	384	1 858	616µs	68µs	9ms	20.2MiB	85.3MiB	203 993	202 416
CIFS ▾	✓	10.3 [redacted]	[redacted]	203 737	18 251	2 614	965µs	1ms	46ms	96.5MiB	29.7MiB	203 737	204 695
CIFS ▾	✓	10.8 [redacted]	[redacted]	192 899	20	317	134µs	3ms	664µs	176.8MiB	483.4KiB	192 899	189 132
CIFS ▾	✓	10.8 [redacted]	[redacted]	187 302	0	0	297µs	1ms	1ms	177.4MiB	33.3KiB	187 302	185 125
CIFS ▾	✓	10.2 [redacted]	[redacted]	176 037	42	364	315µs	16µs	73µs	6.4MiB	76.0MiB	176 037	174 351
CIFS ▾	✓	10.2 [redacted]	[redacted]	167 030	366	393	8ms	1ms	206ms	22.0MiB	16.5MiB	167 030	164 803
CIFS ▾	✓	10.1 [redacted]	[redacted]	154 254	1 162	4 095	50µs	1ms	22ms	71.6MiB	52.8MiB	154 254	151 804
CIFS ▾	✓	10.3 [redacted]	[redacted]	143 971	11	1 220	5ms	106µs	36ms	931.8MiB	2.0MiB	143 971	141 479
CIFS ▾	✓	10.3 [redacted]	[redacted]	125 217	246	603	1ms	4ms	15ms	9.4MiB	34.7MiB	125 217	61 929
CIFS ▾	✓	10.3 [redacted]	[redacted]	96 051	2 394	3 737	3ms	1ms	261ms	31.0MiB	28.2MiB	96 051	94 168
CIFS ▾	✓	10.1 [redacted]	[redacted]	95 946	907	2 207	675µs	178µs	26ms	150.6MiB	33.6MiB	95 946	95 241
CIFS ▾	✓	10.2 [redacted]	[redacted]	89 006	978	3 959	1ms						
CIFS ▾	✓	10.2 [redacted]	[redacted]	85 276	632	2 599	370µs						
CIFS ▾	✓	10.2 [redacted]	[redacted]	82 249	49	419	20ms						
CIFS ▾	✓	10.3 [redacted]	[redacted]	82 188	20	1 302	1ms						
CIFS ▾	✓	10.2 [redacted]	[redacted]	79 134	26	1 139	21ms						

Display SMB / CIFS metrics for the most active **clients**:

- Client **IP**
- Number of **Queries**, **Errors** and **Warnings**
- **Performance** Metrics (SRT, DTT)
- **Payloads** and Number of **Packets** (PDUs)

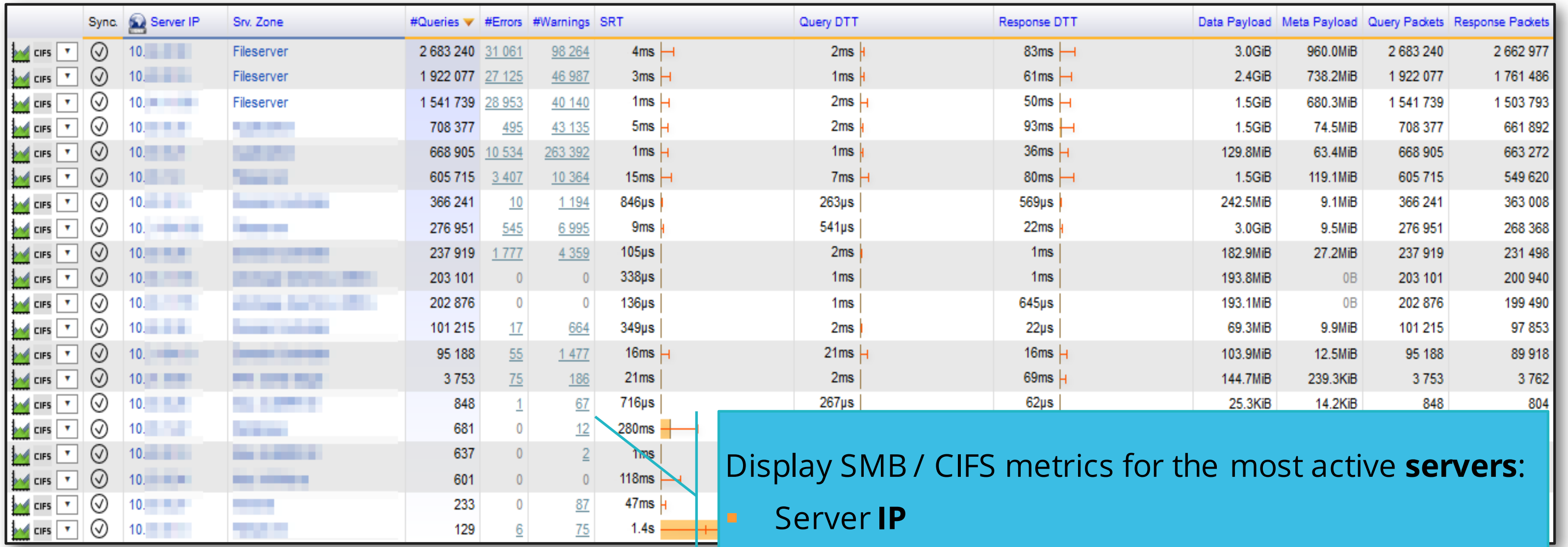
One-click drill down to queries and errors

SMB / CIFS Servers



SMB / CIFS Most Active Servers

SMB / CIFS Most Active Servers



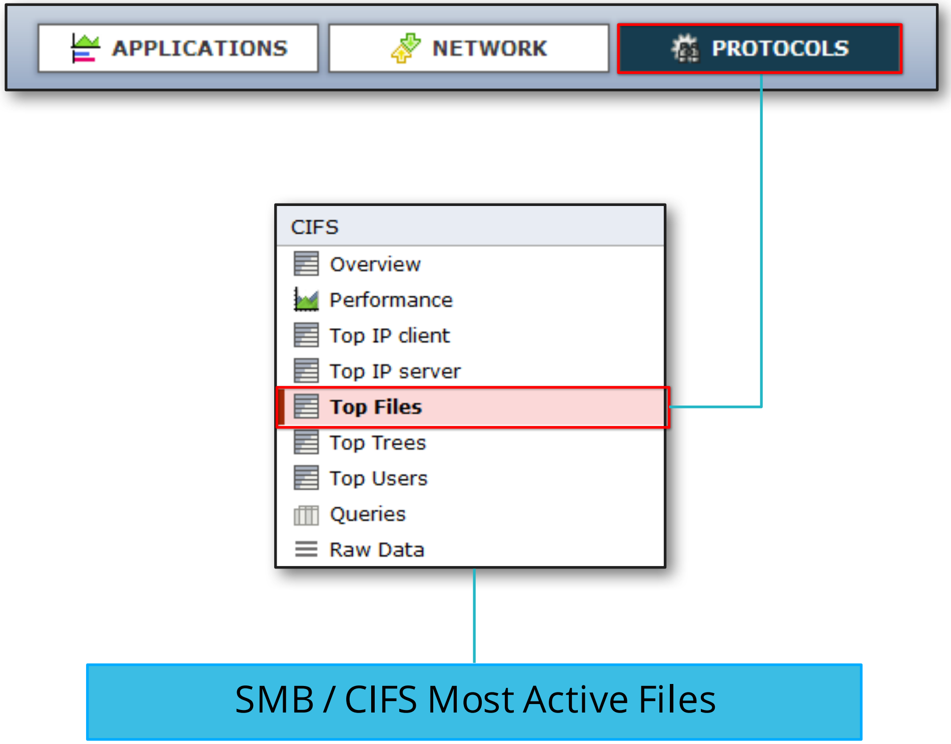
	Sync.	Server IP	Srv. Zone	#Queries ▾	#Errors	#Warnings	SRT	Query DTT	Response DTT	Data Payload	Meta Payload	Query Packets	Response Packets
CIFS ▾	✓	10.[redacted]	Fileserver	2 683 240	31 061	98 264	4ms	2ms	83ms	3.0GiB	960.0MiB	2 683 240	2 662 977
CIFS ▾	✓	10.[redacted]	Fileserver	1 922 077	27 125	46 987	3ms	1ms	61ms	2.4GiB	738.2MiB	1 922 077	1 761 486
CIFS ▾	✓	10.[redacted]	Fileserver	1 541 739	28 953	40 140	1ms	2ms	50ms	1.5GiB	680.3MiB	1 541 739	1 503 793
CIFS ▾	✓	10.[redacted]	[redacted]	708 377	495	43 135	5ms	2ms	93ms	1.5GiB	74.5MiB	708 377	661 892
CIFS ▾	✓	10.[redacted]	[redacted]	668 905	10 534	263 392	1ms	1ms	36ms	129.8MiB	63.4MiB	668 905	663 272
CIFS ▾	✓	10.[redacted]	[redacted]	605 715	3 407	10 364	15ms	7ms	80ms	1.5GiB	119.1MiB	605 715	549 620
CIFS ▾	✓	10.[redacted]	[redacted]	366 241	10	1 194	846µs	263µs	569µs	242.5MiB	9.1MiB	366 241	363 008
CIFS ▾	✓	10.[redacted]	[redacted]	276 951	545	6 995	9ms	541µs	22ms	3.0GiB	9.5MiB	276 951	268 368
CIFS ▾	✓	10.[redacted]	[redacted]	237 919	1 777	4 359	105µs	2ms	1ms	182.9MiB	27.2MiB	237 919	231 498
CIFS ▾	✓	10.[redacted]	[redacted]	203 101	0	0	338µs	1ms	1ms	193.8MiB	0B	203 101	200 940
CIFS ▾	✓	10.[redacted]	[redacted]	202 876	0	0	136µs	1ms	645µs	193.1MiB	0B	202 876	199 490
CIFS ▾	✓	10.[redacted]	[redacted]	101 215	17	664	349µs	2ms	22µs	69.3MiB	9.9MiB	101 215	97 853
CIFS ▾	✓	10.[redacted]	[redacted]	95 188	55	1 477	16ms	21ms	16ms	103.9MiB	12.5MiB	95 188	89 918
CIFS ▾	✓	10.[redacted]	[redacted]	3 753	75	186	21ms	2ms	69ms	144.7MiB	239.3KiB	3 753	3 762
CIFS ▾	✓	10.[redacted]	[redacted]	848	1	67	716µs	267µs	62µs	25.3KiB	14.2KiB	848	804
CIFS ▾	✓	10.[redacted]	[redacted]	681	0	12	280ms						
CIFS ▾	✓	10.[redacted]	[redacted]	637	0	2	1ms						
CIFS ▾	✓	10.[redacted]	[redacted]	601	0	0	118ms						
CIFS ▾	✓	10.[redacted]	[redacted]	233	0	87	47ms						
CIFS ▾	✓	10.[redacted]	[redacted]	129	6	75	1.4s						

Display SMB / CIFS metrics for the most active **servers**:

- Server **IP**
- Number of **Queries**, **Errors** and **Warnings**
- **Performance** Metrics (SRT, DTT)
- **Payloads** and Number of **Packets** (PDUs)

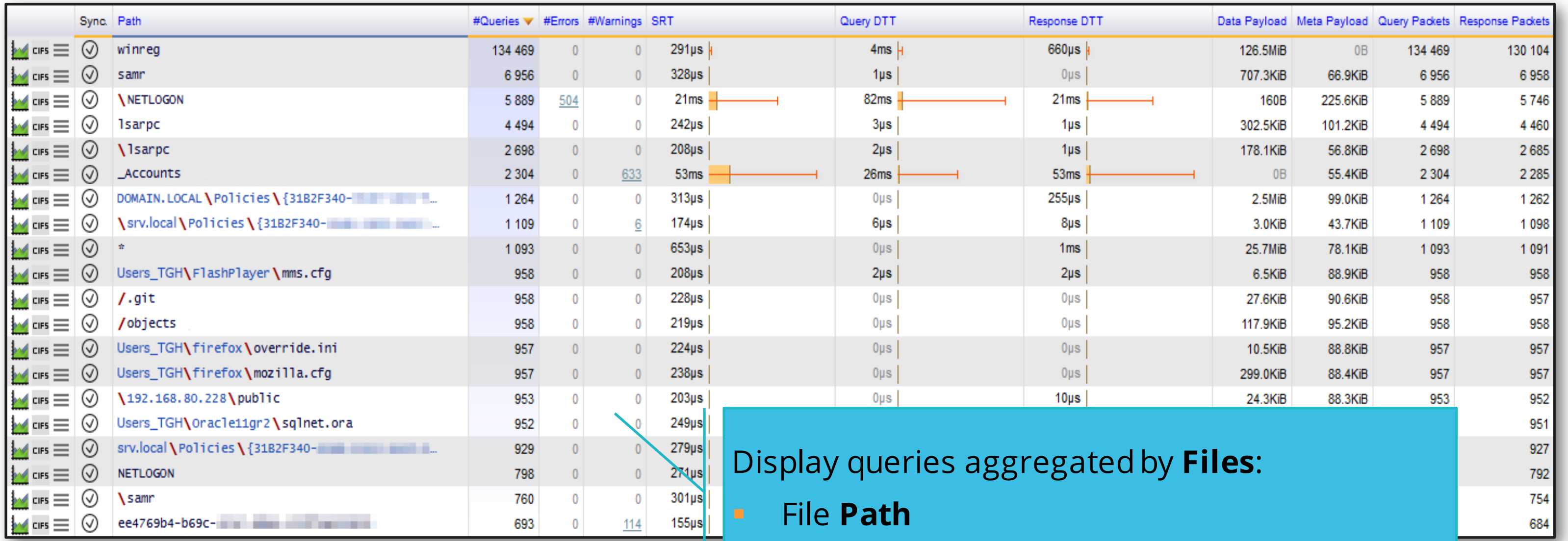
One-click drill down to queries and errors

SMB / CIFS Files



SMB / CIFS Most Active Files

SMB / CIFS Top Files



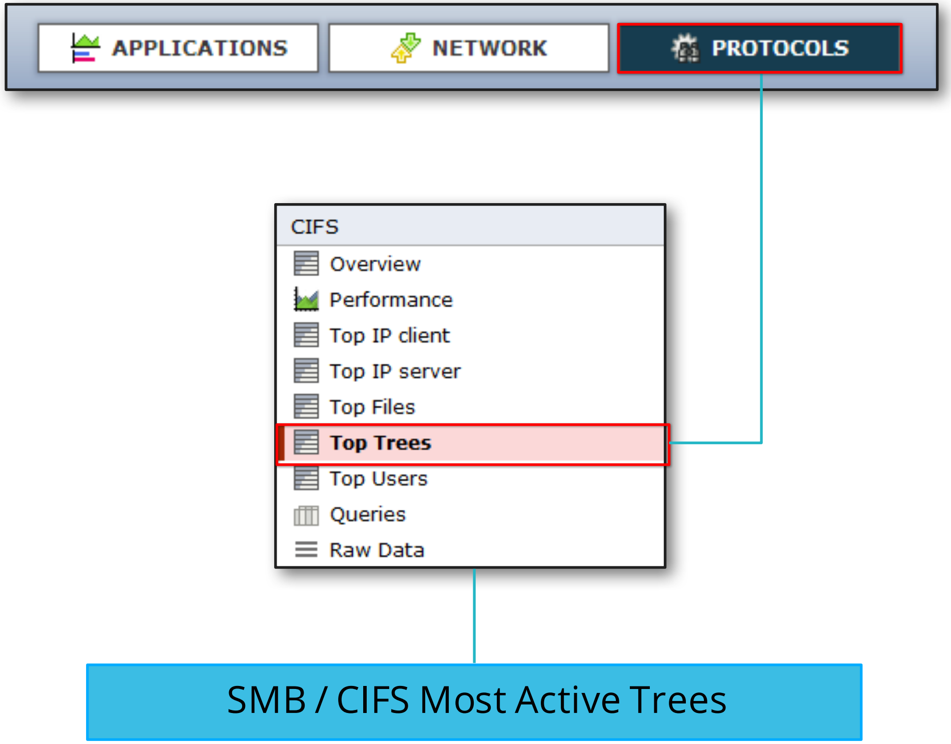
	Sync.	Path	#Queries	#Errors	#Warnings	SRT	Query DTT	Response DTT	Data Payload	Meta Payload	Query Packets	Response Packets
CIFS	✓	winreg	134 469	0	0	291µs	4ms	660µs	126.5MiB	0B	134 469	130 104
CIFS	✓	samr	6 956	0	0	328µs	1µs	0µs	707.3KiB	66.9KiB	6 956	6 958
CIFS	✓	\NETLOGON	5 889	504	0	21ms	82ms	21ms	160B	225.6KiB	5 889	5 746
CIFS	✓	lsarpc	4 494	0	0	242µs	3µs	1µs	302.5KiB	101.2KiB	4 494	4 460
CIFS	✓	\lsarpc	2 698	0	0	208µs	2µs	1µs	178.1KiB	56.8KiB	2 698	2 685
CIFS	✓	_Accounts	2 304	0	633	53ms	26ms	53ms	0B	55.4KiB	2 304	2 285
CIFS	✓	DOMAIN.LOCAL\Policies\{31B2F340-[redacted]...	1 264	0	0	313µs	0µs	255µs	2.5MiB	99.0KiB	1 264	1 262
CIFS	✓	\srv.local\Policies\{31B2F340-[redacted]...	1 109	0	6	174µs	6µs	8µs	3.0KiB	43.7KiB	1 109	1 098
CIFS	✓	*	1 093	0	0	653µs	0µs	1ms	25.7MiB	78.1KiB	1 093	1 091
CIFS	✓	Users_TGH\FlashPlayer\mms.cfg	958	0	0	208µs	2µs	2µs	6.5KiB	88.9KiB	958	958
CIFS	✓	/.git	958	0	0	228µs	0µs	0µs	27.6KiB	90.6KiB	958	957
CIFS	✓	/objects	958	0	0	219µs	0µs	0µs	117.9KiB	95.2KiB	958	958
CIFS	✓	Users_TGH\firefox\override.ini	957	0	0	224µs	0µs	0µs	10.5KiB	88.8KiB	957	957
CIFS	✓	Users_TGH\firefox\mozilla.cfg	957	0	0	238µs	0µs	0µs	299.0KiB	88.4KiB	957	957
CIFS	✓	\192.168.80.228\public	953	0	0	203µs	0µs	10µs	24.3KiB	88.3KiB	953	952
CIFS	✓	Users_TGH\Oracle11gr2\sqlnet.ora	952	0	0	249µs						951
CIFS	✓	srv.local\Policies\{31B2F340-[redacted]...	929	0	0	279µs						927
CIFS	✓	NETLOGON	798	0	0	271µs						792
CIFS	✓	\samr	760	0	0	301µs						754
CIFS	✓	ee4769b4-b69c-[redacted]	693	0	114	155µs						684

