

SYNAPSE: NETWORKS

TRACE:MAGIC



Kurze Leistungsbeschreibung

Stand: 2004-09-16

Trace:Magic

Offline LAN-WAN Analysis Expert System - Reporting System - Knowledgebase

TraceMagic stellt in vielerlei Hinsicht einen neuen Meilenstein in der LAN-Analyse dar.

Ein paar der wesentlichen Highlights sind:

- Es können mehrere Gigabytes an Messdaten völlig automatisch ausgewertet werden. Damit können Messzeiträume von Stunden, wenn nicht Tagen, völlig automatisch analysiert werden. Diese Art von **Analysis Engine** ist weltweit zur Zeit ohne Konkurrenz.

TraceMagic verarbeitet die Capture-Files, die herkömmliche LAN-Analyser auf die Festplatte gebracht haben.

TraceMagic liefert selbst über Gigabyte-Mengen den Total-Befund, voll-automatisch.

- Alle LAN-Pakete, die zu Ereignis-Abläufen oder Fehlern im Sinne der Analyse gehören, werden aus den Original-Messdaten heraus gezogen und in neu erzeugte Trace-Dateien hinein kopiert. Auf diese Weise entsteht ein Substrat, das genau die Ereignisse und Fehler abbildet, die gesucht werden. Ausführliche **Event-Logs** unterstützen das durch lesbare Text-Dateien.

- Die Analyse kann eingeschränkt bzw. gesteuert werden über die **Filter Engine** von TraceMagic. Über 500 Filter-Kriterien können maximal über die Filter-Datenbank aktiviert und kombiniert werden.

- TraceMagic verfügt über ein hoch leistungsfähige **Report Engine**. Denn Analyse geschieht zu dem Zweck, am Ende unanfechtbare, vollständige und revisionsfähige Ergebnisse zu haben.

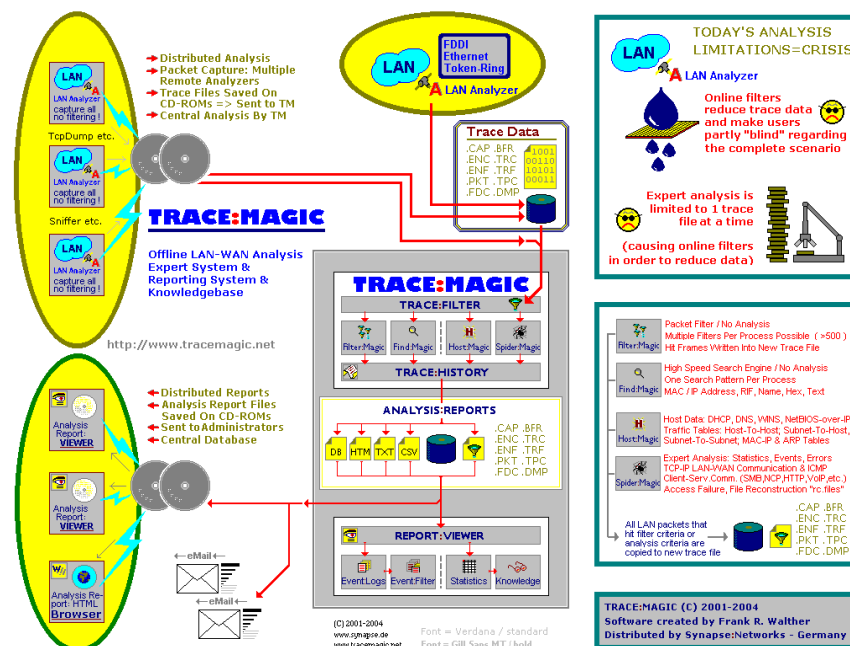
Über ein breites Spektrum von Ereignissen und Fehlern werden automatisch Berichte erzeugt.

- .TXT - lesbare Text-Dateien.
- .CSV - Tabellen (gedacht für MS-Excel und Makro-Verarbeitung)
- .HTML - voll indiziertes und über Links querverbundes Bericht-Projekt
- .DB - Datenbanken mit komplexen Ergebnis-Darstellungen

- Die Report-Ergebnisse, insbesondere die Report-Datenbanken, können über ein **lizenz-freies REPORT-VIEWER-Modul** durch beliebige Dritte betrachtet und weiter verarbeitet werden.

