



# Tuning Trace:Magic

Richtlinien für schnelle Datenverarbeitung mit Trace:Magic

Stand: 2004-11-19

<http://www.synapse.de/2005/download/synapse-networks.tracemagic.slow-analysis.ger.pdf>

TraceMagic arbeitet langsam. Warum? Was könnte man tun? .....	2
Physical Memory (Hauptspeicher): 2 GB RAM min. ....	2
Virtual Memory (Auslagerungs-Datei): PAGEFILE.SYS .....	2
Intel Multi-Prozessor-Plattform mit HyperThreading .....	3
Festplatte: IDE Stripe Set / SCSI / RAID-0 / RAID-5.....	4
Viren-Scanner .....	5
MS-Windows: Auto-Journal Funktion von MS-Outlook .....	5
MS-Windows: Verzeichnis- und Datei-Index .....	6
Aufzeichnung der MessDaten läuft noch: CAPTURING .....	10
TraceMagic liest vom / schreibt auf Server-Laufwerk .....	10
Zu viele Datenbank-Tabellen der Trace:Statistics aktiv während der Analyse.....	11
Zu viele Analyse-Funktionen in HostMagic / SpiderMagic .....	13
Zu viele stets wiederkehrende Event-Log-Einträge .....	15
Zu viele Event-Log-Einträge überhaupt bei laufendem „Log View“.....	16
Zu viel Leerlauf bei Vorlauf / Rücklauf .....	18
Zu viel Leerlauf in TCP-ReTx-Analyse .....	20
Zu viele HTTP-Dialoge in TCP-ReTx-Analyse .....	20
Mirror-Port: Mehrere Client/Server/Uplink-Ports auf Mirror-Port gespiegelt.....	21
Mirror-Port: Alle Daten eines VLANs werden auf den Mirror-Port gespiegelt.....	21



## **TraceMagic arbeitet langsam. Warum? Was könnte man tun?**

### **Physical Memory (Hauptspeicher): 2 GB RAM min.**

Ohne genügend RAM ist TraceMagic eine Schnecke.

Es wird empfohlen, TraceMagic auf Windows-Versionen ab Win2K/WinXP (oder später) zu betreiben bei

min. 2 GB RAM / besser: 3 GB RAM

Die Geschwindigkeits-Unterschiede liegen im Gebrauch (oder Nicht-Gebrauch) des Auslagerungs-Speichers (PAGESFILE.SYS, siehe unten), falls der RAM nicht ausreicht.

### **Virtual Memory (Auslagerungs-Datei): PAGESFILE.SYS**

Die Fähigkeit, MessDaten in den Mengen mehrerer GigaBytes verarbeiten zu können, hängt wesentlich vom verfügbaren Speicher des MS-Windows-Systems ab.

Rufen Sie die Systemsteuerung auf und stellen Sie den "VIRTUAL MEMORY" so ein, dass die Festplatte mit dem meisten freien Speicherplatz für das "PAGE FILE" benutzt wird.

Trace:Magic ist erheblich abhängig davon, dass optimal mit "Swapping" gearbeitet werden kann.

Win2K und WinXP unterstützen bis zu max. 4 GB (4.095 MB) je Festplatte.

Dies sollte genutzt werden.



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Intel Multi-Prozessor-Plattform mit HyperThreading**

Ein TraceMagic-Anwender schreibt (November 2004):

Nachdem wir Trace-Magic jetzt einige Zeit im Einsatz haben und ich eigene Erfahrungen bezüglich der Performance-Optimierung sammeln konnte, hätte ich eine Tip, den ich den anderen Anwendern nicht vorenthalten möchte und der noch nicht in den Performance-Hinweisen steht:

**Bei CPUs mit Intels Hyperthreading sollte dieses unbedingt im Bios deaktiviert werden.**

Wie Sie aus den angehängten Screenshots (die Sie übrigens nach Belieben verwenden können) erkennen, verwendet TM mehr oder weniger nur eine der vier virtuellen CPUs komplett und nutzt dabei die verfügbare Prozessorzeit der gesamten Maschine nur zu 25%. Bei abgeschaltetem HT steigt die Nutzung auf 50% mit entsprechend schnellerer Abarbeitung der gleichen Aufgabe. Einstellungen und Traces waren dabei identisch, das Bild sieht über fast den gesamten Lauf genau so aus.

Dabei ist zu beobachten, dass die Aufgaben von TM offensichtlich nur schlecht zu parallelisieren sind. Das Programm nutzt auf der Zweiprozessormaschine zwar abwechselnd die eine und die andere CPU, aber nie gleichzeitig beide in nennenswertem Umfang. Die Empfehlung sollte also aus meiner Sicht lauten:

Besser eine Ein-Prozessor-Maschine mit möglichst schneller CPU als eine Mehr-Prozessor-Maschine mit weniger hoher Leistung pro Prozessor (vorausgesetzt die Maschine soll nicht auch z.B. als Webserver für Analyseberichte dienen, wie bei uns).

Synapse:Networks schließt sich dieser Beobachtung bzw. Empfehlung an.



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Festplatte: IDE Stripe Set / SCSI / RAID-0 / RAID-5**

Die Festplatte hat noch weit mehr Einfluss als der Prozessor; oder, besser gesagt: Der schnellste Prozessor nutzt nichts, wenn die Festplatte nicht mithalten kann.

TraceMagic ist unter Umständen sehr zugriffs-freudig, wenn viele Text-Einträge in den sog. EVENT LOGs vorzunehmen sind.

Hier ist eine Festplatte mit hoher Schreib-Geschwindigkeit wichtig.