Display queries aggregated by **Files**:

- File **Path**
- Number of **Queries**, **Errors** and **Warnings**
- **Performance** Metrics (SRT, DTT)
- **Payloads** and Number of **Packets** (PDUs)

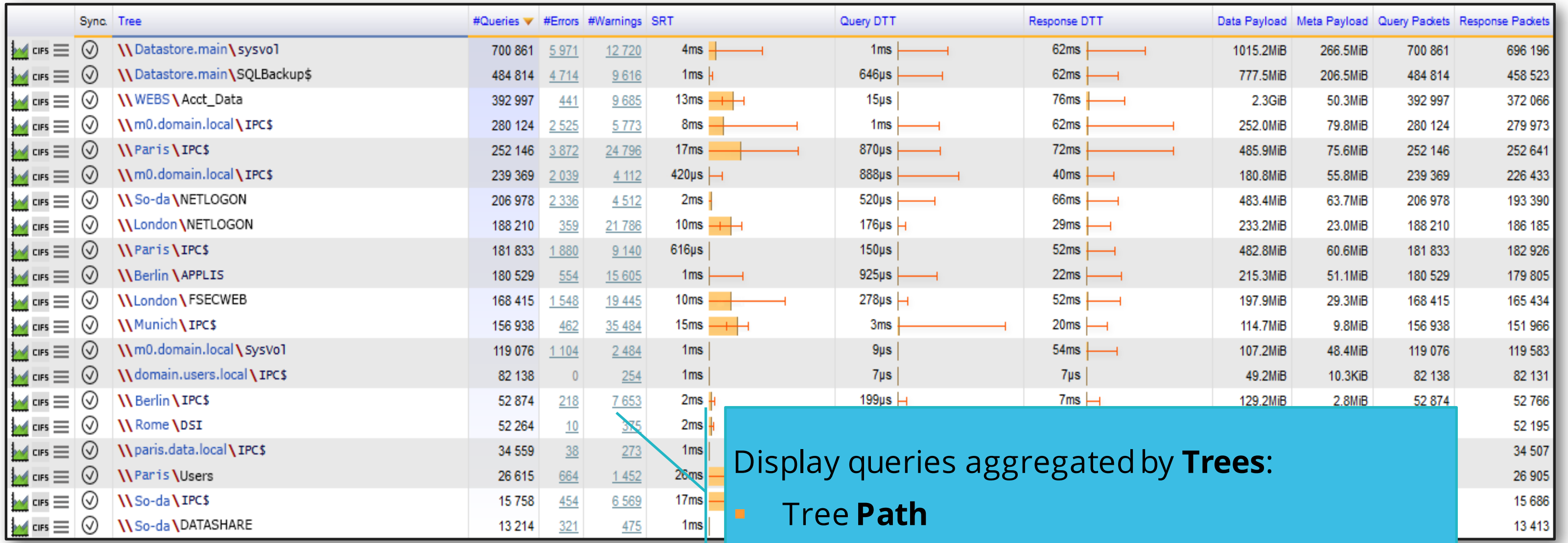
One-click drill down to queries and errors

SMB / CIFS Trees



SMB / CIFS Most Active Trees

SMB / CIFS Top Trees



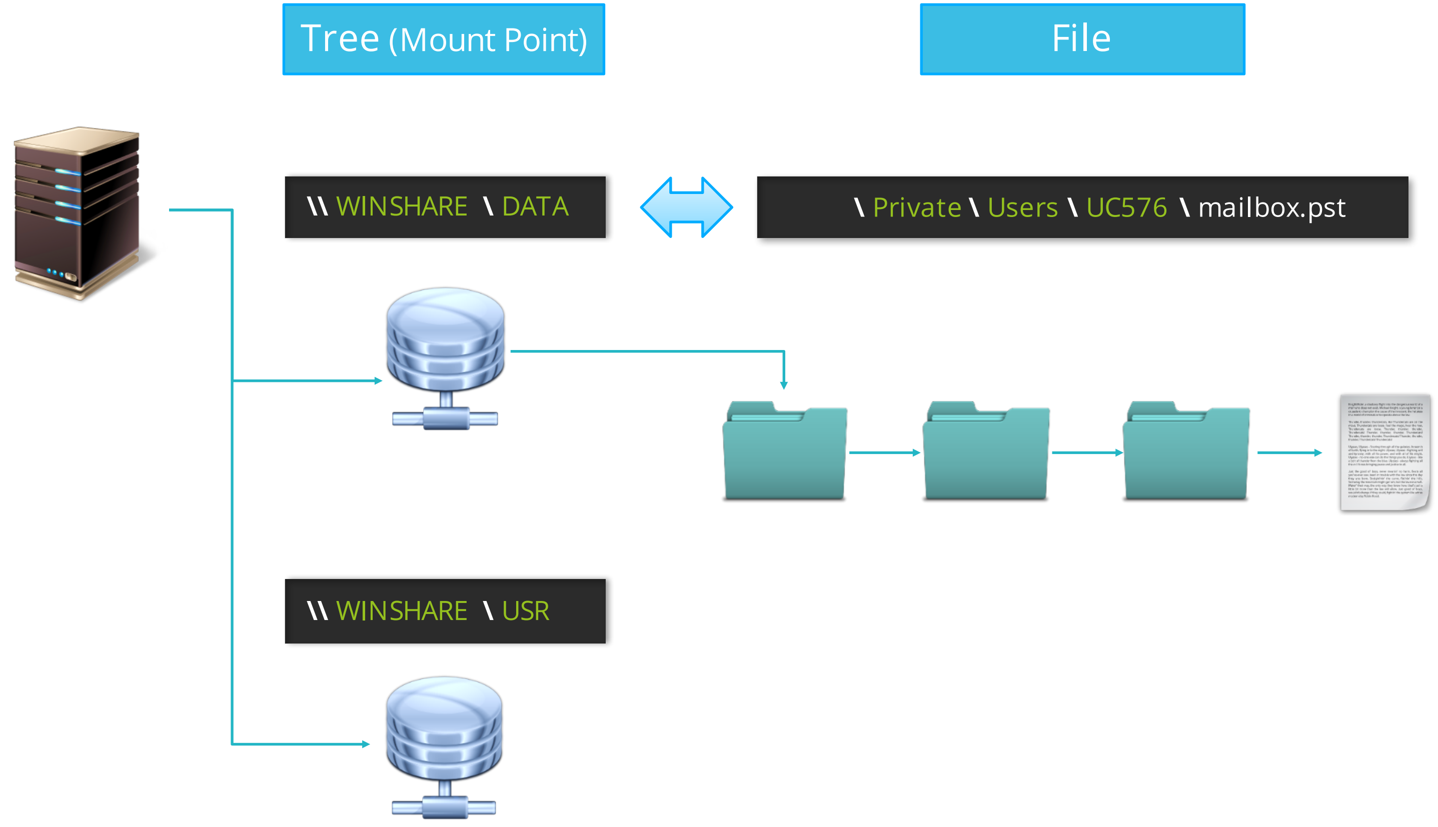
	Sync.	Tree	#Queries	#Errors	#Warnings	SRT	Query DTT	Response DTT	Data Payload	Meta Payload	Query Packets	Response Packets
CIFS	✓	\\Datastore.main\sysvol	700 861	5 971	12 720	4ms	1ms	62ms	1015.2MiB	266.5MiB	700 861	696 196
CIFS	✓	\\Datastore.main\SQLBackup$	484 814	4 714	9 616	1ms	646µs	62ms	777.5MiB	206.5MiB	484 814	458 523
CIFS	✓	\\WEBS\Acct_Data	392 997	441	9 685	13ms	15µs	76ms	2.3GiB	50.3MiB	392 997	372 066
CIFS	✓	\\m0.domain.local\IPC$	280 124	2 525	5 773	8ms	1ms	62ms	252.0MiB	79.8MiB	280 124	279 973
CIFS	✓	\\Paris\IPC$	252 146	3 872	24 796	17ms	870µs	72ms	485.9MiB	75.6MiB	252 146	252 641
CIFS	✓	\\m0.domain.local\IPC$	239 369	2 039	4 112	420µs	888µs	40ms	180.8MiB	55.8MiB	239 369	226 433
CIFS	✓	\\So-da\NETLOGON	206 978	2 336	4 512	2ms	520µs	66ms	483.4MiB	63.7MiB	206 978	193 390
CIFS	✓	\\London\NETLOGON	188 210	359	21 786	10ms	176µs	29ms	233.2MiB	23.0MiB	188 210	186 185
CIFS	✓	\\Paris\IPC$	181 833	1 880	9 140	616µs	150µs	52ms	482.8MiB	60.6MiB	181 833	182 926
CIFS	✓	\\Berlin\APPLIS	180 529	554	15 605	1ms	925µs	22ms	215.3MiB	51.1MiB	180 529	179 805
CIFS	✓	\\London\FSECWEB	168 415	1 548	19 445	10ms	278µs	52ms	197.9MiB	29.3MiB	168 415	165 434
CIFS	✓	\\Munich\IPC$	156 938	462	35 484	15ms	3ms	20ms	114.7MiB	9.8MiB	156 938	151 966
CIFS	✓	\\m0.domain.local\SysVol	119 076	1 104	2 484	1ms	9µs	54ms	107.2MiB	48.4MiB	119 076	119 583
CIFS	✓	\\domain.users.local\IPC$	82 138	0	254	1ms	7µs	7µs	49.2MiB	10.3KiB	82 138	82 131
CIFS	✓	\\Berlin\IPC$	52 874	218	7 653	2ms	199µs	7ms	129.2MiB	2.8MiB	52 874	52 766
CIFS	✓	\\Rome\DSI	52 264	10	375	2ms						52 195
CIFS	✓	\\paris.data.local\IPC$	34 559	38	273	1ms						34 507
CIFS	✓	\\Paris\Users	26 615	664	1 452	26ms						26 905
CIFS	✓	\\So-da\IPC$	15 758	454	6 569	17ms						15 686
CIFS	✓	\\So-da\DATASHARE	13 214	321	475	1ms						13 413

Display queries aggregated by **Trees**:

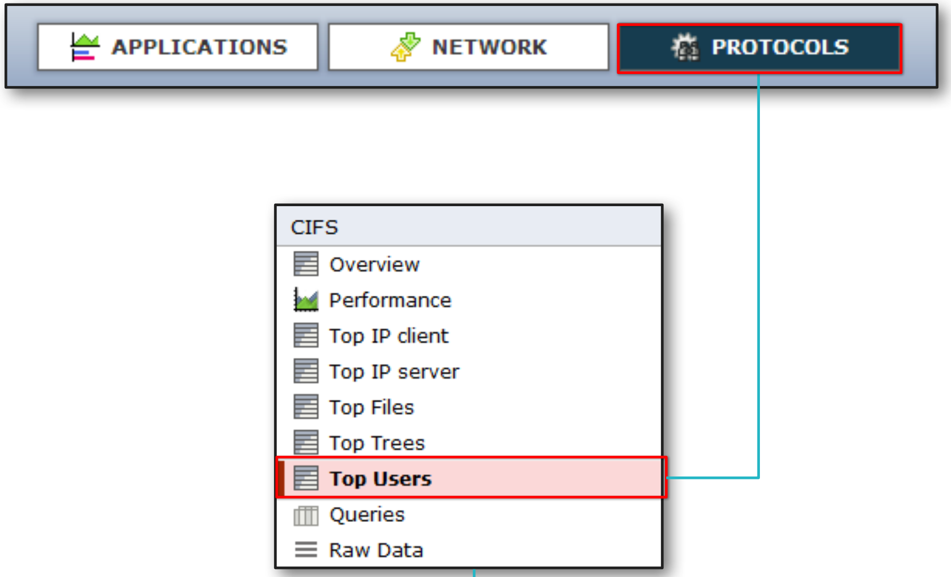
- Tree **Path**
- Number of **Queries**, **Errors** and **Warnings**
- **Performance** Metrics (SRT, DTT)
- **Payloads** and Number of **Packets** (PDUs)

One-click drill down to queries and errors

Difference Between Tree and File

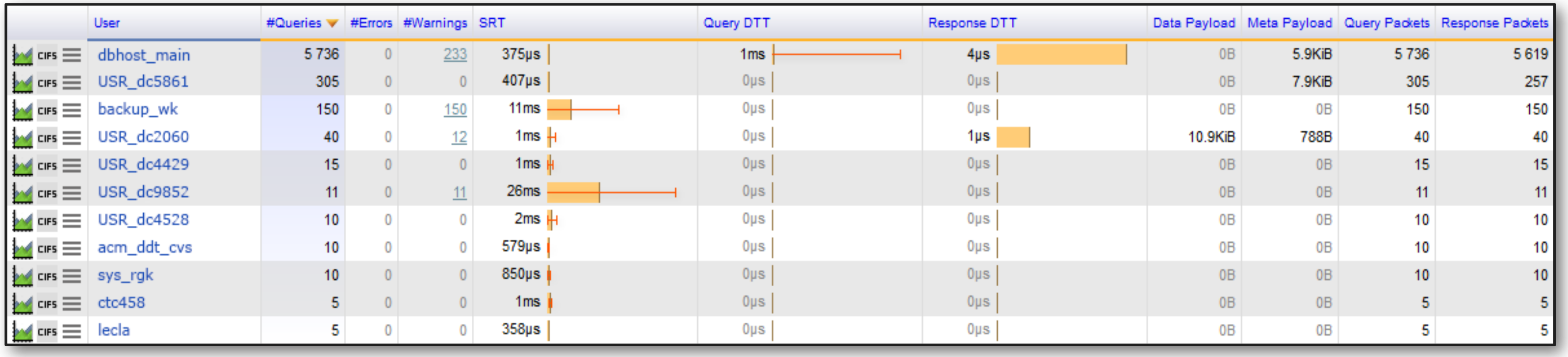


SMB / CIFS Users



SMB / CIFS Most Active Users

SMB / CIFS Top Users



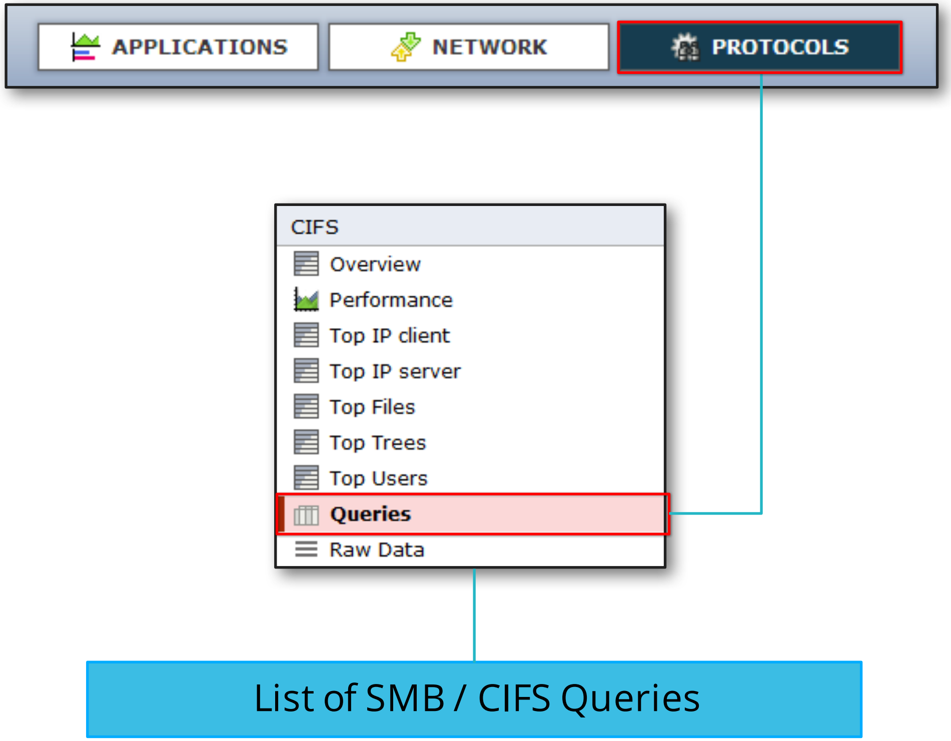
	User	#Queries	#Errors	#Warnings	SRT	Query DTT	Response DTT	Data Payload	Meta Payload	Query Packets	Response Packets
CIFS	dbhost_main	5 736	0	233	375µs	1ms	4µs	0B	5.9KiB	5 736	5 619
CIFS	USR_dc5861	305	0	0	407µs	0µs	0µs	0B	7.9KiB	305	257
CIFS	backup_wk	150	0	150	11ms	0µs	0µs	0B	0B	150	150
CIFS	USR_dc2060	40	0	12	1ms	0µs	1µs	10.9KiB	788B	40	40
CIFS	USR_dc4429	15	0	0	1ms	0µs	0µs	0B	0B	15	15
CIFS	USR_dc9852	11	0	11	26ms	0µs	0µs	0B	0B	11	11
CIFS	USR_dc4528	10	0	0	2ms	0µs	0µs	0B	0B	10	10
CIFS	acm_ddt_cvs	10	0	0	579µs	0µs	0µs	0B	0B	10	10
CIFS	sys_rgk	10	0	0	850µs	0µs	0µs	0B	0B	10	10
CIFS	ctc458	5	0	0	1ms	0µs	0µs	0B	0B	5	5
CIFS	lecla	5	0	0	358µs	0µs	0µs	0B	0B	5	5