Dies schafft eine **universelle Schnittstelle für die Berichts-Auswertung und -Weitergabe**, zumal jeder Empfänger der Ergebnis-Daten auf die Knowledgebase (Wissens-Datenbank) zugreifen kann.

- Das **Datenfluss-Modell von TraceMagic** ist daher ebenso einfach wie effizient und universell (volle Größe der Grafik: siehe unten, am Fuß des Dokuments):



- Wirkung: **Arbeitszeit wird gespart, und Reaktionszeiten werden verkürzt.**

An zentraler Stelle werden die Messdaten des ganzen Unternehmens ausgewertet (keine oder kaum Handarbeit mehr!) - und die Ergebnis-Reports (Text, CSV, HTML, Datenbanken) werden verteilt an alle, die es betrifft.

- TraceMagic verfügt über eine **Knowledgebase**, die sowohl im Analyse-Modul wie auch im Viewer-Modul arbeitet.

Auf diese Weise wird der Analyse-Techniker unterstützt, desgleichen aber auch sämtliche Empfänger der Ergebnis-Reports.

- TraceMagic erkennt Fehler auf folgenden OSI-Schichten bzw. in folgenden Protokoll-Stapeln:

OSI Layer 1-2:

Fehler in der Physik, insbesondere versteckte Switch-Fehler.

Beispiel (in 2002 mehrfach festgestellt): Das automatische Vervielfältigen von LAN-Paketen durch Switch-Ports wird von TraceMagic vollständig erkannt.

OSI Layer 2 + SNA:

Die LLC-Dialog-Kontrolle samt einem darüber laufenden SNA-Protokoll werden umfangreich und automatisch analysiert. Für Banken und Versicherungen heute noch interessant.

OSI Layer 3 (Network):

IP-Routing-Fehler insbesondere auf WAN-Strecken werden selbst dann erkannt, wenn es sich um höchst versteckte Ereignisse handelt, die von anderen Analyzern nicht erkannt werden. Der Nachweis mangelhaft arbeitender Provider-Strecken gelingt mittels TraceMagic (fast) nahtlos.

Da WAN-Provider gerne die ICMP-Meldungen ihrer Router den Kunden gegenüber unterdrücken (durch Filter beim Übergang zum Campus-LAN des Kunden), können WAN-Fehler durch viele herkömmliche Analyser nicht mehr nachgewiesen werden, da sie zur Erkennung der WAN-Fehler auf eben diese ICMP-Meldungen angewiesen sind.

TraceMagic ist davon in weitem Umfang unabhängig und ermöglicht somit Nachweise, die sonst nicht mehr gegeben wären.

OSI Layer 4 (Transport):

Fehler in der Datenfluss-Kontrolle, im Dialog-Verhalten, im Sitzungs-Verhalten werden vollständig erkannt und in vielfacher Form ausgegeben (Text, CSV, Datenbank).

OSI Layer 5-7 (Name Services):

Mit hohem Anteil an Netzwerk-Fehlern sind die Microsoft Name-Services beteiligt (NetBIOS, WINS, DNS). TraceMagic ist die einzige Software, die hier gründlich aufräumt und die bislang versteckt ablaufenden Fehler sichtbar macht.

OSI Layer 7 (File Services, Application):

File Services:

Unterstützt werden die drei großen Client-Server-Protokolle:

- SMB (Windows, OS-2, Samba) (über LLC, NetBIOS, TCP/IP, Vines IP)
- NCP (Novell NetWare) (über IPX oder TCP/IP)
- HTTP (WWW, Internet)

Bislang war kaum bekannt, dass das Basis-Geschäft des lokalen Netzwerkes, die Datei-Dienste, ebenfalls bizarre Fehler aufweisen können, die bis zu Endlos-Schleifen und Programm-Abstürzen führen können. TraceMagic deckt diese Fehler auf und macht sie eingehender Untersuchung zugänglich.