Je mehr Schreib-Lese-Köpfe die Festplatte (bzw. der Festplatten-Verbund) hat, um so schneller ist die Verarbeitung der MessDaten.

Von Wichtigkeit ist auch der On-Board Read/Write CACHE des Festplatten-Controllers.

IDE Stripe Sets und SCSI Festplatten gehören hierher wie auch RAID-0 und RAID-5.

Zwar läuft TraceMagic auch auf Laptops; aber: Während Prozessor-Takt (3 GHz) und RAM (1 GB) zwar verfügbar sind, bleiben doch die kleinen Festplatten-Laufwerke das Nadelöhr. Hier sollten die Erwartungen also nicht zu hoch angesetzt werden.



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Viren-Scanner**

Viren-Scanner können die System-Leistung erheblich beeinträchtigen; dies gilt auch für die Auto-Journal Funktion von MS-Outlook.

Viren-Scanner sollten de-aktiviert werden.

ACHTUNG!

Es wurden schon Viren-Scanner beobachtet, die sich nur vorübergehend abschalten ließen – und die sich nach einer gewissen Zeit (10-20 Min.) wieder von selbst aktivierten. In diesem Falle wäre wenig gewonnen.

**MS-Windows: Auto-Journal Funktion von MS-Outlook**

Die Auto-Journal Funktion von MS-Outlook kann zu erheblichen Leistungs-Einbußen führen.

Die MS-Outlook Auto-Journal-Funktion sollte abgestellt werden:

**HKEY\_CURRENT\_USER\Software\Microsoft\SharedTools\Outlook\Journaling**  
**HKEY\_USERS\.DEFAULT\Software\Microsoft\SharedTools\Outlook\Journaling**

Ggf sollten Sie auch die Journal-Datei "offitems.log" löschen.

WICHTIG:

Auch auf Windows-Rechnern, die **keine** MS-Outlook-Installation besitzen, können über die Auto-Journal-Funktion verfügen!

Siehe MS-Knowledgebase (Auswahl):

196108 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;196108>

201079 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;201079>

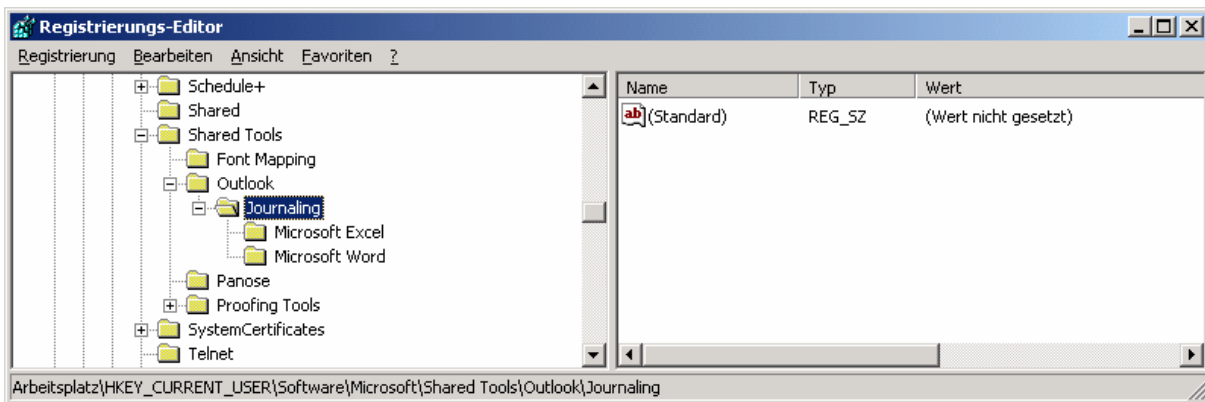
291145 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;291145>

312959 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;312959>

Mittels REGEDIT kann der entsprechende Schalter unmittelbar in der Windows-Registry geändert werden:



## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?



Hierzu ist auf die Beschreibung von Microsoft zu achten (siehe oben: Knowledgebase-Eintrag 196108).

### MS-Windows: Verzeichnis- und Datei-Index

Versuche haben ergeben, dass schnell bis zu 20% Verzögerung eintreten können, wenn der Datei- und Verzeichnis-Index von MS-Windows aktiv ist.

In Einzelfällen haben Vergleichs-Tests sogar bis zu 50% Verzögerung ergeben!

(**3** Stunden Dauer mit Index-Dienst gegenüber nur **2** Stunden ohne Index-Dienst.)

Daher wird daher **dringend** empfohlen, den Index-Dienst abzuschalten!