Display queries aggregated by **Users**:

- **Username**
- Number of **Queries**, **Errors** and **Warnings**
- **Performance** Metrics (SRT, DTT)
- **Payloads** and Number of **Packets** (PDUs)

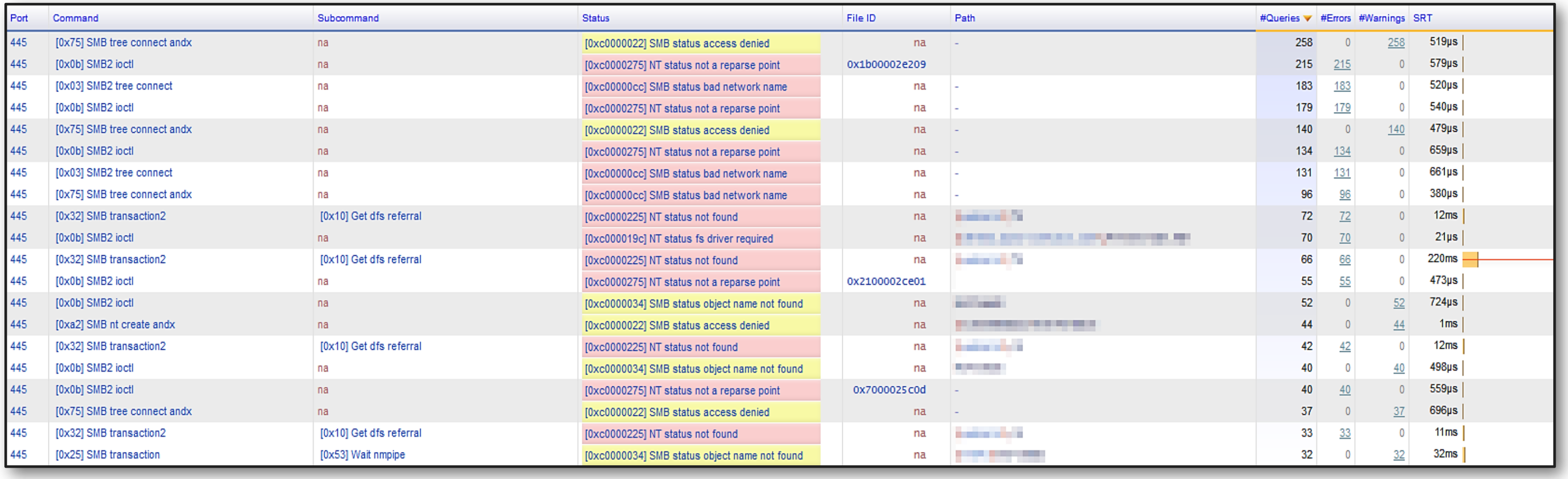
One-click drill down to queries and errors

SMB / CIFS Queries



List of SMB / CIFS Queries

SMB / CIFS Queries



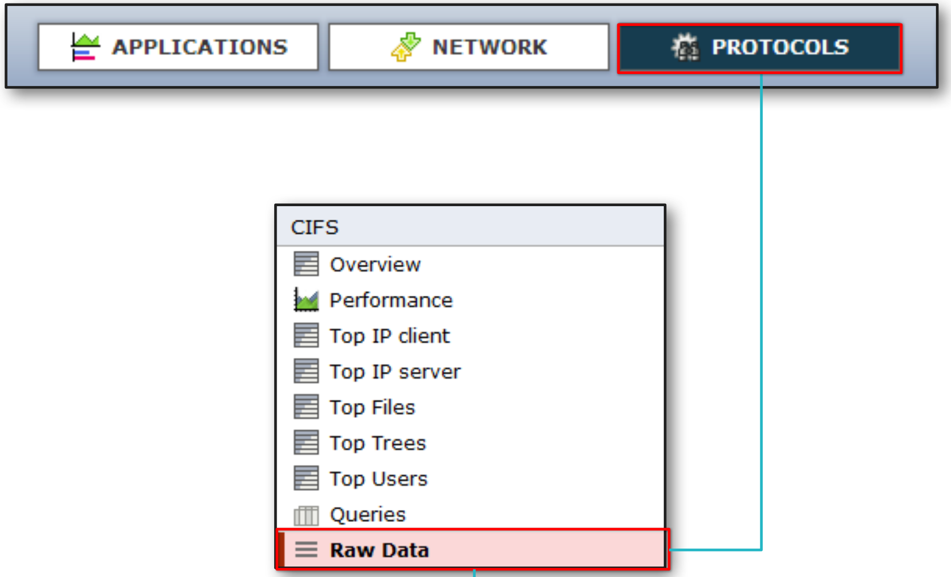
Port	Command	Subcommand	Status	File ID	Path	#Queries	#Errors	#Warnings	SRT
445	[0x75] SMB tree connect andx	na	[0xc0000022] SMB status access denied	na	-	258	0	258	519µs
445	[0x0b] SMB2 ioctl	na	[0xc0000275] NT status not a reparse point	0x1b00002e209		215	215	0	579µs
445	[0x03] SMB2 tree connect	na	[0xc00000cc] SMB status bad network name	na	-	183	183	0	520µs
445	[0x0b] SMB2 ioctl	na	[0xc0000275] NT status not a reparse point	na	-	179	179	0	540µs
445	[0x75] SMB tree connect andx	na	[0xc0000022] SMB status access denied	na	-	140	0	140	479µs
445	[0x0b] SMB2 ioctl	na	[0xc0000275] NT status not a reparse point	na	-	134	134	0	659µs
445	[0x03] SMB2 tree connect	na	[0xc00000cc] SMB status bad network name	na	-	131	131	0	661µs
445	[0x75] SMB tree connect andx	na	[0xc00000cc] SMB status bad network name	na	-	96	96	0	380µs
445	[0x32] SMB transaction2	[0x10] Get dfs referral	[0xc0000225] NT status not found	na	[redacted]	72	72	0	12ms
445	[0x0b] SMB2 ioctl	na	[0xc000019c] NT status fs driver required	na	[redacted]	70	70	0	21µs
445	[0x32] SMB transaction2	[0x10] Get dfs referral	[0xc0000225] NT status not found	na	[redacted]	66	66	0	220ms
445	[0x0b] SMB2 ioctl	na	[0xc0000275] NT status not a reparse point	0x2100002ce01		55	55	0	473µs
445	[0x0b] SMB2 ioctl	na	[0xc0000034] SMB status object name not found	na	[redacted]	52	0	52	724µs
445	[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	[redacted]	44	0	44	1ms
445	[0x32] SMB transaction2	[0x10] Get dfs referral	[0xc0000225] NT status not found	na	[redacted]	42	42	0	12ms
445	[0x0b] SMB2 ioctl	na	[0xc0000034] SMB status object name not found	na	[redacted]	40	0	40	498µs
445	[0x0b] SMB2 ioctl	na	[0xc0000275] NT status not a reparse point	0x7000025c0d	-	40	40	0	559µs
445	[0x75] SMB tree connect andx	na	[0xc0000022] SMB status access denied	na	-	37	0	37	696µs
445	[0x32] SMB transaction2	[0x10] Get dfs referral	[0xc0000225] NT status not found	na	[redacted]	33	33	0	11ms
445	[0x25] SMB transaction	[0x53] Wait nmpipe	[0xc0000034] SMB status object name not found	na	[redacted]	32	0	32	32ms

Available SMB / CIFS Data

- **Command**, **Subcommand** and **Status**
- File **ID** and **Path**
- Number of **Queries**, **Errors** & **Warnings**
- **Performance** Metrics (SRT, DTT)
- **Username**

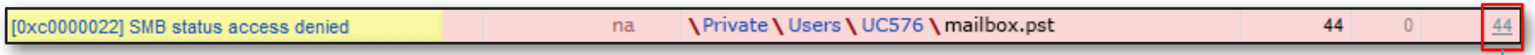
- **Domain** name
- Tree **ID** and **Tree** name
- **Data** Payload: Reads, Writes
- **Metadata** Payload: Reads, Writes
- Number of **Packets** (PDUs)

SMB / CIFS Raw Data



Details of all SMB / CIFS Transactions

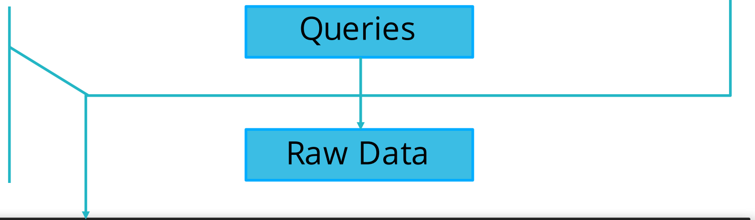
SMB / CIFS Raw Data: True Root Cause Analysis

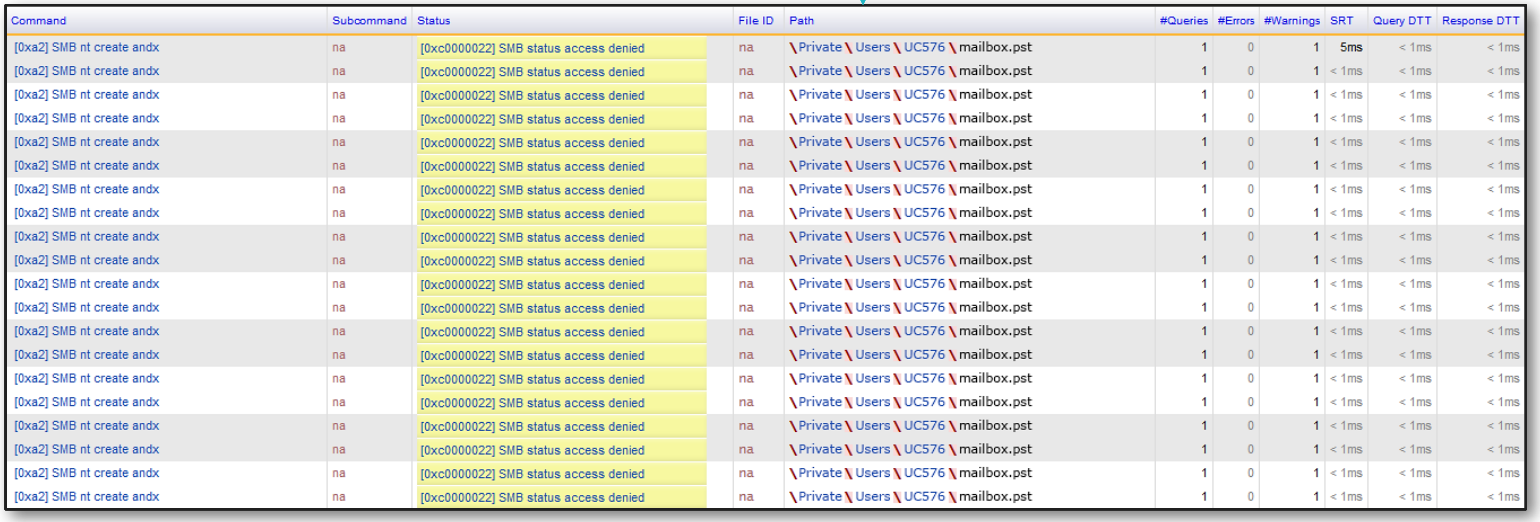


[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	44	0	44

SMB / CIFS transactions **without** any **grouping**

- Useful for advanced troubleshooting
- Application behavior auditing





Command	Subcommand	Status	File ID	Path	#Queries	#Errors	#Warnings	SRT	Query DTT	Response DTT
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	5ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms
[0xa2] SMB nt create andx	na	[0xc0000022] SMB status access denied	na	\Private\Users\UC576\mailbox.pst	1	0	1	< 1ms	< 1ms	< 1ms

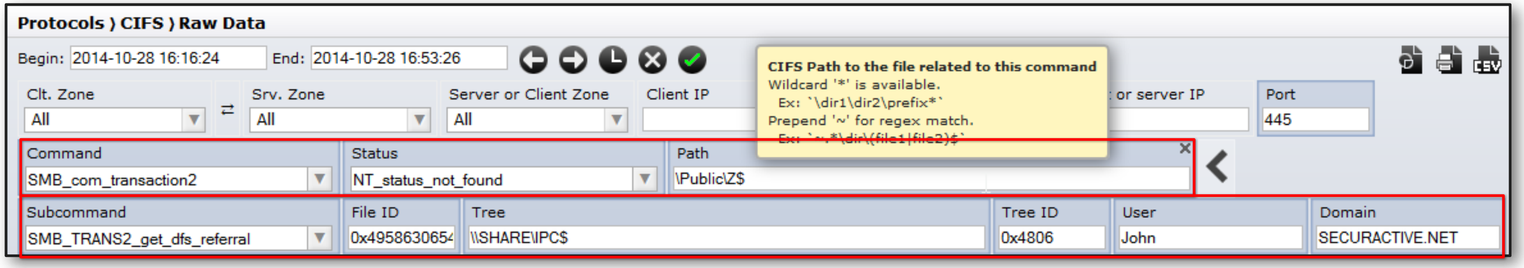
SMB / CIFS Dedicated Filters

Dedicated SMB / CIFS filters:

Refine search for specific issues

Search **results** by:

- **Port** number
- **Command** type
- **Status** name
- **Path** name and File **ID**
- **Subcommand** type
- **Tree** name and Tree **ID**
- **User** and **Domain**



Protocols) CIFS) Raw Data

Begin: 2014-10-28 16:16:24 End: 2014-10-28 16:53:26

CIFS Path to the file related to this command
Wildcard '*' is available.
Ex: `\dir1\dir2\prefix*`
Prepend '~' for regex match.
Ex: `~.*\dir\(file1|file2)$`

Clt. Zone: All

Srv. Zone: All

Server or Client Zone: All

Client IP:

or server IP:

Port: 445

Command: SMB_com_transaction2

Status: NT_status_not_found

Path: \Public\Z$

Subcommand: SMB_TRANS2_get_dfs_referral

File ID: 0x4958630654

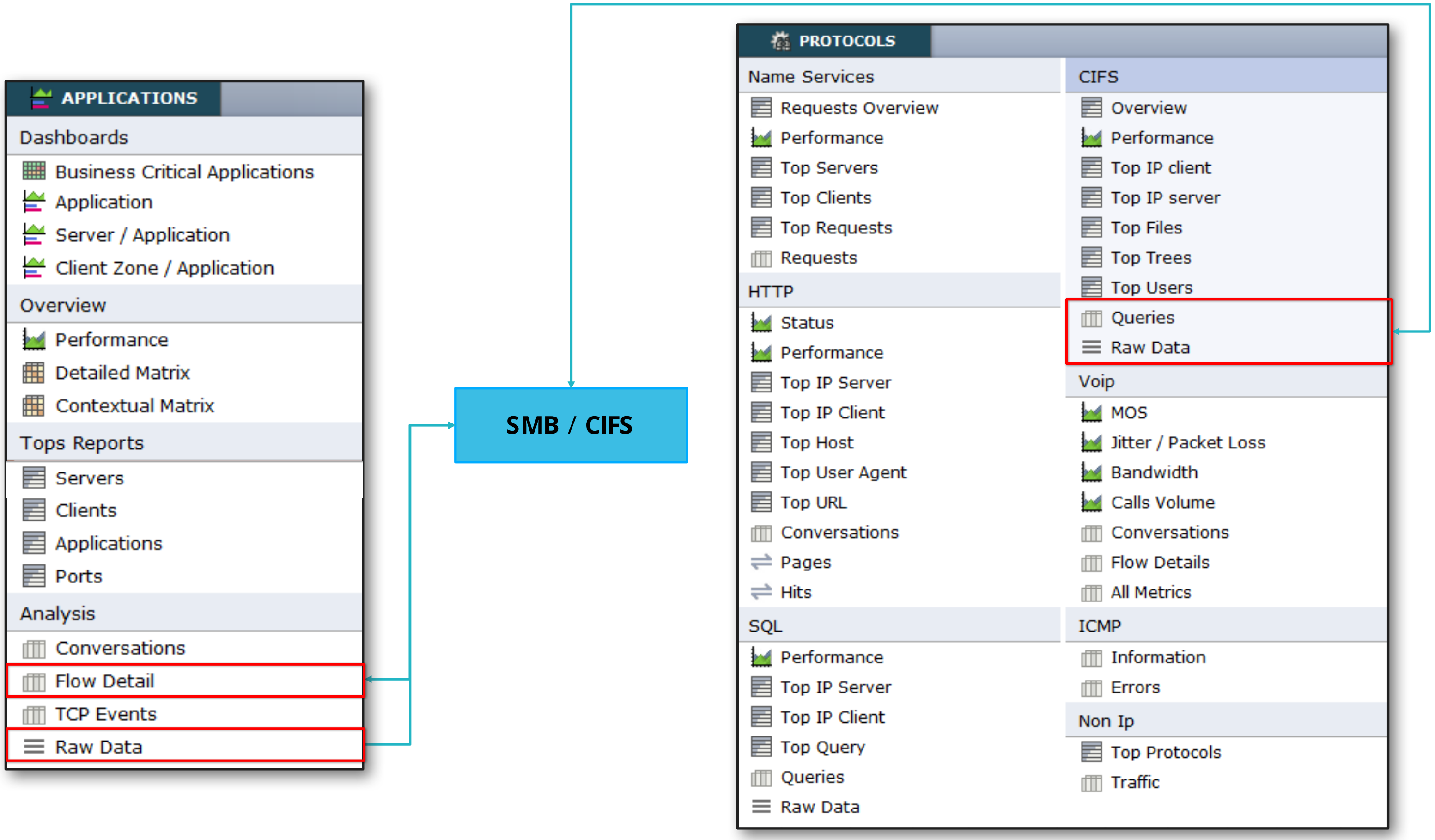
Tree: \\SHARE\IPC$

Tree ID: 0x4806

User: John

Domain: SECURACTIVE.NET

Correlation Between Network Issues & SMB / CIFS Transactions



Content

performance vision

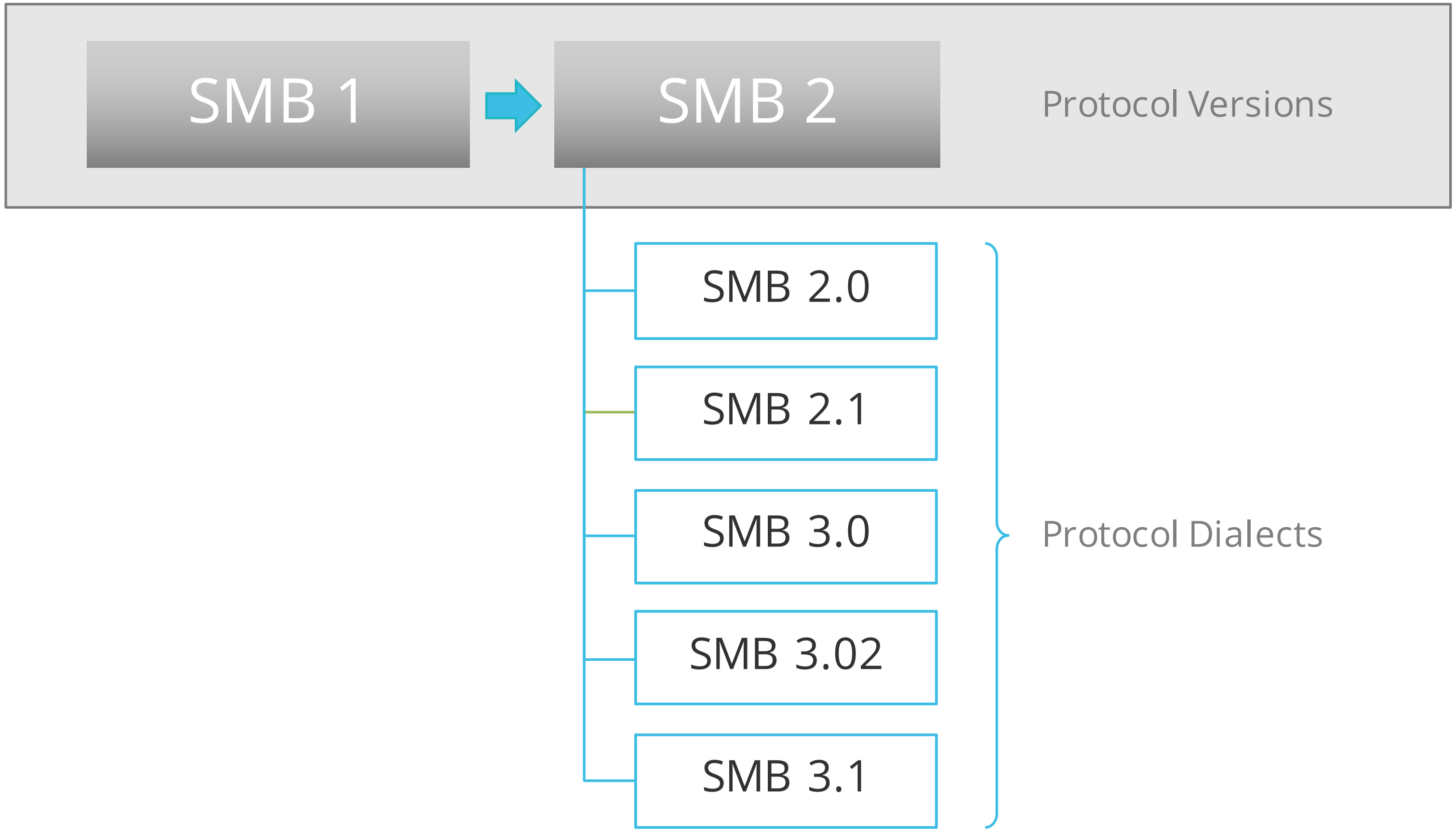
1. Product Features

2. SMB Overview & Use Cases

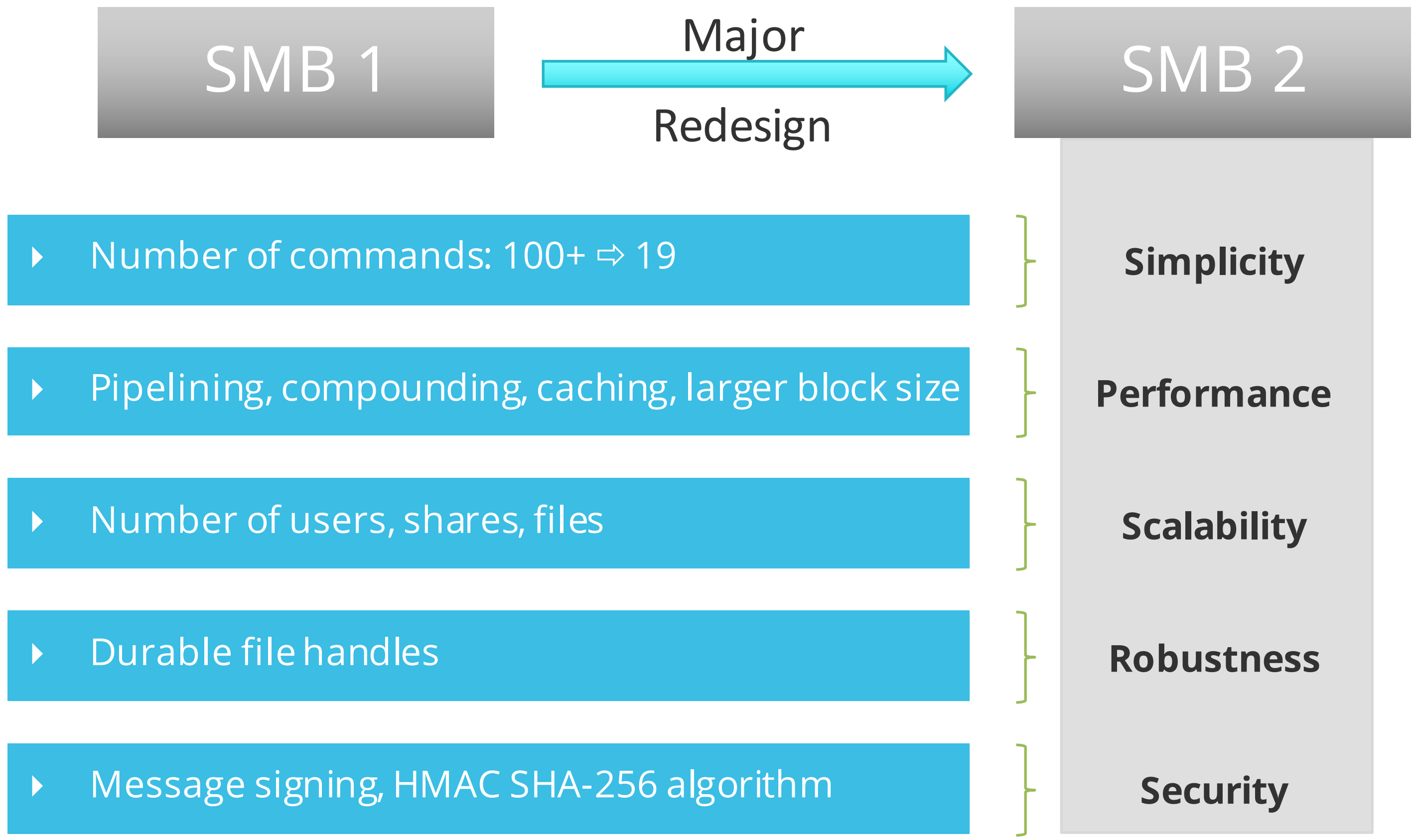
- 1. Connect and Browse Files
- 2. Login Authorization Failure
- 3. Put a File on a Remote Folder
- 4. Not Authorized to Delete a Remote File

3. Documentation + Q&A

SMB Versions & Dialects



SMB 2: Major Improvements over SMB 1



SMB 1

Major Redesign

SMB 2

- Number of commands: 100+ ⇨ 19
- Pipelining, compounding, caching, larger block size
- Number of users, shares, files
- Durable file handles
- Message signing, HMAC SHA-256 algorithm

Simplicity

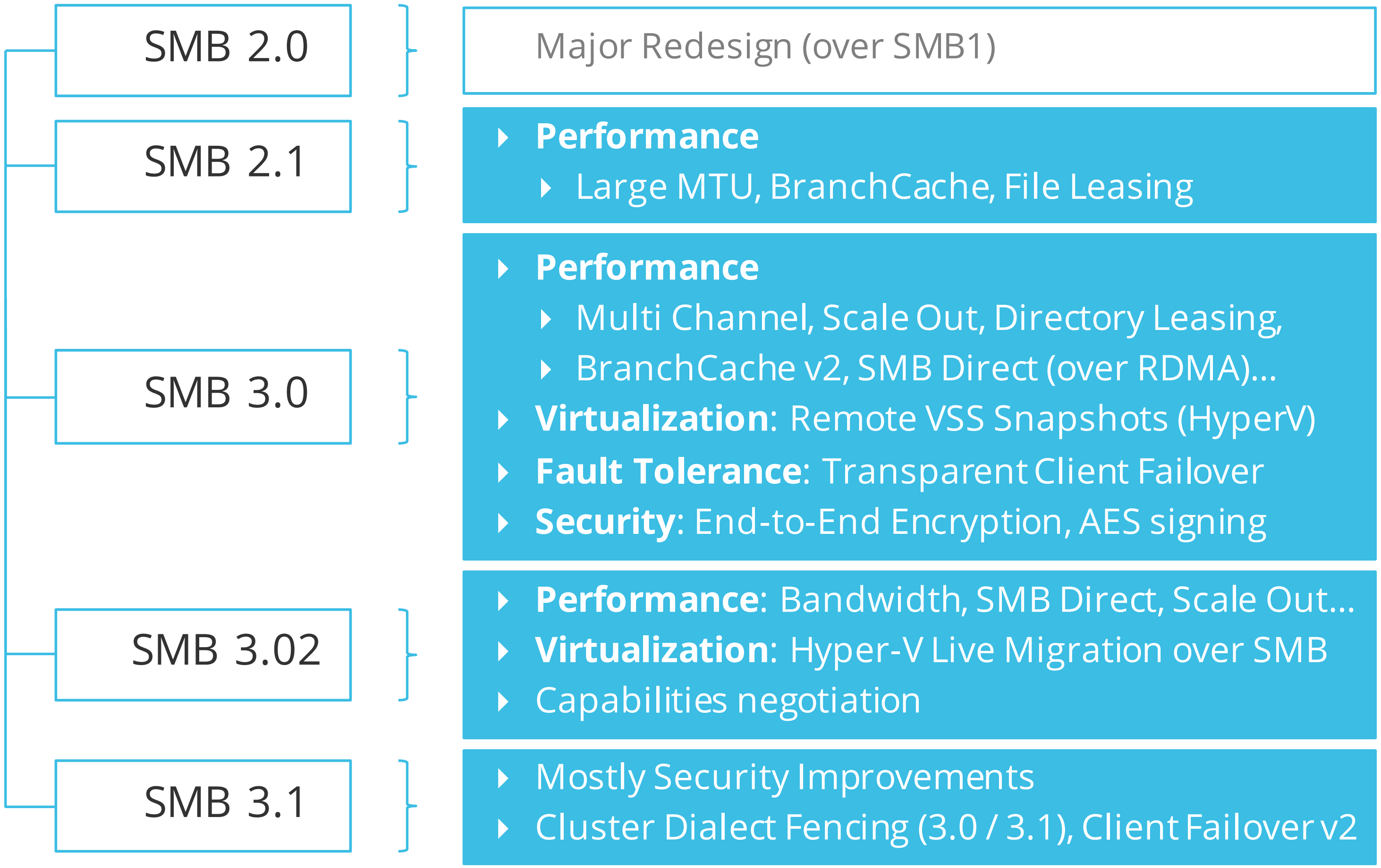
Performance

Scalability

Robustness

Security

SMB Evolution



SMB 2.0

Major Redesign (over SMB1)

SMB 2.1

- **Performance**
  - Large MTU, BranchCache, File Leasing

SMB 3.0

- **Performance**
  - Multi Channel, Scale Out, Directory Leasing,
  - BranchCache v2, SMB Direct (over RDMA)…
- **Virtualization**: Remote VSS Snapshots (HyperV)
- **Fault Tolerance**: Transparent Client Failover
- **Security**: End-to-End Encryption, AES signing

SMB 3.02

- **Performance**: Bandwidth, SMB Direct, Scale Out…
- **Virtualization**: Hyper-V Live Migration over SMB
- Capabilities negotiation

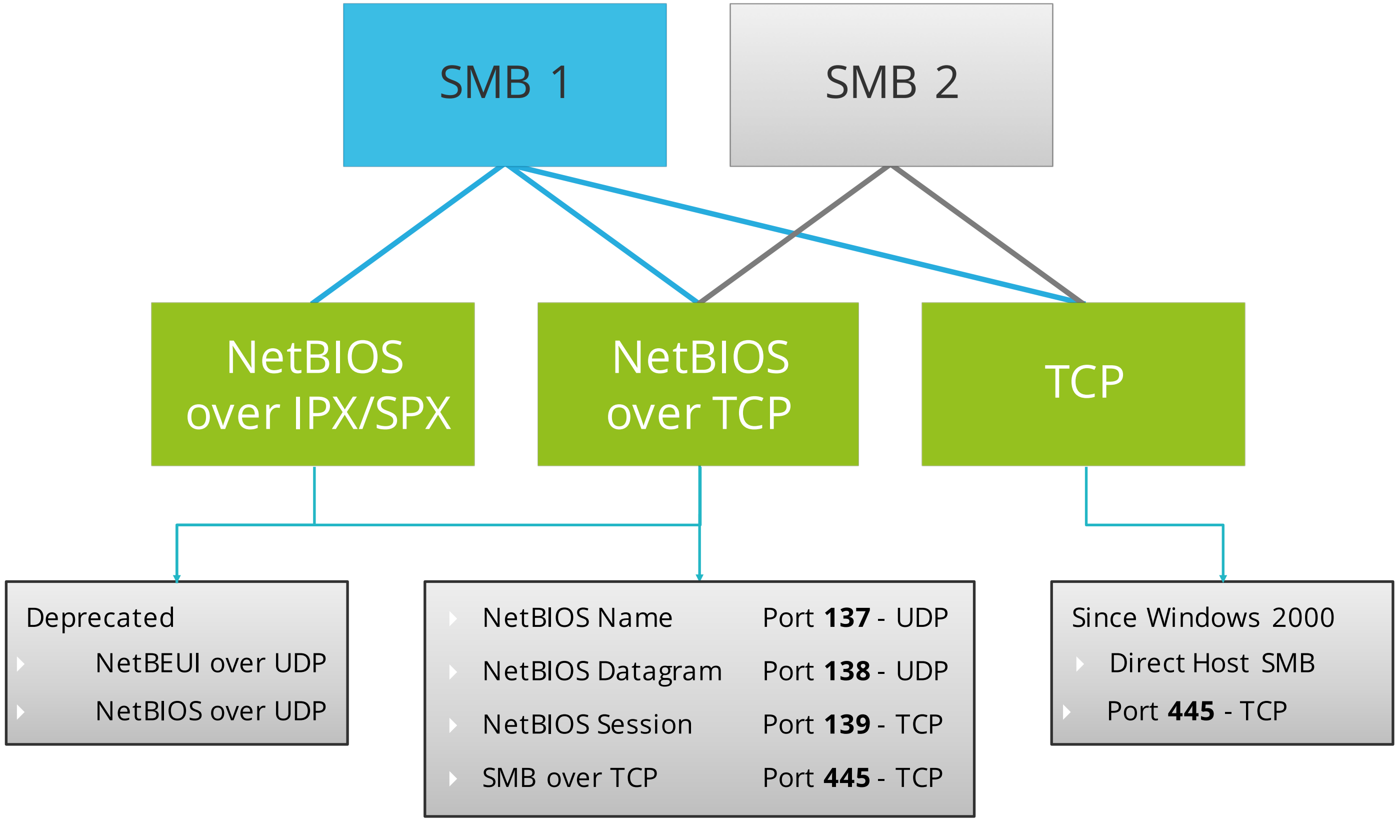
SMB 3.1

- Mostly Security Improvements
- Cluster Dialect Fencing (3.0 / 3.1), Client Failover v2

Supported SMB Versions by Major Implementations

SMB 1	Windows XP	Windows 2000, Server 2003	Samba
SMB 2.0	Windows Vista	Windows Server 2008	Samba 3.6
SMB 2.1	Windows 7	Windows Server 2008 R2	Samba 4.0
SMB 3.0	Windows 8	Windows Server 2012	Samba 4.1
SMB 3.02	Windows 8.1	Windows Server 2012 R2	Samba 4.2 ?
SMB 3.1	Windows 10	Windows Server 10	Samba ?