File Reconstruction:

Neben der Analyse der Datei-Dienste ist TraceMagic in der Lage, den Inhalt der Dateien dokumentarisch zu rekonstruieren, die seitens der Clients auf den Servern gelesen werden. Dies ermöglicht Fehler-Erkennungen, die bislang nicht bekannt waren.

Script Follow-Up:

TraceMagic kann erkennen, ob der fehl geschlagene Zugriff eines Clients auf eine Server-Ressource auf eine zuvor geladene Script-Datei zurück zu führen ist (.BAT, .CMD, etc.). Diese Fähigkeit ist weltweit bislang einmalig.

ORACLE:

Eine Spezial-Funktion für die Oracle-Analyse erlaubt es, spezielle Fehler, die im Zusammenhang zwischen Oracle-TNS und TCP/IP-Ereignissen auftreten, nahtlos zu erkennen.

- TraceMagic verfügt vermutlich über **die ausgedehnteste TCP/IP-Analyse weltweit**, verglichen mit herkömmlichen LAN-Analysern. Über 200 Ereignis- und Fehler-Zähler werden je IP-Teilnehmer geführt und in den Berichten ausgegeben (Text, CSV, Datenbank) !

So wurden bereits im Dezember 2001 in einem der größten WANs Deutschland **die TCP/IP-Fehler von genau 22.661 IP-Teilnehmern automatisch erfasst und in Berichtsform ausgegeben!**

Im Februar 2004 wurde eine Name-Service-Analyse mit dem TraceMagic-Modul "HostMagic" durchgeführt - dabei wurden **binnen 32 Stunden 252 Mio LAN-Pakete verarbeitet!**

Diese Leistungskraft ist bisher völlig unerreicht und einmalig.

(Nur möglich mit der "Unlimited"-Lizenz.)

- TraceMagic verfügt als einziger Analyzer über **ausgedehnte Fähigkeiten, auf Layer 7 Applikations-Ereignisse und -Fehler zu erkennen**, auch in schwierigen Wechselwirkungen.

Die für MS-Windows typischen Fehler in den File Services, die kaum jemandem bislang bekannt waren (da sie von traditionellen Analyzern nur ungenügend sichtbar gemacht werden), werden weitgehend, wenn nicht gar vollständig aufgedeckt.

Auch bestimmte MS-Windows-Probleme in der Kompatibilität zwischen Client und Server (OS-Version, SP-Version) können durch TraceMagic sichtbar gemacht werden. Dies ist für Migrations-Verifikation (Change Management) von großer Bedeutung.

- Script Follow-Up: TraceMagic ist inzwischen in der Lage, Client-Zugriffe, die von Servern abgelehnt oder nicht bedient werden, auf zuvor geladene Script-Dateien zurück zu führen (etwa: .BAT, .CMD, .REG, Login Scripts).

- **TraceMagic automatisiert den Prozess der LAN-Analyse (fast) vollkommen.**

Sämtliche LAN-Pakete, die mit einem handelsüblichen Analyzer aufgenommen wurden (Sniffer, Observer, LANdecoder32, Ethereal, etc.) und in so genannten "Trace-Dateien" abgespeichert wurden, **werden vollkommen automatisch ausgewertet (mit Hinterlegung der Ergebnisse in abrufbaren Datenbanken).**

- Inzwischen haben sich in Deutschland Kunden wie die folgenden für TraceMagic entschieden:

- Bundesverteidigungsministerium (BMVg)
- Krauss-Maffei (Rüstung)
- DaimlerChrysler
- Ruhrgas AG
- Gelsenwasser AG
- T-Systems
- Bayerischer Rundfunk
- RBT - Rundfunk-Betriebs-Technik der öffentl.-rechtl. Sendeanstalten
- Bosch-Rexrodt
- Viessmann AG
- Nestlé Deutschland
- ERGO-Versicherungen
- Universitätsklinikum Düsseldorf
- Fachhochschule Merseburg
- ... und andere mehr

- Der erste veröffentlichte **Anwender-Bericht mit Erfahrungen zu TraceMagic** erschien in Oktober 2002 in der Zeitschrift "Network World" (Heft 19-2000):

"Netzwerk-Management und LAN-Analyse beim Bayerischen Rundfunk"

Network World (Germany), Heft 19-2002, 11. Okt. 2002

http://www.synapse.de/tracemagic/ger/htm/tracemagic_press_releases.htm

Zitat von Herrn Rennollet, dem Sachgebietsleiter beim Bayerischen Rundfunk:

"Dieses Expertensystem erleichtert unsere Arbeit erheblich. Es verkürzt den Zeitaufwand für die Fehlersuche und lässt sich sehr schnell produktiv einsetzen. Auch für nicht speziell geschulte Netzwerk-Administratoren ist es möglich, mit TraceMagic rasch gute Ergebnisse zu erzielen."