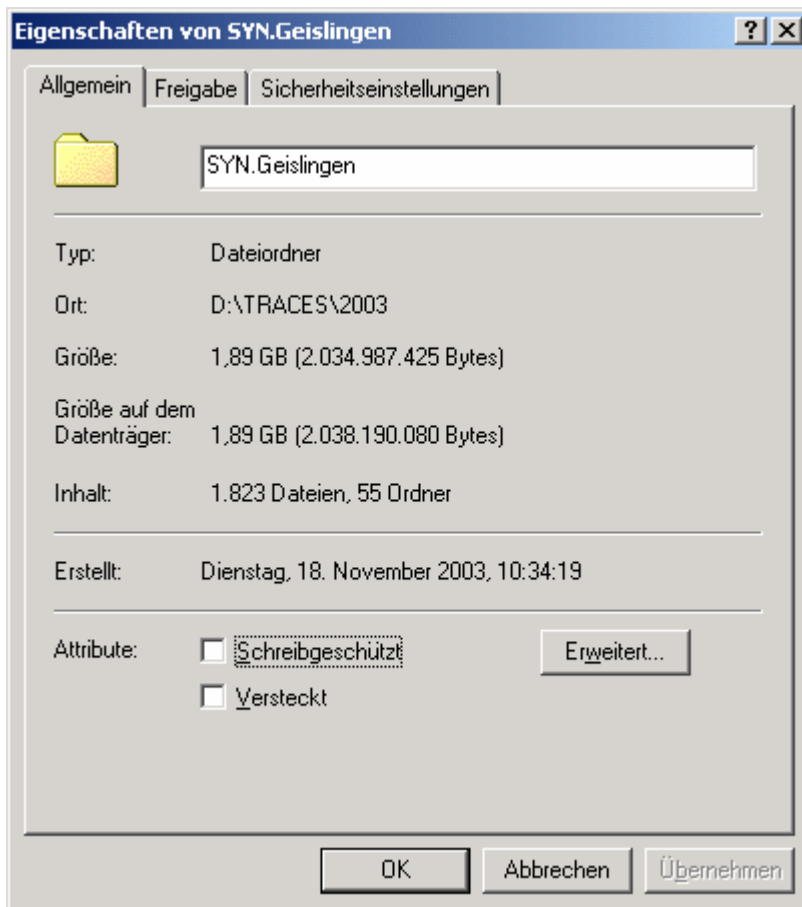
Dies geschieht über den Windows-Explorer.

Um festzustellen, ob der Index-Dienst aktiv ist, und um ihn ggf abzuschalten, ist wie folgt vorzugehen:

- Windows-Explorer öffnen, Verzeichnis mit den MessDaten und TraceMagic-Reports mit Maus anwählen.
- Rechte Maustaste -> Popup-Menü.
- Ggf das Attribut "schreibgeschützt" (read-only) entfernen (falls von CD-ROM einkopiert!).
- Dann auf den Button "[ >>> ERWEITERT ] " drücken.
- Den Index-Dienst abschalten.
- Dann auf "Übernehmen" drücken; darauf achten, dass alle Unterverzeichnisse "mitgenommen" werden.



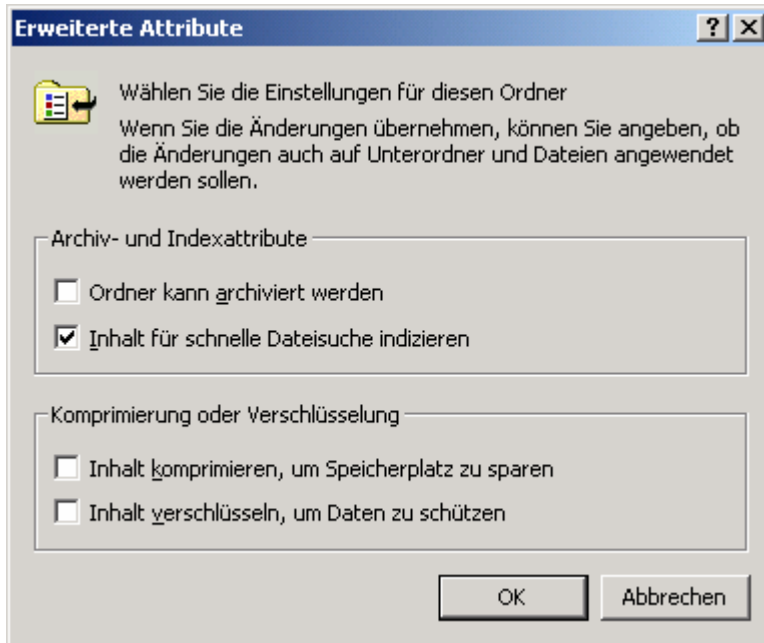
## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?



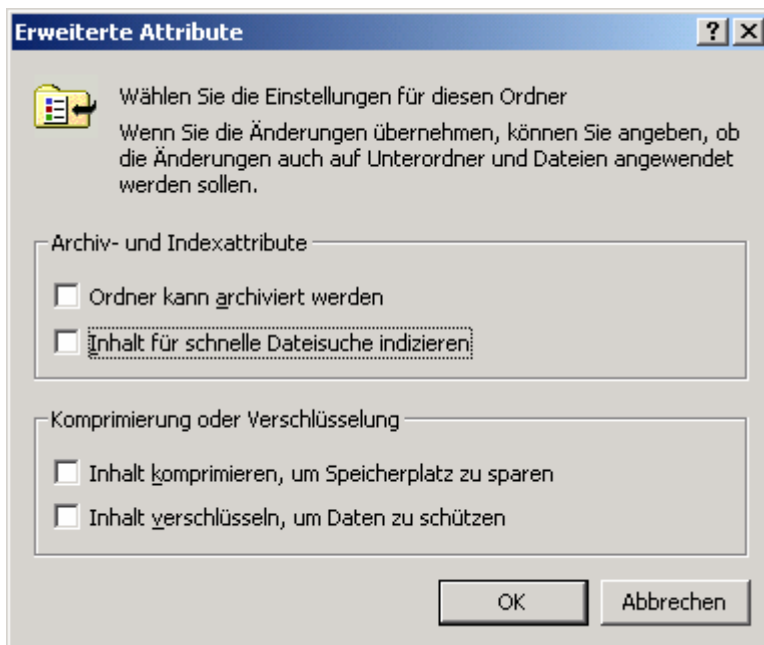


## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?