Default SMB Ports Assignation



SMB 1

SMB 2

NetBIOS over IPX/SPX

NetBIOS over TCP

TCP

Deprecated

- NetBEUI over UDP
- NetBIOS over UDP

NetBIOS Name	Port **137** - UDP
NetBIOS Datagram	Port **138** - UDP
NetBIOS Session	Port **139** - TCP
SMB over TCP	Port **445** - TCP

Since Windows 2000

- Direct Host SMB
- Port **445** - TCP

Auto-Detection of SMB Ports

Performance Vision **automatically** detects **SMB** traffic through to Port Independent Protocol Identification (PiPi)

Nothing to configure!

SMB traffic is detected independently of the port used: 139, 445 or other non standard port (TCP)

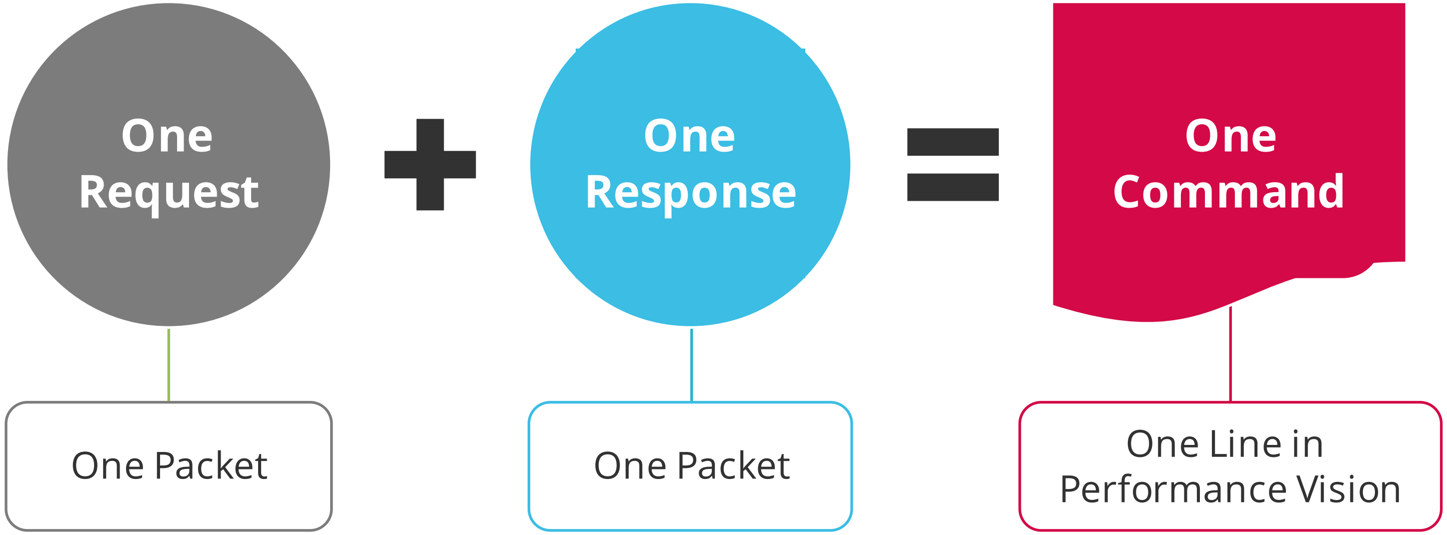
SMB Dialect Negotiation

	SMB 3.1	SMB 3.02	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
SMB 3.1	3.1	3.02	3.0	2.1	2.0	1.0
SMB 3.02	3.02	3.02	3.0	2.1	2.0	1.0
SMB 3.0	3.0	3.0	3.0	2.1	2.0	1.0
SMB 2.1	2.1	2.1	2.1	2.1	2.0	1.0
SMB 2.0	2.0	2.0	2.0	2.0	2.0	1.0
SMB 1.0	1.0	1.0	1.0	1.0	1.0	1.0

SMB Dialect Negotiation on Windows Systems

	Win 10 Server 10	Win 8.1 Server 2012 R2	Win 8 Server 2012	Win 7 Server 2008 R2	Win Vista Server 2008	Previous versions
Win 10 Server 10	3.1	3.02	3.0	2.1	2.0	1.0
Win 8.1 Server 2012 R2	3.02	3.02	3.0	2.1	2.0	1.0
Win 8 Server 2012	3.0	3.0	3.0	2.1	2.0	1.0
Win 7 Server 2008 R2	2.1	2.1	2.1	2.1	2.0	1.0
Win Vista Server 2008	2.0	2.0	2.0	2.0	2.0	1.0
Previous versions	1.0	1.0	1.0	1.0	1.0	1.0

Typical SMB Dialog



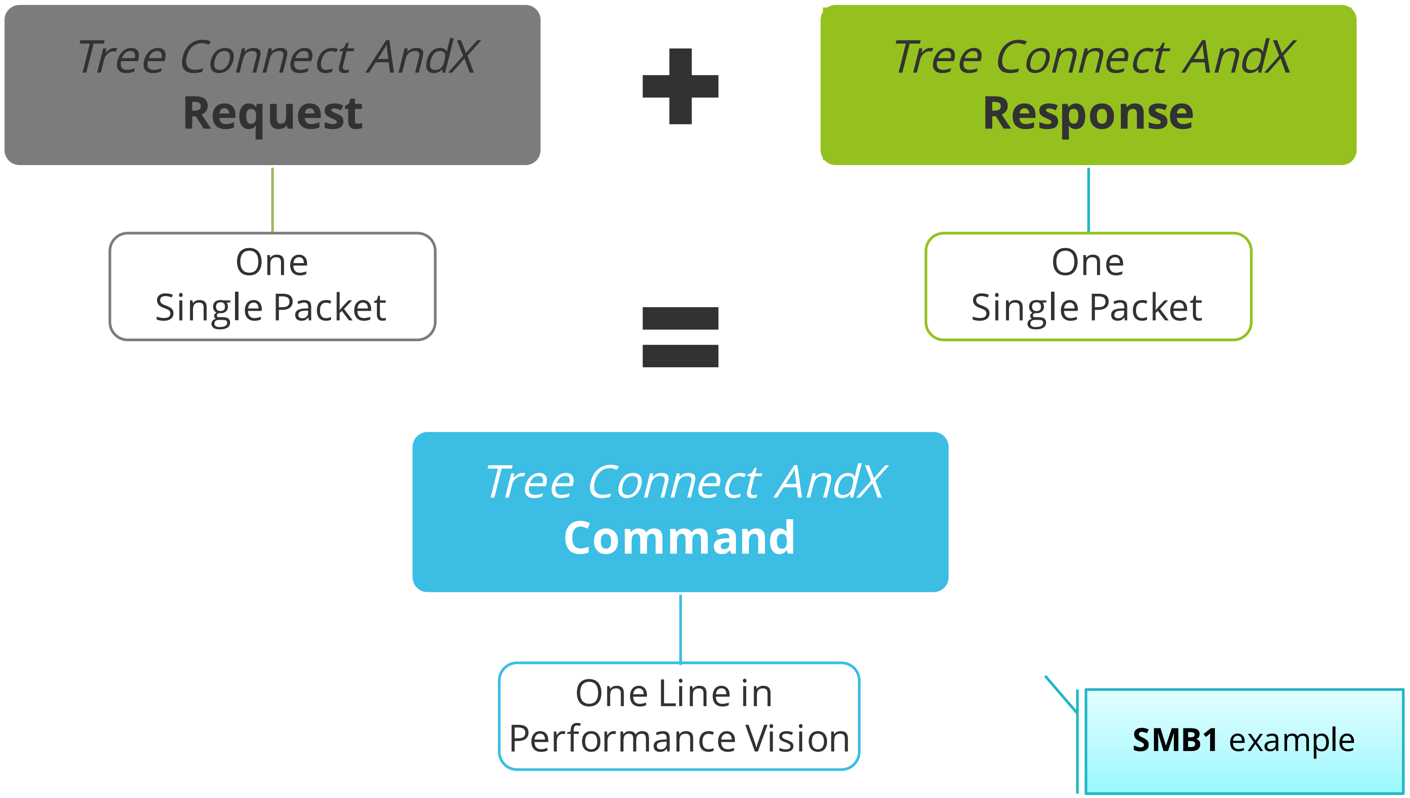
One Request + One Response = One Command

One Packet

One Packet

One Line in Performance Vision

Typical SMB1 Dialog Example


Tree Connect AndX **Request**

One Single Packet

+

Tree Connect AndX **Response**

One Single Packet

=

Tree Connect AndX **Command**

One Line in Performance Vision

SMB1 example

Basic Use Case: Connect and Browse Files

SMB1 - Use Case: Connect to Share Directory and Browse Fi

Use Case

```
smbclient //fileserver.securactive.lan/public/test -U tbouchette -c "ls" password -m NT1
```

SMB2 - Use Case: Connect to Share Directory and Browse Fi

Use Case

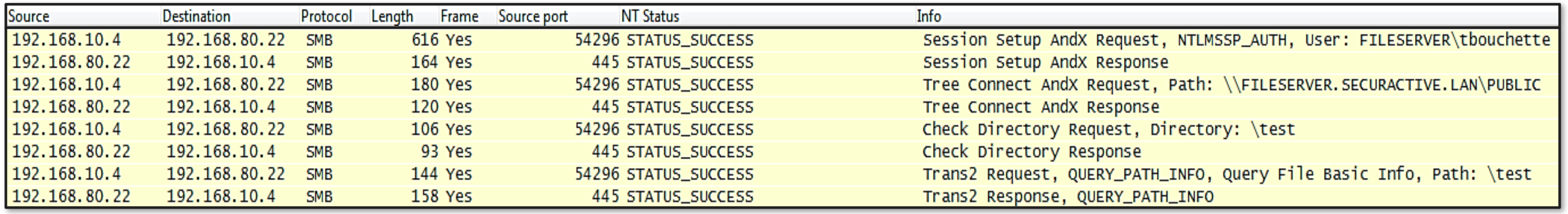
```
smbclient //nas.securactive.lan/public/test -U admin -c "ls" password -mSMB2
```

Basic Use Case - SMB1 Example With Wireshark

SMB1 **Commands**:

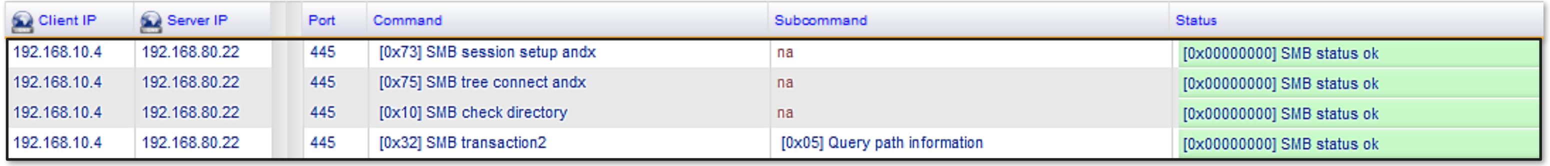
- Session Setup AndX
- Tree Connect AndX
- Check Directory
- Transaction2 (Query_Path_Info)

- Eight Packets
  - 4 Requests
  - 4 Responses

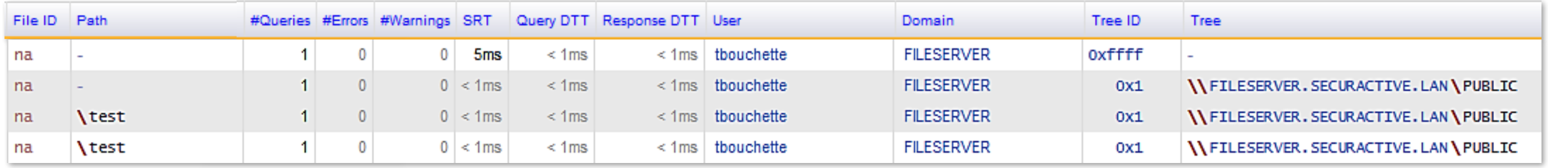


Source	Destination	Protocol	Length	Frame	Source port	NT Status	Info
192.168.10.4	192.168.80.22	SMB	616	Yes	54296	STATUS_SUCCESS	Session Setup AndX Request, NTLMSSP_AUTH, User: FILESERVER\tbouchette
192.168.80.22	192.168.10.4	SMB	164	Yes	445	STATUS_SUCCESS	Session Setup AndX Response
192.168.10.4	192.168.80.22	SMB	180	Yes	54296	STATUS_SUCCESS	Tree Connect AndX Request, Path: \\FILESERVER.SECURACTIVE.LAN\PUBLIC
192.168.80.22	192.168.10.4	SMB	120	Yes	445	STATUS_SUCCESS	Tree Connect AndX Response
192.168.10.4	192.168.80.22	SMB	106	Yes	54296	STATUS_SUCCESS	Check Directory Request, Directory: \test
192.168.80.22	192.168.10.4	SMB	93	Yes	445	STATUS_SUCCESS	Check Directory Response
192.168.10.4	192.168.80.22	SMB	144	Yes	54296	STATUS_SUCCESS	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \test
192.168.80.22	192.168.10.4	SMB	158	Yes	445	STATUS_SUCCESS	Trans2 Response, QUERY_PATH_INFO

Basic Use Case - SMB1
Example With PerformanceVision



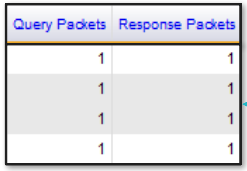
Client IP	Server IP	Port	Command	Subcommand	Status
192.168.10.4	192.168.80.22	445	[0x73] SMB session setup andx	na	[0x00000000] SMB status ok
192.168.10.4	192.168.80.22	445	[0x75] SMB tree connect andx	na	[0x00000000] SMB status ok
192.168.10.4	192.168.80.22	445	[0x10] SMB check directory	na	[0x00000000] SMB status ok
192.168.10.4	192.168.80.22	445	[0x32] SMB transaction2	[0x05] Query path information	[0x00000000] SMB status ok



File ID	Path	#Queries	#Errors	#Warnings	SRT	Query DTT	Response DTT	User	Domain	Tree ID	Tree
na	-	1	0	0	5ms	< 1ms	< 1ms	tbouchette	FILESERVER	0xffff	-
na	-	1	0	0	< 1ms	< 1ms	< 1ms	tbouchette	FILESERVER	0x1	\\FILESERVER.SECURACTIVE.LAN\PUBLIC
na	\test	1	0	0	< 1ms	< 1ms	< 1ms	tbouchette	FILESERVER	0x1	\\FILESERVER.SECURACTIVE.LAN\PUBLIC
na	\test	1	0	0	< 1ms	< 1ms	< 1ms	tbouchette	FILESERVER	0x1	\\FILESERVER.SECURACTIVE.LAN\PUBLIC

SMB1 **Commands**:

- Session Setup AndX
- Tree Connect AndX
- Check Directory
- Transaction2 (Query_Path_Info)



Query Packets	Response Packets
1	1
1	1
1	1
1	1

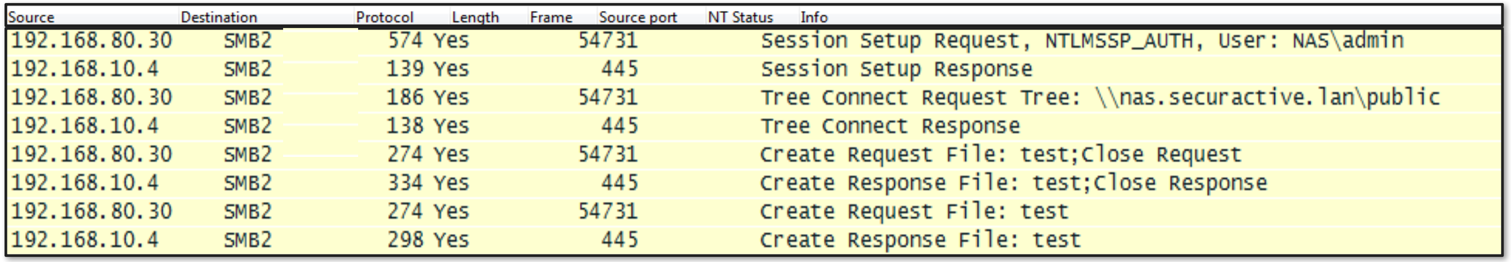
- Eight Packets
  - 4 Requests
  - 4 Responses