"Sehr wichtig ist für uns die Rationalisierung: Ich habe insgesamt neun interne und externe Mitarbeiter, die ein Netz mit rund 5000 Nodes betreuen. Deshalb brauchen wir möglichst einfache, aber dennoch aussagekräftige Analysen auf Knopfdruck."

(Zitat: Network World, 11. Nov. 2002, Heft 19-2002)

- **Die TraceMagic-Referenz ist im Standard-Werk "Networkers's Guide" veröffentlicht.**

Networker's Guide (Autor: Frank R. Walther; Verlag: Markt+Technik, München 2003):

In diesem Standard-Werk (2. Auflage 2003) ist die Arbeitsweise von TraceMagic sehr weitreichend beschrieben, von der Installation bis zur TCP/IP- und Applikations-Analyse, einschließlich ausführlicher Praxis-Beispiele etwa zu Windows-XP oder Voice-over-IP.



- **FAZIT: Mit TraceMagic lässt sich ZEIT + GELD sparen.**

Beispiel:

An einer zentralen Stelle steht eine schnelle Auswertungs-Maschine mit TraceMagic.

Von beliebigen Außenstellen oder Abteilungen werden Messdaten zur Untersuchung an die Zentrale geschickt.

Bevor die Messdaten überhaupt manuell angefasst werden (was viel zu viel Zeit kostet und fehlerhaft ist, da unvollständig), werden die Messdaten durch TraceMagic geschickt.

Die automatisch erzeugten Reports können schnell überblickt, kommentiert und weiter gegeben / zurück gegeben werden.

Da TraceMagic in der Lage ist, nicht nur komplexe Auswertungen in den Bereichen TCP/IP, Name Services, File Services, Applications durchzuführen, sondern auch benutzer-definierte Filter anzuwenden (über 500 Filter-Kriterien sind in der Filter-Datenbank aktivierbar und kombinierbar!), können beliebige LAN-Packets selbst aus Hunderten von Trace-Files nachträglich heraus gezogen werden, und das sogar mit äußerst hoher Geschwindigkeit.

TraceMagic ersetzt somit das Stichproben-Prinzip, das bis dato überall angewendet wurde, mit dem Total-Befund, indem über den gesamten Netzwerk-Traffic von Stunden oder Tagen die automatische Analyse betrieben werden kann. Denn bis heute ist es bei Analyzern wie Sniffer (und anderen) so: Das Offline-Experten-System kann immer nur eine (in Worten: 1) Trace-Datei zur selben Zeit auswerten. Bei Hunderten von Trace-Files, die auf Gigabit-Leitungen pro Stunde anfallen können, ergibt eine solche Auswertungsform einfach keinen Sinn mehr. TraceMagic ist die natürliche und zwangsläufige Alternative.

In der Vergangenheit hat die Unfähigkeit der Analyzer, mehr als 1 Trace-Datei zur selben Zeit im Experten-System zu verarbeiten, dazu geführt, dass die Techniker beim Packet-Capture mit Online-Filtern arbeiteten, um die resultierende Datenmenge klein zu halten. Das ist untragbar, weil die Messergebnisse somit nur noch rein zufällig 100% zuverlässige Befunde liefern können.