Falsch:



Richtig:

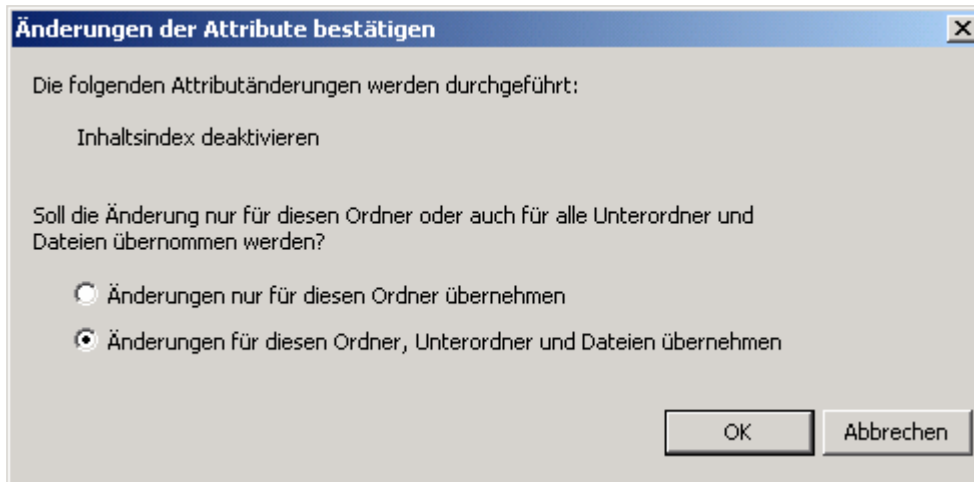




---

## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?

---





---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Aufzeichnung der MessDaten läuft noch: CAPTURING**

Sollte TraceMagic schon gestartet werden, während in einem anderen Prozess noch die CAPTURE ENGINE (Sniffer, EtherPeek NX, Observer, etc.) damit beschäftigt ist, LAN-Verkehr aufzuzeichnen, sollte sich von selbst verstehen, dass dies auf Kosten der System-Leistung geht.

In diesem Falle dürfte nicht nur TraceMagic langsam sein (weil der Prozessor anderweitig Prioritäten setzt), - sondern auch das Capturing dürfte beeinträchtigt sein, was sich am Ende in Paket-Verlusten niederschlagen dürfte.

Je nach Rechner-Architektur kann sogar folgendes geschehen:

Die LAN-Aufzeichnung bzw. das Capturing wurde beendet; der LAN-Analyzer wurde beendet; und trotzdem ist das PC-System auffällig langsam. In diesem Falle wird der Prozessor behindert durch die hohe Zahl der Hardware-Interrupts, die vom LAN-Adapter nach wie vor durch den Paket-Empfang (Rx) ausgelöst werden.

In diesem Falle also: LAN-Kabel vom PC trennen!

**TraceMagic liest vom / schreibt auf Server-Laufwerk**

Theoretisch wäre möglich, dass TraceMagic auf einem Arbeitsrechner (Client, Workstation) läuft und die Trace-Dateien von einem Server-Laufwerk liest und die Report-Dateien wiederum auf diesem Server-Laufwerk anlegt.

Da TraceMagic sehr schreib-intensiv ist (TM.HIT.FRAMES.\*.TXT), kann das erheblich Geschwindigkeit kosten.

Spätestens das Schreiben der Statistiken in die Datenbank-Tabellen (in Sonderheit: Tabelle [3] / TCP Port Statistics) verläuft in dieser Weise sehr langsam.



## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?

### Zu viele Datenbank-Tabellen der Trace:Statistics aktiv während der Analyse

Schon während der laufenden Analyse können die Ergebnis-Datenbanken (mit wenigen Einschränkungen) eingesehen und z.T. bearbeitet werden.

Das kann zwar sinnvoll sein, wenn nicht gewartet werden kann, bis die Analyse zu Ende gelaufen ist (Zeitdruck!).

Aber es ist äußerst leistungshemmend, wenn (siehe Abbildung) beispielsweise alle 2 Minuten die Tabelle mit den Ergebnissen zu „SMB Denied Resources“ („ACCESS\_FAILURE,“) aktualisiert wird !!

The screenshot shows the Trace:Magic Trace:Statistics window. The title bar reads "Trace:Magic -> Trace:Statistics [Spider:Magic]". The main window displays a table titled "SMB Client Resource Requests / Server Error Returns (Denied Resources)". The table has columns for #, Count, Status, Resource Path (as requested by client), and [Path Directory]. The table is populated with 20 rows of data. A dropdown menu is open over the table, showing refresh intervals: --5- Min., -30- Sec., --1- Min., --2- Min. (selected), --5- Min., -10- Min., -20- Min., -30- Min., and -60- Min. The table data is as follows:

#	Count	Status	Resource Path (as requested by client)	[Path Directory]
1	0	0	Trace:Magic	max. 40000 Item
2	1	0	\rge009\RICHED20.DLL	\rge009\
3	1	0	\rge009\msi.dll	\rge009\
4	1	1	\ppdk01\winspool.driv	\ppdk01\
5	1	1	\rge009\WINSPOOL.DRV	\rge009\
6	12	3	\vessn152\rghomel\$	\vessn152\
7	1	0	\rg0485\shim.dll	\rg0485\
8	75	1	\tzia01\wdmaud.driv	\tzia01\
9	4	0	\tzia01\rsabase.dll	\tzia01\
10	1	0	\tzia01\USERENV.dll	\tzia01\
11	1	0	\tzia01\CRYPT32.dll	\tzia01\
12	1	0	\tzia01\MSASN1.DLL	\tzia01\
13	1	0	\tzia01\netapi32.dll	\tzia01\
14	1	0	\tzia01\SECUR32.DLL	\tzia01\
15	1	0	\tzia01\NETRAP.DLL	\tzia01\
16	1	0	\tzia01\SAMLIB.DLL	\tzia01\
17	1	0	\tzia01\DNSAPI.DLL	\tzia01\
18	1	0	\tzia01\PegConnectConfirm.WAV	\tzia01\
19	2	0	\tzia01\PegConnectConfirm	\tzia01\
20	2	0	\tzia01\CLBCATQ.DLL	\tzia01\



## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?