Basic Use Case - SMB2 Example With Wireshark

SMB2 **Commands**:

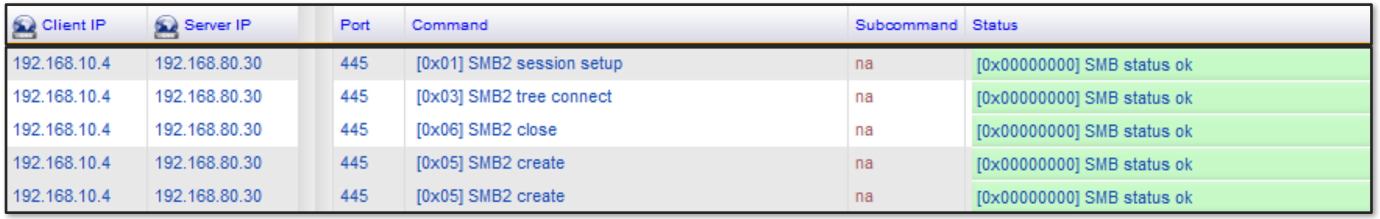
- Session Setup
- Tree Connect
- Create Request + Close Request
- Create Request

- Eight Packets
  - 5 Requests
  - 5 Responses

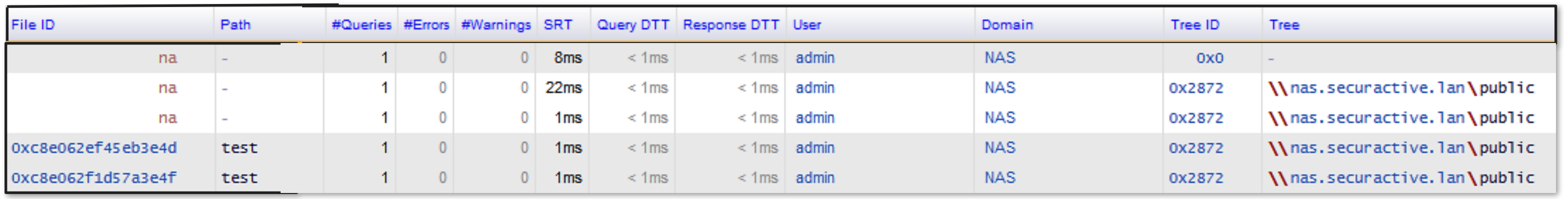


```
Source              Destination         Protocol   Length   Frame   Source port   NT Status   Info
192.168.80.30       SMB2                574 Yes             54731           Session Setup Request, NTLMSSP_AUTH, User: NAS\admin
192.168.10.4        SMB2                139 Yes               445           Session Setup Response
192.168.80.30       SMB2                186 Yes             54731           Tree Connect Request Tree: \\nas.securactive.lan\public
192.168.10.4        SMB2                138 Yes               445           Tree Connect Response
192.168.80.30       SMB2                274 Yes             54731           Create Request File: test;Close Request
192.168.10.4        SMB2                334 Yes               445           Create Response File: test;Close Response
192.168.80.30       SMB2                274 Yes             54731           Create Request File: test
192.168.10.4        SMB2                298 Yes               445           Create Response File: test
```

Basic Use Case - SMB2 Example With Performance Vision



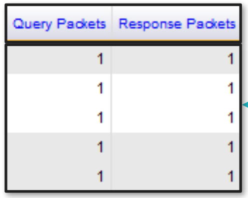
Client IP	Server IP	Port	Command	Subcommand	Status
192.168.10.4	192.168.80.30	445	[0x01] SMB2 session setup	na	[0x00000000] SMB status ok
192.168.10.4	192.168.80.30	445	[0x03] SMB2 tree connect	na	[0x00000000] SMB status ok
192.168.10.4	192.168.80.30	445	[0x06] SMB2 close	na	[0x00000000] SMB status ok
192.168.10.4	192.168.80.30	445	[0x05] SMB2 create	na	[0x00000000] SMB status ok
192.168.10.4	192.168.80.30	445	[0x05] SMB2 create	na	[0x00000000] SMB status ok



File ID	Path	#Queries	#Errors	#Warnings	SRT	Query DTT	Response DTT	User	Domain	Tree ID	Tree
na	-	1	0	0	8ms	< 1ms	< 1ms	admin	NAS	0x0	-
na	-	1	0	0	22ms	< 1ms	< 1ms	admin	NAS	0x2872	\\nas.securactive.lan\public
na	-	1	0	0	1ms	< 1ms	< 1ms	admin	NAS	0x2872	\\nas.securactive.lan\public
0xc8e062ef45eb3e4d	test	1	0	0	1ms	< 1ms	< 1ms	admin	NAS	0x2872	\\nas.securactive.lan\public
0xc8e062f1d57a3e4f	test	1	0	0	1ms	< 1ms	< 1ms	admin	NAS	0x2872	\\nas.securactive.lan\public

SMB2 **Commands**:

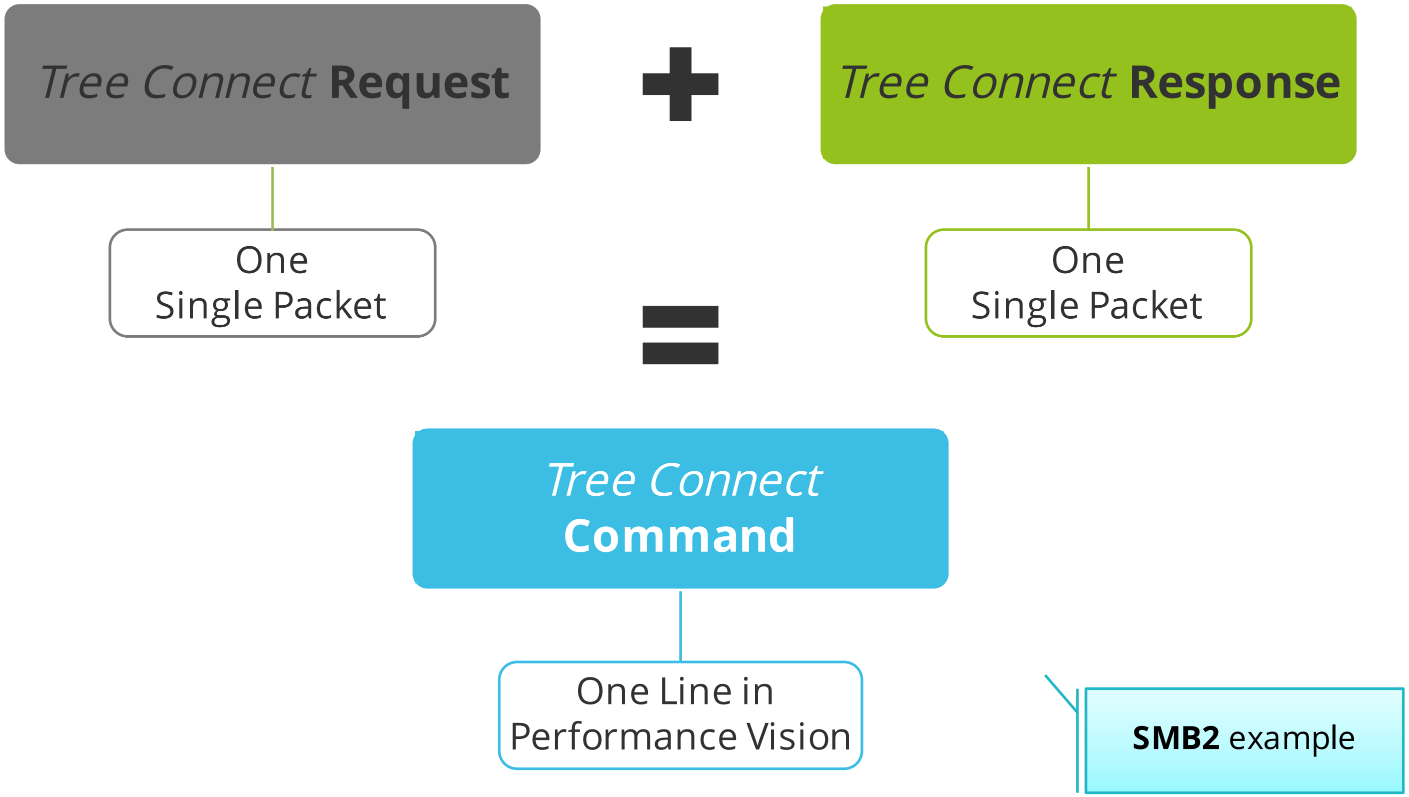
- Session Setup
- Tree Connect
- Create Request + Close Request
- Create Request



Query Packets	Response Packets
1	1
1	1
1	1
1	1
1	1

- Query Packets
  - 5 Requests
  - 5 Responses

Typical SMB2 Dialog Example



Tree Connect **Request** + *Tree Connect* **Response**

One Single Packet

One Single Packet

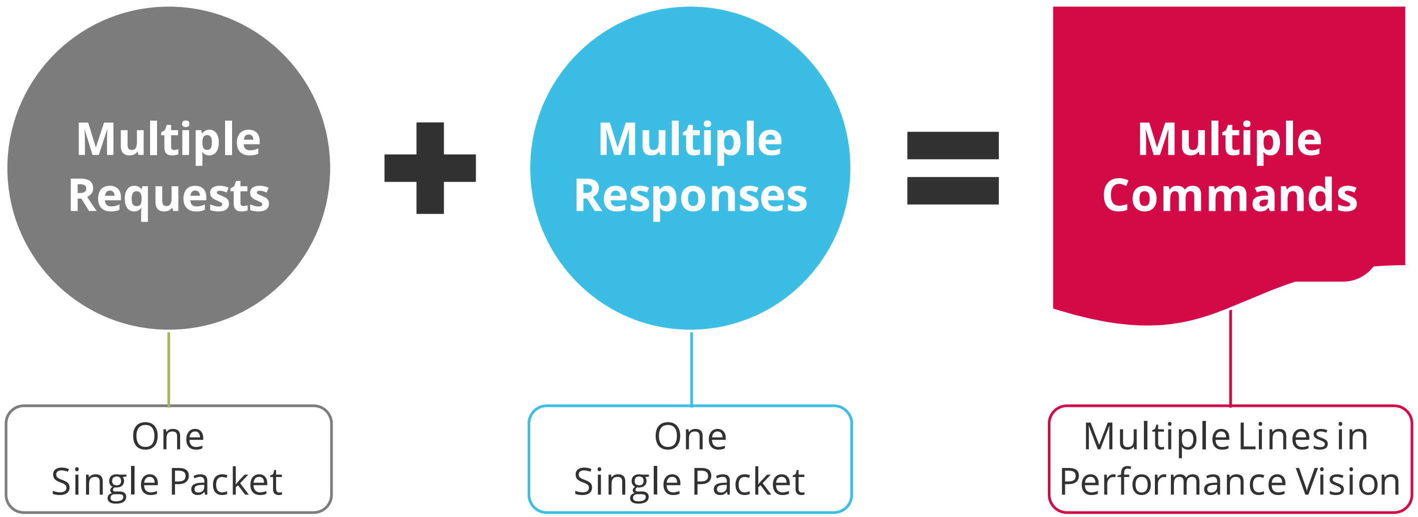
=

Tree Connect **Command**

One Line in Performance Vision

SMB2 example

Compounded SMB2 Requests



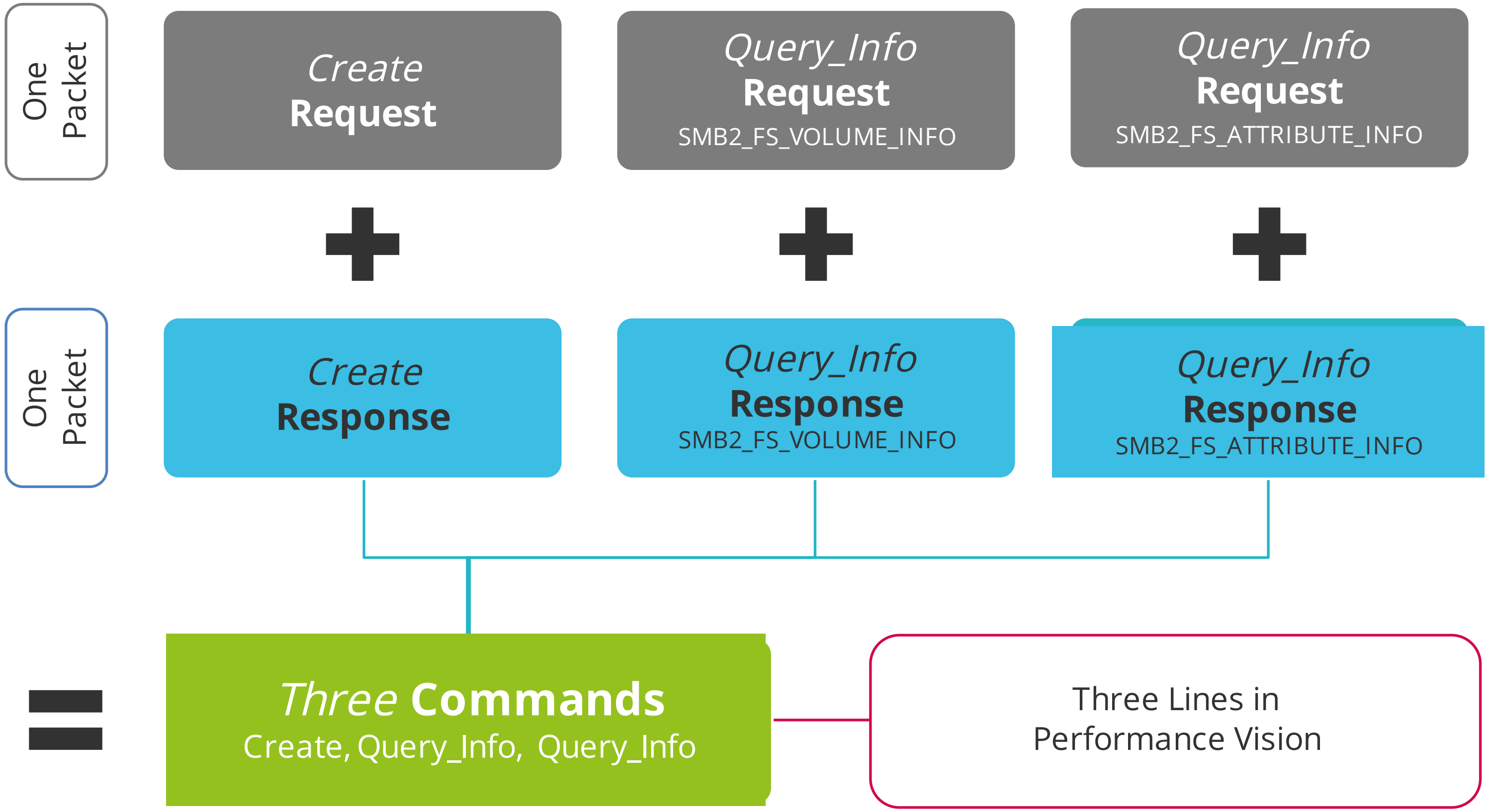
Multiple Requests + Multiple Responses = Multiple Commands

One Single Packet

One Single Packet

Multiple Lines in Performance Vision

Compounded SMB2 Requests Example



One Packet

Create **Request**

Query_Info **Request** SMB2_FS_VOLUME_INFO

Query_Info **Request** SMB2_FS_ATTRIBUTE_INFO

One Packet

Create **Response**

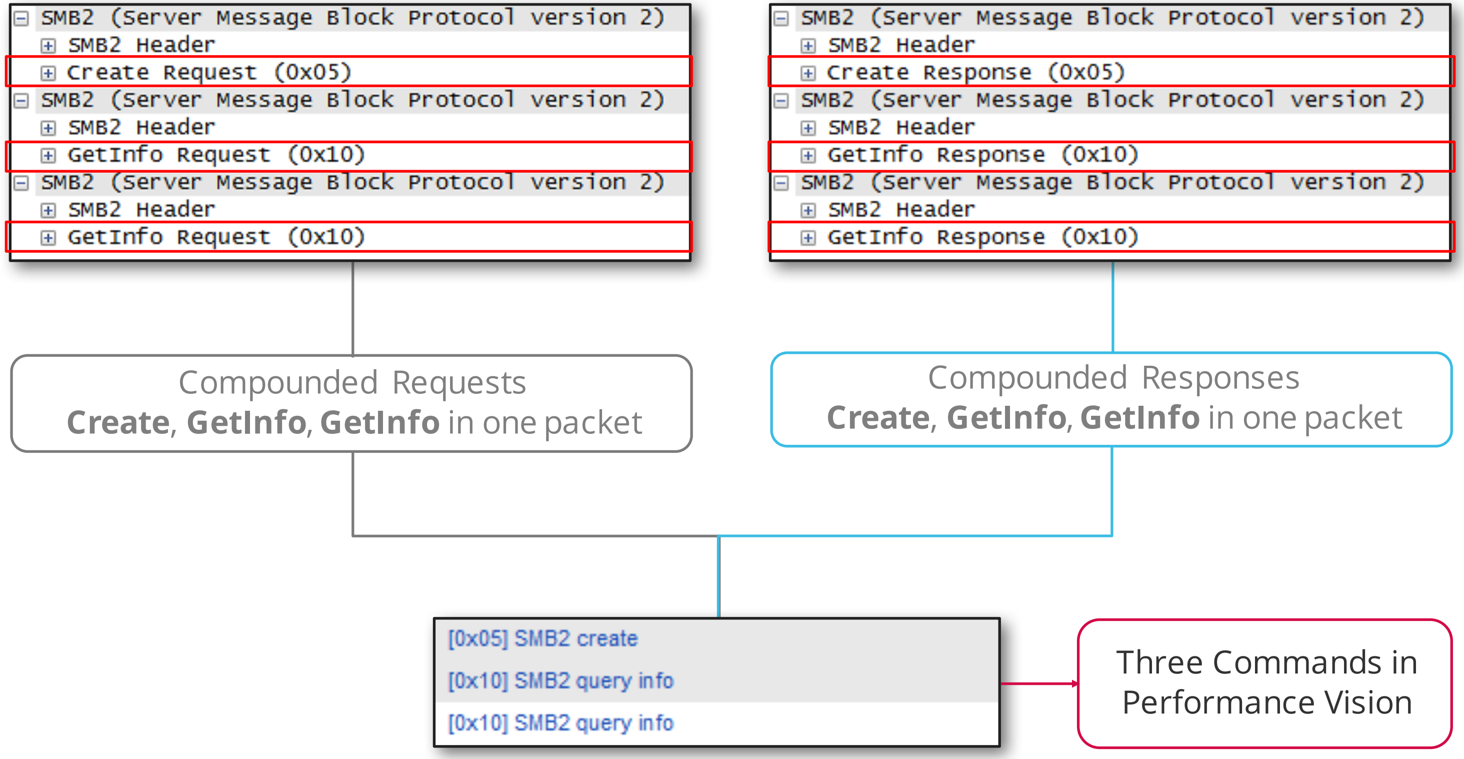
Query_Info **Response** SMB2_FS_VOLUME_INFO