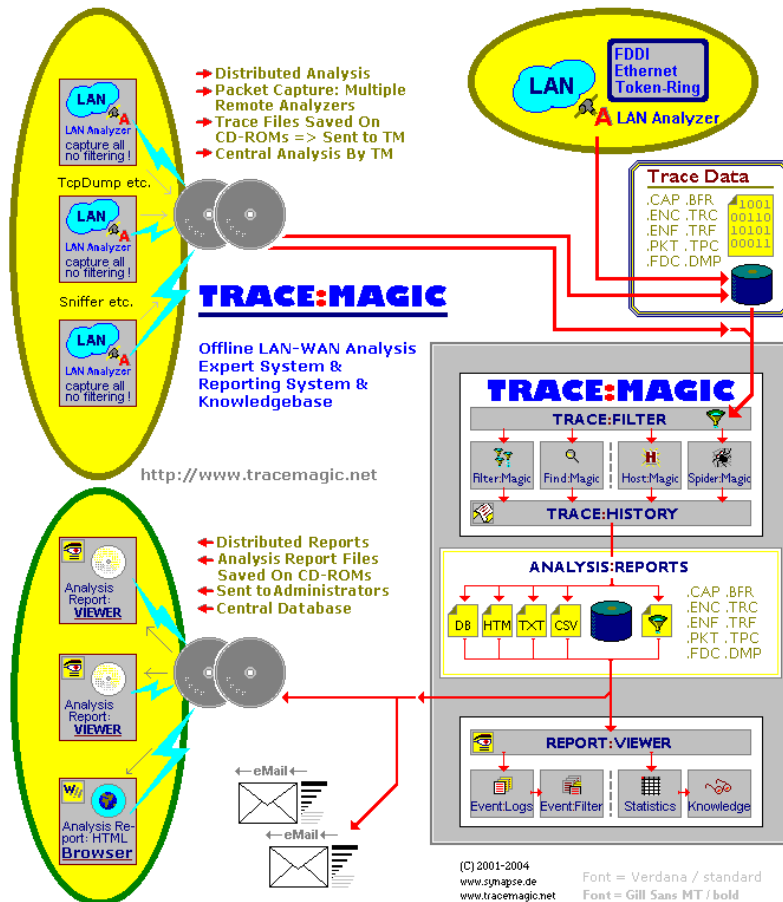
TraceMagic erlaubt nunmehr, bei der Messung online *ohne* jeglichen Filter zu arbeiten. Die automatische Total-Verarbeitung hinterher entlastet den Techniker, und die Befunde sind umfassend, lückenlos und revisionssicher.

Externe Dienstleister und die Lieferanten werden nunmehr mit exakten Ergebnissen versorgt. Das bekannte "Schwarze-Peter-Spiel" hat sofort ein Ende. Auf klarer Faktenbasis wird eben gehandelt, und nicht mehr lamentiert.

TraceMagic im Internet:

<http://www.tracemagic.net/>

Synapse:Networks GmbH
 Bonner Str. 10
 53424 Rolandseck bei Bonn
 +49. 2228. 9138.0 - phone
 +49. 2228. 9138.99 - fax
 +49. 170. 7334608 - mobile
 +49. 171. 7421000 - mobile
<http://www.synapse.de/>
info@synapse.de



TODAY'S ANALYSIS LIMITATIONS=CRISIS

LAN
 LAN Analyzer

Online filters reduce trace data and make users partly "blind" regarding the complete scenario

Expert analysis is limited to 1 trace file at a time (causing online filters in order to reduce data)

Filter:Magic Packet Filter / No Analysis
 Multiple Filters Per Process Possible (>500)
 Hit Frames Written Into New Trace File

Find:Magic High Speed Search Engine / No Analysis
 One Search Pattern Per Process
 MAC / IP Address, RIF, Name, Hex, Text

Host:Magic Host Data: DHCP, DNS, WINS, NetBIOS-over-IP
 Traffic Tables: Host-To-Host, Subnet-To-Host, Subnet-To-Subnet, MAC-IP & ARP Tables

Spider:Magic Expert Analysis: Statistics, Events, Errors
 TCP-IP LAN-WAN Communication & ICMP
 Client-Serv Comm. (SMB, NCP, HTTP, VoIP, etc.)
 Access Failure, File Reconstruction "rc.files"

All LAN packets that hit filter criteria or analysis criteria are copied to new trace file

.CAP, .BFR, .ENC, .TRC, .ENF, .TRF, .PKT, .TPC, .FDC, .DMP

TRACE:MAGIC (C) 2001-2004
 Software created by Frank R. Walther
 Distributed by Synapse:Networks - Germany