Abbildung: Das Aktualisierungs-Intervall der Trace:Statistics (während der Analyse!) wird hier im Beispiel auf 2 Minuten gesetzt – eine Katastrophe, wenn Tausende von Tabellen-Einträgen in diesem kurzen Zeit-Abstand stets erneuert werden!

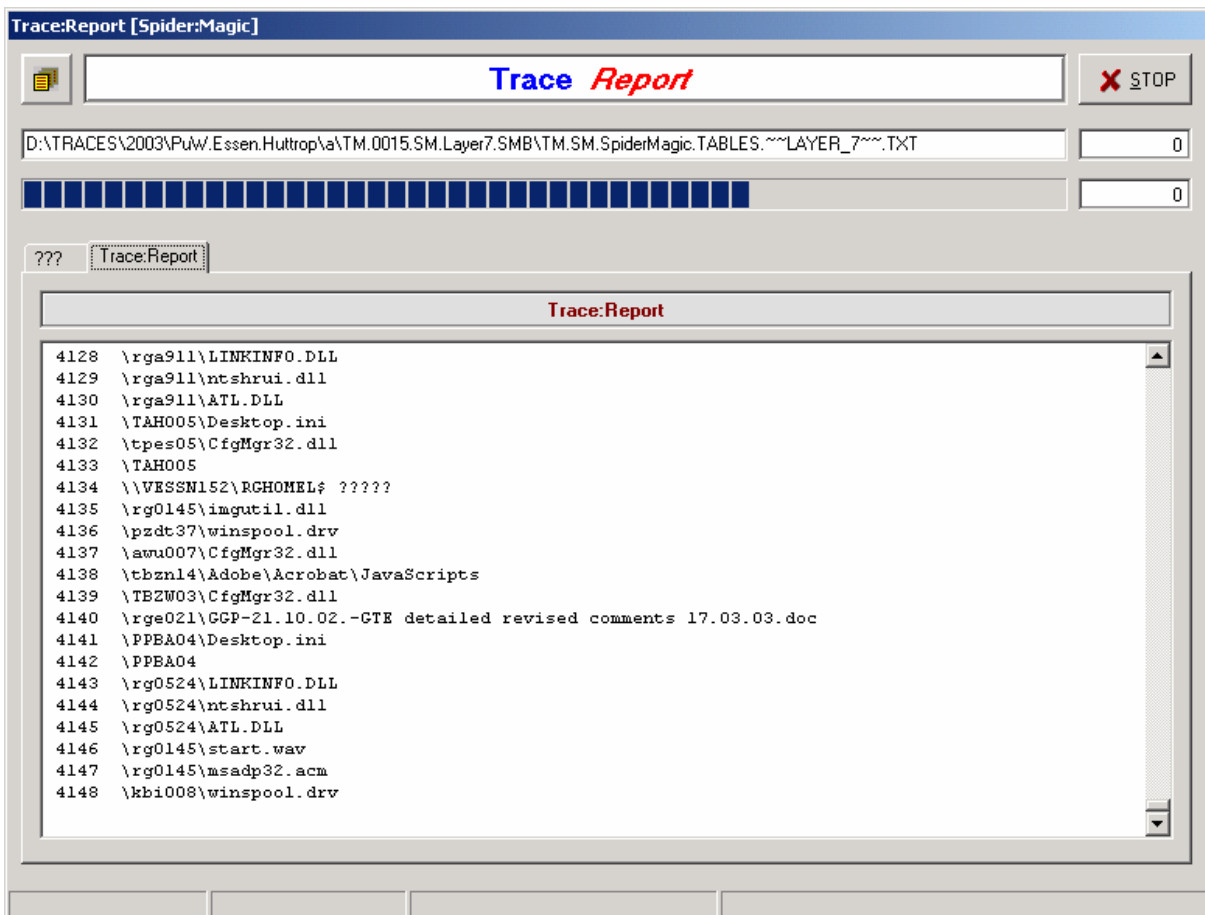


Abbildung: Das TraceReport-Fenster erscheint, wenn die Aktualisierung der „Tabelle 5“ (SMB: Denied Resources / ACCESS\_DENIED) gerade läuft.



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Zu viele Analyse-Funktionen in HostMagic / SpiderMagic**

Bei der Verarbeitung von max. 1.024 Dateien ist klar, dass sich die Verarbeitungszeit extrem dehnt, wenn alle Teil-Funktionen aktiv sind - Funktionen, die prozessor-intensiv sind ... auch dann, wenn die gesuchten Fehler am Ende gar nicht da sind.

Die Lösung liegt hier in den ab TMv4 verfügbaren Analyse-Profilen:

" Analysis:Profiles "