Query_Info **Response** SMB2_FS_ATTRIBUTE_INFO

Three **Commands**
Create, Query_Info, Query_Info

Three Lines in
Performance Vision

Compounded SMB2 Requests Example



```
⊟ SMB2 (Server Message Block Protocol version 2)
  ⊞ SMB2 Header
  ⊞ Create Request (0x05)
⊟ SMB2 (Server Message Block Protocol version 2)
  ⊞ SMB2 Header
  ⊞ GetInfo Request (0x10)
⊟ SMB2 (Server Message Block Protocol version 2)
  ⊞ SMB2 Header
  ⊞ GetInfo Request (0x10)
```

```
⊟ SMB2 (Server Message Block Protocol version 2)
  ⊞ SMB2 Header
  ⊞ Create Response (0x05)
⊟ SMB2 (Server Message Block Protocol version 2)
  ⊞ SMB2 Header
  ⊞ GetInfo Response (0x10)
⊟ SMB2 (Server Message Block Protocol version 2)
  ⊞ SMB2 Header
  ⊞ GetInfo Response (0x10)
```

Compounded Requests
Create, **GetInfo**, **GetInfo** in one packet

Compounded Responses
Create, **GetInfo**, **GetInfo** in one packet

```
[0x05] SMB2 create
[0x10] SMB2 query info
[0x10] SMB2 query info
```

Three Commands in Performance Vision

List of The 19 SMB2 Commands

Protocol Negotiation, User Authentication and Share Access

- □ NEGOTIATE
- □ SESSION_SETUP
- □ LOGOFF
- □ TREE_CONNECT
- □ TREE_DISCONNECT

File, Directory and Volume Access

- □ CANCEL
- □ CHANGE_NOTIFY
- □ CLOSE
- □ CREATE
- □ FLUSH
- □ IOCTL
- □ LOCK
- □ QUERY_DIRECTORY
- □ QUERY_INFO
- □ READ
- □ SET_INFO
- □ WRITE

Other

- □ ECHO
- □ OPLOCK_BREAK

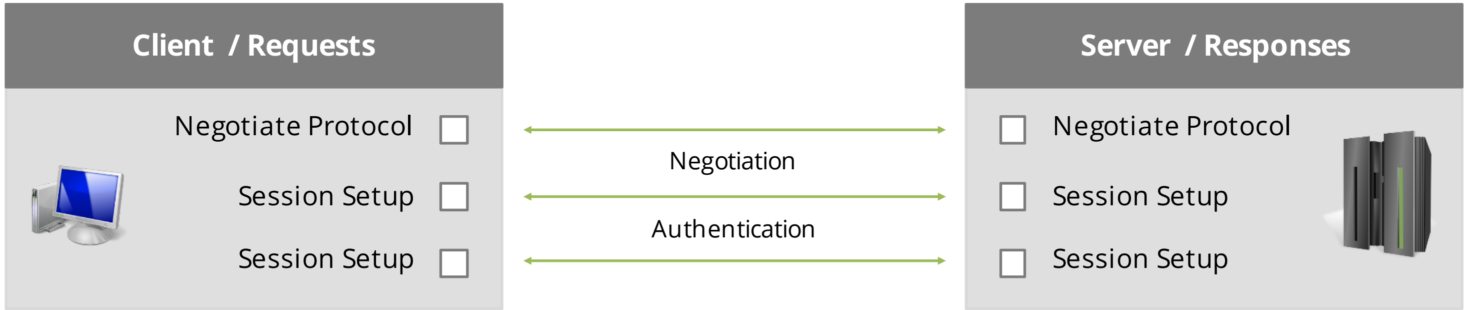
Login Authorization Failure

Use Case

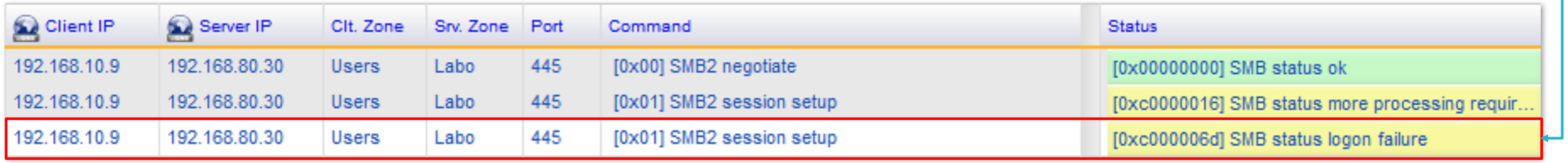
SMB2 - Wrong password when connecting to a remote resource

- **smbclient** *//nas.securactive.lan/public* **-U***demo* **-c** "*rm demo*" ***wrong_password*** **-m***SMB2*

Login Authorization Failure



- User “*demo*” was **not authorized** to connect to the remote resource



Client IP	Server IP	Clt. Zone	Srv. Zone	Port	Command	Status
192.168.10.9	192.168.80.30	Users	Labo	445	[0x00] SMB2 negotiate	[0x00000000] SMB status ok
192.168.10.9	192.168.80.30	Users	Labo	445	[0x01] SMB2 session setup	[0xc0000016] SMB status more processing requir…
192.168.10.9	192.168.80.30	Users	Labo	445	[0x01] SMB2 session setup	[0xc000006d] SMB status logon failure

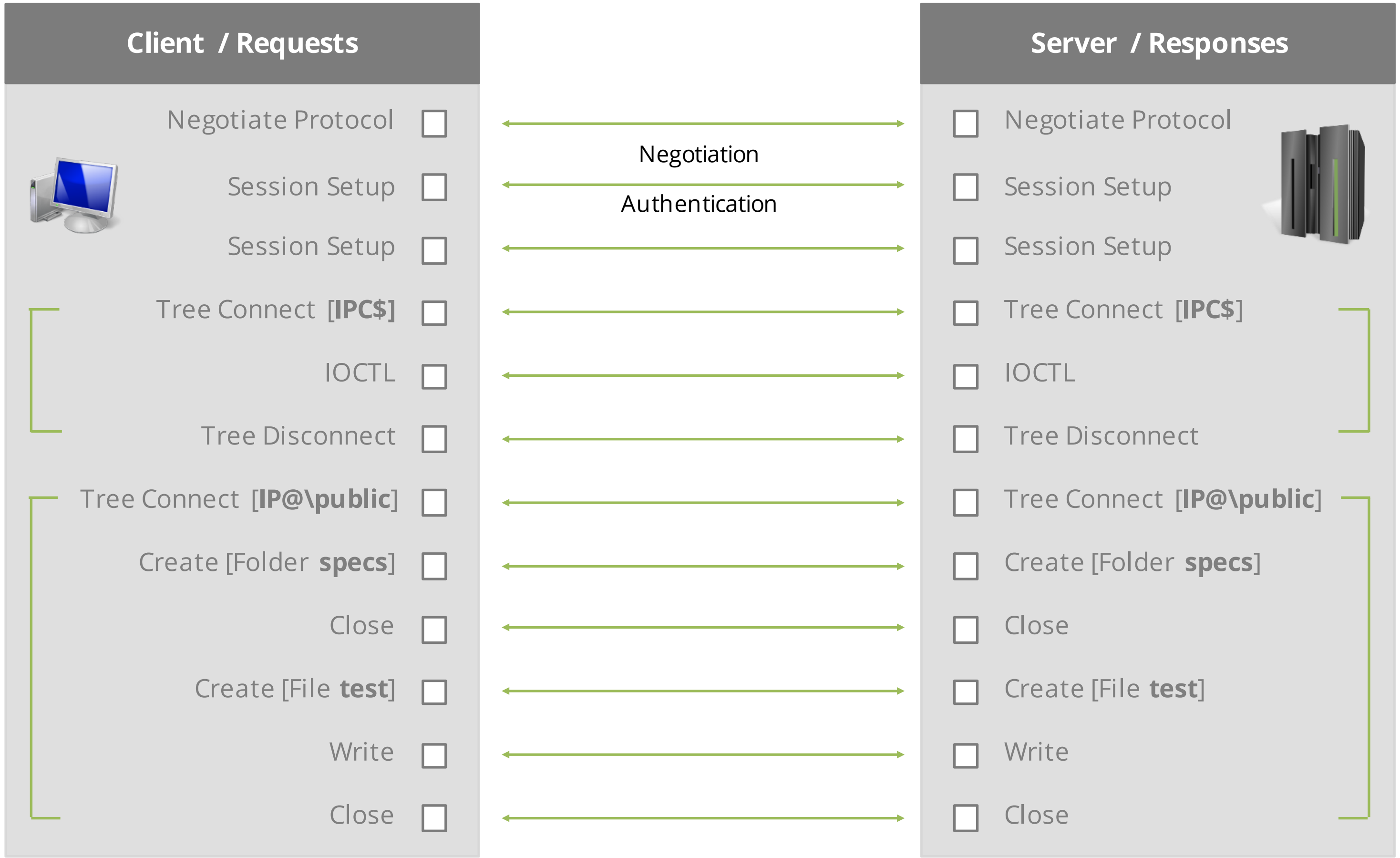
Put a File on a Remote Folder - SMB2

SMB2 - Use Case: Put a File on a Remote Folder

Use Case

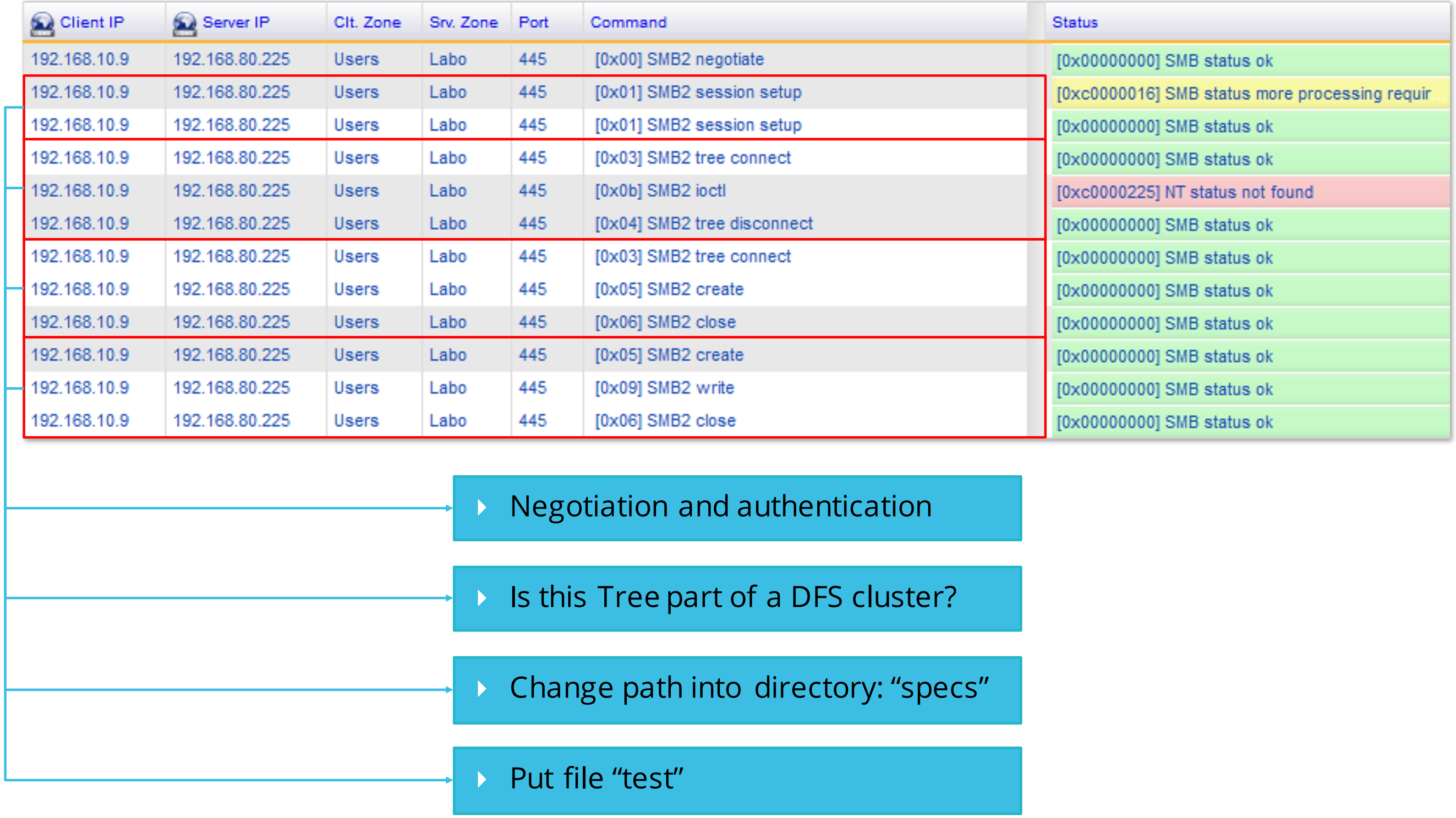
```
echo "Content!" > test
smbclient //nas.securactive.lan/public -Udemo -c "cd specs; put test" password -mSMB2
```

Put a File on a Remote Folder - SMB2



Client / Requests		Server / Responses
Negotiate Protocol □	Negotiation	□ Negotiate Protocol
Session Setup □	Authentication	□ Session Setup
Session Setup □		□ Session Setup
Tree Connect **[IPC$]** □		□ Tree Connect **[IPC$]**
IOCTL □		□ IOCTL
Tree Disconnect □		□ Tree Disconnect
Tree Connect **[IP@\public]** □		□ Tree Connect **[IP@\public]**
Create [Folder **specs**] □		□ Create [Folder **specs**]
Close □		□ Close
Create [File **test**] □		□ Create [File **test**]
Write □		□ Write
Close □		□ Close