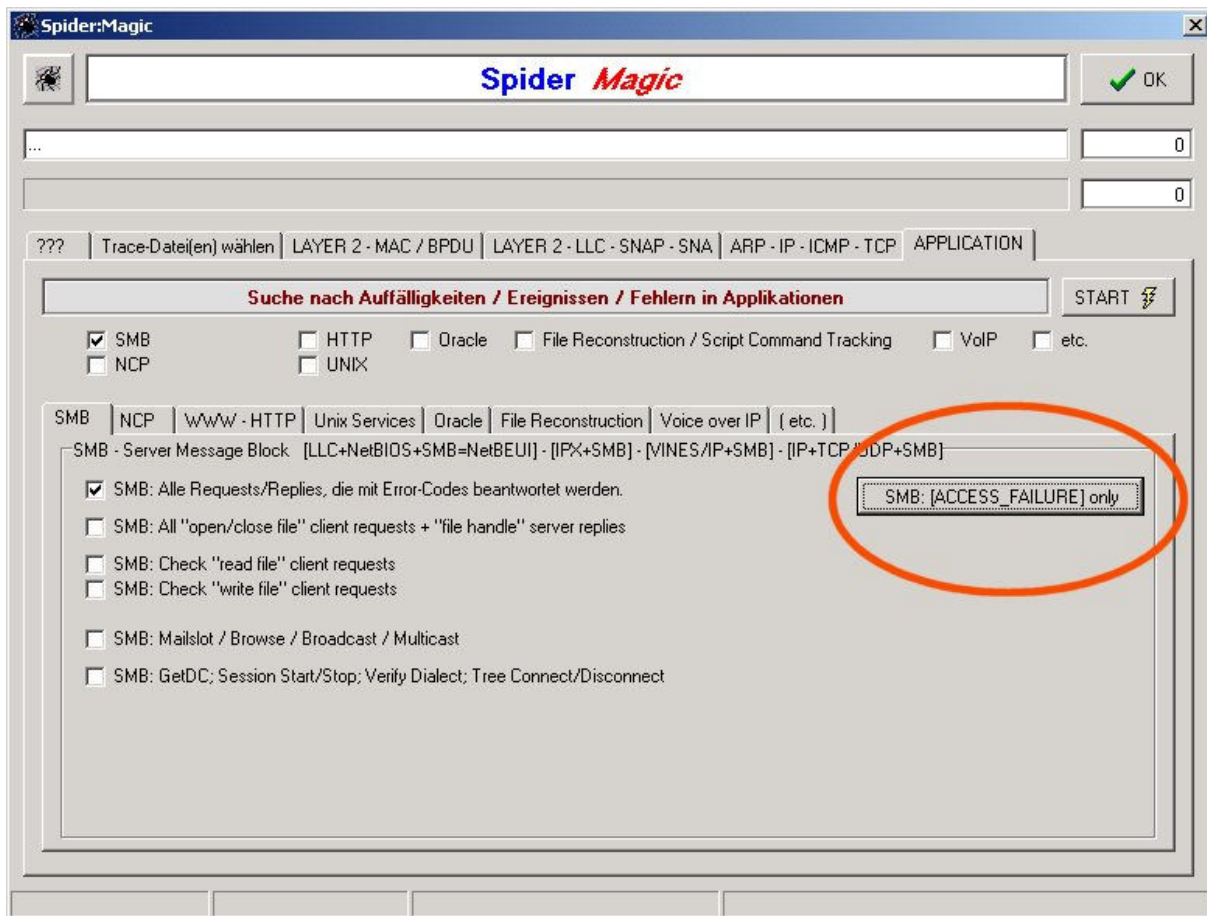
Hierzu sind die näheren Beschreibungen abzuwarten, die mit TMv4 erscheinen werden.

Bis dahin ist zu empfehlen:

Es sollten manuell Einstellungen vorgenommen werden, welche sich darauf beschränken, wahrscheinliche bzw. mögliche Fehler zu suchen (z.B. "ACCESS\_FAILURE" bei Windows-SMB), unwahrscheinliche bzw. unmögliche Fehler aber auszulassen (z.B. WAN-Fehler, wo nur Campus-LAN vorhanden ist).



## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?



Die Abbildung zeigt den Button „SMB: [ACCESS\_FAILURE] only“, mit dem die Analyse beschränkt werden kann auf Fehlzugriffe in Client-Server-Dialogen (Windows/SMB).

Ähnliche, auf bestimmte Fehler-Profile zielende Einstellungen lassen sich ab TMv4 mittels der „Analysis:Profiles“ weitgehend automatisiert verwenden.



## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?

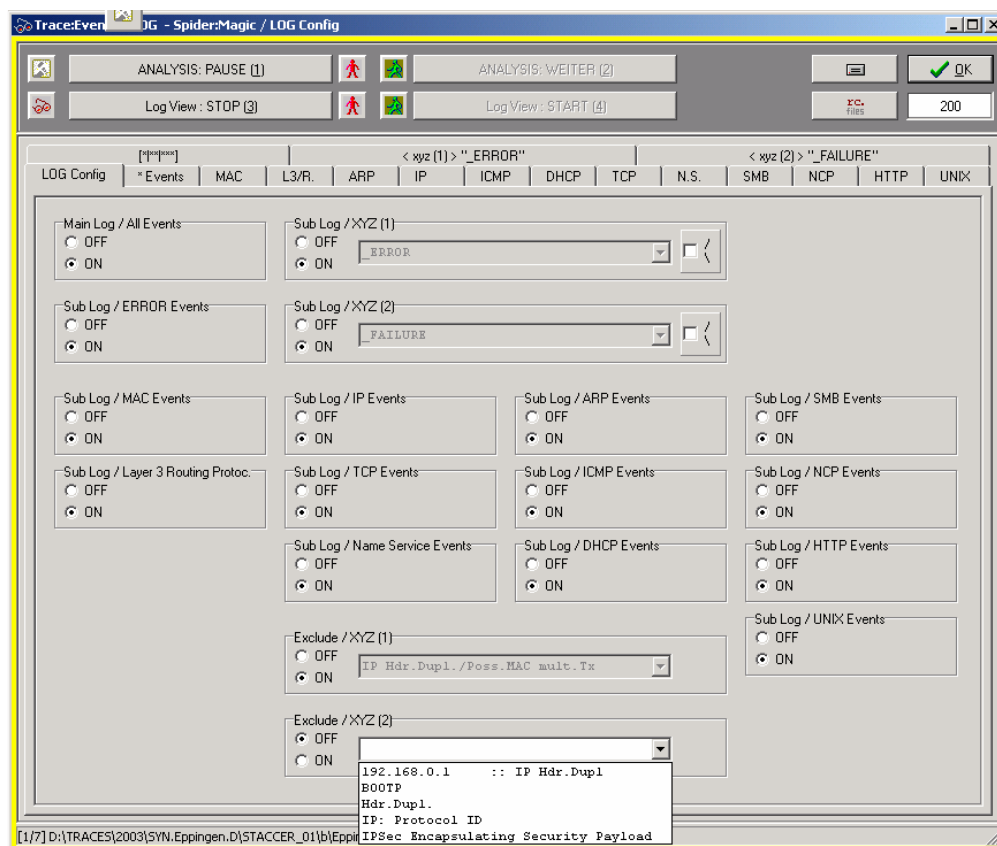
### Zu viele stets wiederkehrende Event-Log-Einträge

Es bleibt nicht aus, dass im einen oder anderen Netzwerk die selben Ereignisse stets erneut zu sehen sind und daher stets erneut von TraceMagic in die Log-Dateien geschrieben werden.

Da sich während der laufenden Verarbeitung die Einstellungen zu den aktivierten Analyse-Funktionen **nicht** mehr ändern lassen, kann wenigstens hilfsweise während der laufenden Analyse im großen EVENT-LOG-Fenster (Seite „LOG Config“) ein EXCLUDE-Filter setzen:

Dieser Ausschluss-Filter bewirkt, dass alle Text-Zeilen **nicht** mehr in die Event-Log-Datei(en) geschrieben werden, welche das angegebene Text-Merkmal enthalten.

Hierzu zählen z.B. Meldungen wie „IP Hdr.Dupl.“ (IP Header Duplicated) oder „TCP: One Way“ (in einer TCP-Sitzung werden je IP-Teilnehmer nur Rx oder nur Tx „gesehen“).



Die Abbildung zeigt, wie ein EXCLUDE-Filter im EVENT LOG gesetzt werden kann.



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Zu viele Event-Log-Einträge überhaupt bei laufendem „Log View“**

Es kann während der laufenden Analyse eine Voraus-Schau auf die im Hintergrund in Datei(en) geschriebene(n) EVENT LOGs genommen werden.

Bei einer hohen Zahl von LOG-Einträgen kann ein mitlaufendes LOG VIEW erhebliche Leistungseinbußen bewirken.

Besonders schlimm wird es, wenn bei einem Monitor mit hoher Auflösung auch noch das große EVENT-LOG-(XXL)-Fenster aktiv ist.

Die Aktualisierung der Text-Zeilen beschäftigt das Windows-GUI erheblich und kann u.U. die Analyse-Geschwindigkeit **brutal** verlangsamen.

Hier gilt:

Das LOG VIEW Fenster nur so lange aktiv lassen, wie es auch benötigt wird!

So lange niemand aktiv am Bildschirm arbeitet, sollte die Einstellung „LogView = OFF“ gewählt werden (siehe Abbildung).



## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?

Abbildung: Die START-STOP-Tasten für das Anschalten/Abschalten der „Log View“-Funktion (Vorschau auf das EVENT LOG).

Der äußerste Brems-Effekt kann zudem übrigens erreicht werden, wenn nicht nur das XXL-Fenster geöffnet wurde über den Button mit der Brille: [ >>> ], sondern wenn zuvor die Anzahl der je Log-Fenster angezeigten Text-Zeilen von den voreingestellten 200 auf 1.000 oder gar 10.000 hoch gesetzt wurde (siehe Abbildung: das kleine Auswahl-Menü rechts neben dem START Button).

In diesem Falle ist das Windows-GUI so sehr mit den Darstellungs-Aufgaben beschäftigt, dass an schnelle Datenverarbeitung nicht mehr zu denken ist.

Die „Log View“ Funktion ist eben eine Vorschau-Funktion, die nicht benutzt werden sollte, wenn niemand hinsieht.



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Zu viel Leerlauf bei Vorlauf / Rücklauf**

Bei verschiedenen Analyse-Funktionen unterbricht TraceMagic die Interpretation des aktuell erreichten LAN-Pakets, um im Trace vorwärts / rückwärts zu laufen (und dann zurück zu kehren).

Dies geschieht bei TCP-Retransmit-Analyse, und dies geschieht bei Client-Server-Analyse der „Server Error Return“ Szenarien („ACCESS\_FAILURE“).

Normalerweise geschieht bei dem ACCESS\_FAILURE Szenario folgendes:

**Beispiel 1:** Rücklauf bei ACCESS\_FAILURE

Die aktuell in Bearbeitung befindliche Datei enthält 100.000 LAN-Pakete.

TraceMagic ist bei Paket Nummer 45.000 angelangt und erkennt, dass ein Server dem Client einen Error-Code zurück gibt.

Sodann sucht TraceMagic den zugehörigen Client-Request und läuft hierzu in der Aufzeichnung rückwärts – und zwar (DEFAULT) bis zu LAN-Paket # 1.

Wenn nun häufiger zwar Server-Error-Replies zu sehen sind, die zugehörigen Client-Requests aber nicht im Trace sind (mögliche legale Gründe: HSRP, Load Balancing, Adapter Teaming), so führt dies zu erheblichem Zeitverlust:

Je weiter TraceMagic in der Trace-Datei nach hinten kommen (nahe 100.000 im Beispiel), um so mehr Wartezeit fällt an für den Trace-Rücklauf.