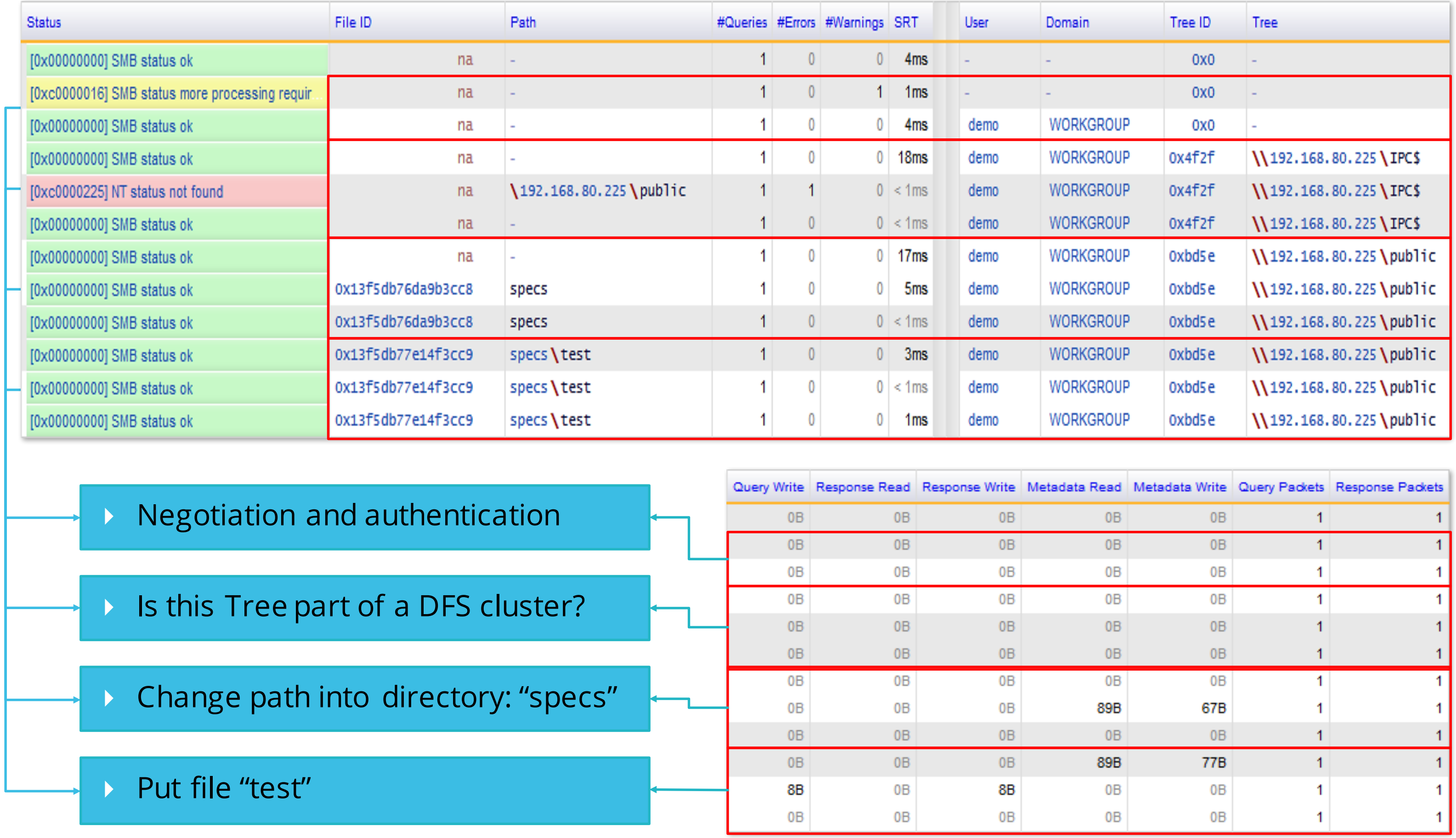
Put a File on a Remote Folder - SMB2



Client IP	Server IP	Clt. Zone	Srv. Zone	Port	Command	Status
192.168.10.9	192.168.80.225	Users	Labo	445	[0x00] SMB2 negotiate	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x01] SMB2 session setup	[0xc0000016] SMB status more processing requir
192.168.10.9	192.168.80.225	Users	Labo	445	[0x01] SMB2 session setup	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x03] SMB2 tree connect	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x0b] SMB2 ioctl	[0xc0000225] NT status not found
192.168.10.9	192.168.80.225	Users	Labo	445	[0x04] SMB2 tree disconnect	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x03] SMB2 tree connect	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x05] SMB2 create	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x06] SMB2 close	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x05] SMB2 create	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x09] SMB2 write	[0x00000000] SMB status ok
192.168.10.9	192.168.80.225	Users	Labo	445	[0x06] SMB2 close	[0x00000000] SMB status ok

- Negotiation and authentication
- Is this Tree part of a DFS cluster?
- Change path into directory: “specs”
- Put file “test”

Put a File on a Remote Folder - SMB2



Status	File ID	Path	#Queries	#Errors	#Warnings	SRT	User	Domain	Tree ID	Tree
[0x00000000] SMB status ok	na	-	1	0	0	4ms	-	-	0x0	-
[0xc0000016] SMB status more processing requir	na	-	1	0	1	1ms	-	-	0x0	-
[0x00000000] SMB status ok	na	-	1	0	0	4ms	demo	WORKGROUP	0x0	-
[0x00000000] SMB status ok	na	-	1	0	0	18ms	demo	WORKGROUP	0x4f2f	\\192.168.80.225\IPC$
[0xc0000225] NT status not found	na	\192.168.80.225\public	1	1	0	< 1ms	demo	WORKGROUP	0x4f2f	\\192.168.80.225\IPC$
[0x00000000] SMB status ok	na	-	1	0	0	< 1ms	demo	WORKGROUP	0x4f2f	\\192.168.80.225\IPC$
[0x00000000] SMB status ok	na	-	1	0	0	17ms	demo	WORKGROUP	0xbd5e	\\192.168.80.225\public
[0x00000000] SMB status ok	0x13f5db76da9b3cc8	specs	1	0	0	5ms	demo	WORKGROUP	0xbd5e	\\192.168.80.225\public
[0x00000000] SMB status ok	0x13f5db76da9b3cc8	specs	1	0	0	< 1ms	demo	WORKGROUP	0xbd5e	\\192.168.80.225\public
[0x00000000] SMB status ok	0x13f5db77e14f3cc9	specs\test	1	0	0	3ms	demo	WORKGROUP	0xbd5e	\\192.168.80.225\public
[0x00000000] SMB status ok	0x13f5db77e14f3cc9	specs\test	1	0	0	< 1ms	demo	WORKGROUP	0xbd5e	\\192.168.80.225\public
[0x00000000] SMB status ok	0x13f5db77e14f3cc9	specs\test	1	0	0	1ms	demo	WORKGROUP	0xbd5e	\\192.168.80.225\public

Query Write	Response Read	Response Write	Metadata Read	Metadata Write	Query Packets	Response Packets
0B	0B	0B	0B	0B	1	1
0B	0B	0B	0B	0B	1	1
0B	0B	0B	0B	0B	1	1
0B	0B	0B	0B	0B	1	1
0B	0B	0B	0B	0B	1	1
0B	0B	0B	0B	0B	1	1
0B	0B	0B	0B	0B	1	1
0B	0B	0B	89B	67B	1	1
0B	0B	0B	0B	0B	1	1
0B	0B	0B	89B	77B	1	1
8B	0B	8B	0B	0B	1	1
0B	0B	0B	0B	0B	1	1

- Negotiation and authentication
- Is this Tree part of a DFS cluster?
- Change path into directory: “specs”
- Put file “test”

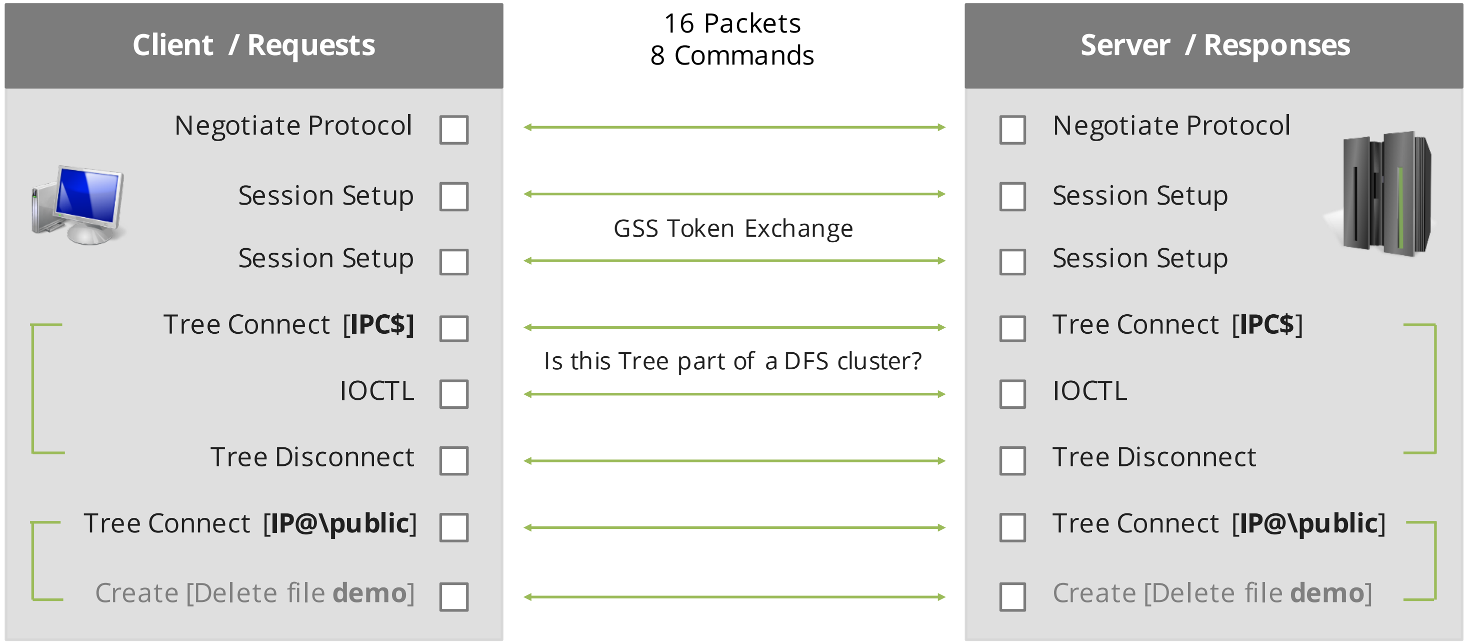
Not Authorized to Delete a Remote File

SMB2 - Not Authorized to Delete a Remote File

Use Case

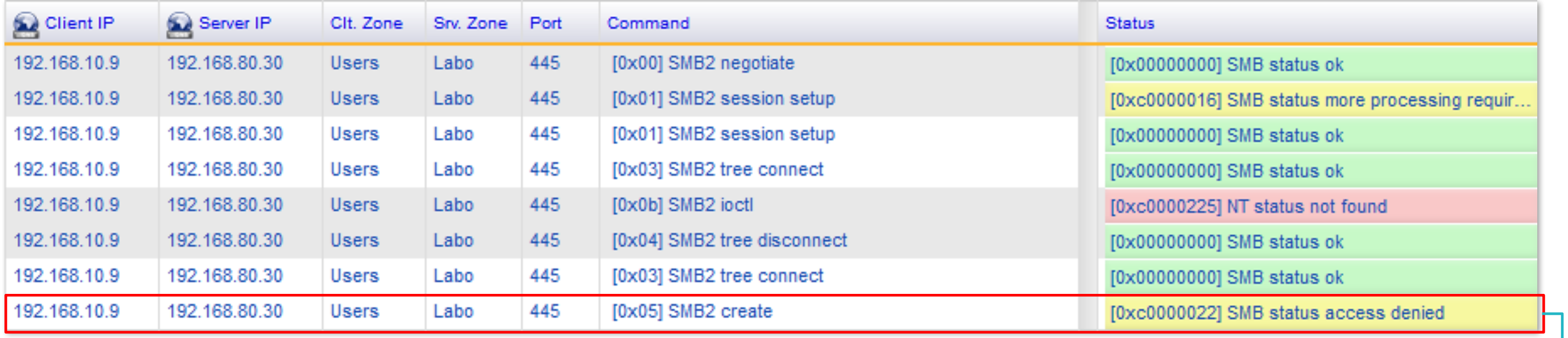
- The user "*demo*" has no write access to the file "*/public/demo*"
- smbclient //nas.securactive.lan/public -Udemo -c "rm demo" password -mSMB2

Not Authorized to Delete a Remote File



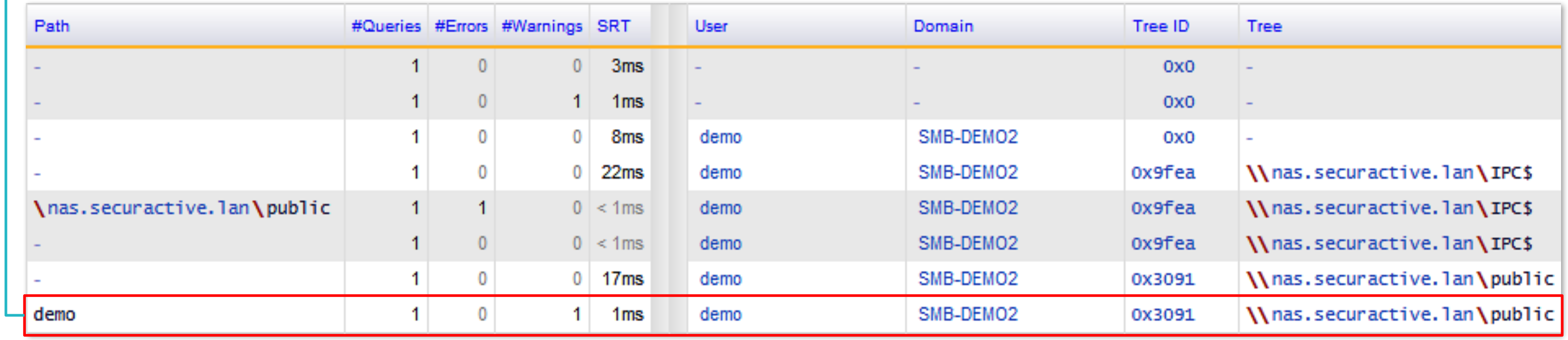
Client / Requests	16 Packets 8 Commands	Server / Responses
Negotiate Protocol □	↔	□ Negotiate Protocol
Session Setup □	↔	□ Session Setup
Session Setup □	GSS Token Exchange ↔	□ Session Setup
Tree Connect **[IPC$]** □	↔	□ Tree Connect **[IPC$]**
IOCTL □	Is this Tree part of a DFS cluster? ↔	□ IOCTL
Tree Disconnect □	↔	□ Tree Disconnect
Tree Connect **[IP@\public]** □	↔	□ Tree Connect **[IP@\public]**
Create [Delete file **demo**] □	↔	□ Create [Delete file **demo**]

Not Authorized to Delete a Remote File



Client IP	Server IP	Clt. Zone	Srv. Zone	Port	Command	Status
192.168.10.9	192.168.80.30	Users	Labo	445	[0x00] SMB2 negotiate	[0x00000000] SMB status ok
192.168.10.9	192.168.80.30	Users	Labo	445	[0x01] SMB2 session setup	[0xc0000016] SMB status more processing requir...
192.168.10.9	192.168.80.30	Users	Labo	445	[0x01] SMB2 session setup	[0x00000000] SMB status ok
192.168.10.9	192.168.80.30	Users	Labo	445	[0x03] SMB2 tree connect	[0x00000000] SMB status ok
192.168.10.9	192.168.80.30	Users	Labo	445	[0x0b] SMB2 ioctl	[0xc0000225] NT status not found
192.168.10.9	192.168.80.30	Users	Labo	445	[0x04] SMB2 tree disconnect	[0x00000000] SMB status ok
192.168.10.9	192.168.80.30	Users	Labo	445	[0x03] SMB2 tree connect	[0x00000000] SMB status ok
192.168.10.9	192.168.80.30	Users	Labo	445	[0x05] SMB2 create	[0xc0000022] SMB status access denied

- The user "*demo*" has not the appropriate **access rights** to the file "*/public/demo*"



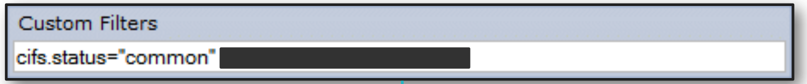
Path	#Queries	#Errors	#Warnings	SRT	User	Domain	Tree ID	Tree
-	1	0	0	3ms	-	-	0x0	-
-	1	0	1	1ms	-	-	0x0	-
-	1	0	0	8ms	demo	SMB-DEMO2	0x0	-
-	1	0	0	22ms	demo	SMB-DEMO2	0x9fea	\\nas.securactive.lan\IPC$
\nas.securactive.lan\public	1	1	0	< 1ms	demo	SMB-DEMO2	0x9fea	\\nas.securactive.lan\IPC$
-	1	0	0	< 1ms	demo	SMB-DEMO2	0x9fea	\\nas.securactive.lan\IPC$
-	1	0	0	17ms	demo	SMB-DEMO2	0x3091	\\nas.securactive.lan\public
demo	1	0	1	1ms	demo	SMB-DEMO2	0x3091	\\nas.securactive.lan\public

Fast Analysis: SMB / CIFS
Common Statuses

Common Statuses:

- STATUS_NO_SUCH_FILE,
- STATUS_NO_SUCH_DEVICE,
- STATUS_OBJECT_NAME_NOT_FOUND,
- STATUS_OBJECT_PATH_INVALID,
- STATUS_OBJECT_PATH_NOT_FOUND,
- STATUS_OBJECT_PATH_SYNTAX_BAD,
- STATUS_DFS_EXIT_PATH_FOUND,
- STATUS_REDIRECTOR_NOT_STARTED,
- STATUS_TOO_MANY_OPENED_FILES,
- STATUS_ACCESS_DENIED,
- STATUS_PORT_CONNECTION_REFUSED,
- STATUS_FILE_DELETED,
- STATUS_INSUFF_SERVER_RESOURCES,
- STATUS_MORE_PROCESSING_REQUIRED,
- STATUS_BUFFER_OVERFLOW,
- STATUS_WRONG_PASSWORD,
- STATUS_NETWORK_ACCESS_DENIED,
- STATUS_TOO_MANY_SESSIONS.

Common statuses category contains the **most common** SMB/CIFS **errors** and **warnings**.



Custom Filters

cifs.status="common" [redacted]

cifs.status = "common"

Note: We do **not** consider *SMB_STATUS_NO_MORE_FILES* as a Warning

Content

1. Product Features

2. SMB Overview & Use Cases

- 1. Connect and Browse Files
- 2. Login Authorization Failure
- 3. Put a File on a Remote Folder
- 4. Not Authorized to Delete a Remote File

3. Documentation + Q&A

© Performance Vision

SMB Documentation

- Server Message Block (SMB) Protocol Versions 2 and 3
- SNIA - SMB Remote Protocol
- SNIA - SMB2 Big Improvements
- Present and Future File Serving with Samba

SMB / CIFS Transactions Performance Analysis

Performance Vision helps keeping your customers happy!

performance vision

Satisfied Customers

performance
vision

🌐 www.performancevision.com

✉ sales@performancevision.com

☎ +33 1 78 09 07 00