**Beispiel 2:** Vorlauf bei OPEN\_FILE

Ähnlich ist es, wenn TraceMagic in einem LAN-Paket den OpenFile()-Request eines Clients erkennt.

Dann läuft TraceMagic im Trace vorwärts, um den Server-Reply zu finden (zwecks Zuordnung des vom Client genannten Datei-Namens zum vom Server zurück gegebenen File Handle).

Auch hier gilt: Sind regelmäßig zwar solche Client-Requests da, aber keine Server-Replies, so akkumulieren sich erhebliche Leerlauf-Zeiten.

**Lösung:**

Die Vorlauf-Rücklauf-Funktion kann auf 1.000 oder 10.000 LAN-Pakete begrenzt werden. Hierzu ist vorzugehen wie auf den ScreenShots angezeigt.



## Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?

The screenshot shows the Trace:Magic software interface. At the top, the title bar reads "Trace:Analysis [Spider:Magic] -> D:\TRACES\2003\SYN.Eppingen.D\STACCCER\_01\b\TM.0003.SM.IP.SMB.NCP.HTTP.UNIX.Oracle.RC.DS.PS...". The main window has a title "Trace Analysis" and a close button "X SIOP". Below the title, there are several input fields and progress bars. A context menu is open over the "LIMIT: Rewind Limit (NCP/SMB/HTTP); (0)" field, which is circled in red. The menu options are:

- LIMIT: 0 = no limit = all packets
- LIMIT: max. 1 000 packets
- LIMIT: max. 10 000 packets

The menu also includes the text "TRACE FILE: Skip Frames = Skip File". Below the menu, the main interface shows a "Log View" section with "STOP (3)" and "START (4)" buttons. The log window displays several network events, including SMB transactions, TCP ACKs, and VRRP messages. At the bottom, there are status indicators: "[I] (99)", "68291", "Load File: OK", and "2183480".

Die Abbildung zeigt die Einstellungs-Möglichkeiten zur Begrenzung der Vorlauf-Rücklauf-Strecken.

Der rote Kreis zeigt, wie das PopUp-Fenster zu öffnen ist: Mit der Berührung des kleinen Mini-Buttons mit der Maus („MouseOver“).



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Zu viel Leerlauf in TCP-ReTx-Analyse**

Ähnlich den oben genannten Leerlauf-Szenarien innerhalb der Vorlauf-/Rücklauf-Funktionen verhält es sich bei der Analyse von TCP-Paketverlusten bzw. TCP-Retransmissions (TCP-ReTx).

Wenn beispielsweise (etwa bedingt durch "MAC Flooding") von verschiedenen TCP-Teilnehmern die TCP-Pakete jeweils nur in 1 Richtung in den MessDaten enthalten sind (Rx only / Tx only -> "one way only"), so läuft auch die TCP-ReTx-Analyse.

Desgleichen gibt es zum Teil extreme Verzögerungen, wenn mit Mirror-Port gearbeitet wurde und mehrere Client/Server/Uplink-Ports auf den Mirror-Port ausgespiegelt wurden; hierzu -> siehe unten.

Alle diese Einflüsse können zu äußerst schmerzlichen Verzögerungen in der Analyse führen.

Lösung:

Im Moment (TMv3): Keine. Es ist zur Zeit nicht abschließend geklärt, ob diesen Verzögerungen sinnvoll begegnet werden kann.

**Zu viele HTTP-Dialoge in TCP-ReTx-Analyse**

HTTP-Sitzungen zeichnen sich dadurch aus, dass nicht nur für jede HTTP-Seite (Web Page), sondern auch für jedes eingelagertes GIF, JPG etc. eine eigene TCP-Sitzung eröffnet wird.

Die TCP-ReTx-Analyse verlangt, dass alle TCP-Sitzungen getrennt betrachtet werden. Wegen des zum Teil starken Aufkommens von TCP-Sitzungen wegen Dutzender oder Hunderter parallel laufender HTTP-Zugriffe kann die TCP-ReTx-Analyse erheblich verzögert ablaufen.

In diesem Falle sollte die TCP-ReTx-Analyse unter Ausschluss von HTTP stattfinden. Eine entsprechende Konfigurations-Möglichkeit ist in SpiderMagic vorhanden.



---

**Tuning Trace:Magic ⇒ Was tun, wenn die Analyse langsam läuft ?**

---

**Mirror-Port: Mehrere Client/Server/Uplink-Ports auf Mirror-Port gespiegelt**

## Multi-Port Mirroring

Desgleichen gibt es zum Teil extreme Verzögerungen, wenn mit Mirror-Port gearbeitet wurde und mehrere Client/Server/Uplink-Ports auf den Mirror-Port ausgespiegelt wurden; dies kann dazu führen, dass LAN-Pakete bzw. TCP-Pakete doppelt in den MessDaten auftreten (bei Rx an Mirror-Port ausgegeben, dann bei Tx an Mirror-Port ausgegeben); die Erkennung, dass es sich hierbei **nicht** um TCP-ReTx handelt, sondern um gedoppelte Packets (TCP: Sequence Duplicated / Header Duplicated), kostet erhebliche Prozess-Zeit.

Es ist daher schon beim Einrichten des Mirror-Ports darauf zu achten, ob sich das Multi-Port-Mirroring in diesem Sinne "lohnt".

**Mirror-Port: Alle Daten eines VLANs werden auf den Mirror-Port gespiegelt**

## VLAN Mirroring

Hier verhält es sich wie bei Multi-Port-Mirroring. Das kann, aber muss nicht von Vorteil sein. Bei Einrichtung des Mirror-Ports bzw. des Messpunkts muss dies geprüft werden.

#