Warum LAN-WAN-Analyse mit Synapse:Networks ?

Theorie und Praxis
in der Anwendung von

TraceCommander – MiniMagic - TraceMagic

© Frank R. Walther / 2007-04-22

Trace:Commander - Mini:Magic - Trace:Magic

im Urteil der Fachpresse und der Kunden:

• • •

"Das momentan am Markt beste Expertensystem nach Meinung des Autors ist das relativ unbekannte TraceMagic."

Loseblatt-Sammlung **„LAN-Analyse & Troubleshooting"** (WEKA **2007**, 3/5.6, S.4).

• • •

"Gestern habe ich mit dem mobilen Shuttle eine Messung angestoßen (TraceCommander und MiniMagic). Diese lief von gestern 10:00 Uhr bis heute früh 08:30. Dabei wurden 2183 Dump Files mit einem Gesamtvolumen von 77 GB erzeugt. MiniMagic war jetzt beim 2100 Dump File. Es ist also gut nachgekommen und lief stabil durch. Super."

Urteil des Synapse-Kunden **Swisscom** aus März **2007** über den ersten Einsatz der Synapse-Technik für Dauermessungen. Inzwischen befinden sich die Mess-Systeme im Dauer-Einsatz.

• • •

"Die Kombination aus Trace:Commander / Mini:Magic / Trace:Magic ist das Beste, was ich im Bereich der IT-Systemanalyse je gesehen habe. In kürzester Zeit habe ich aussagekräftige Ergebnisse! Herkömmliche Tools versagen hier."

Aussage eines Kunden im April **2007** (der Kunde ist ein weltweit tätiges Maschinenbau-Unternehmen).

• • •

Synapse:Networks GmbH

Synapse:Networks bietet seit 1992 Dienstleistungen der LAN-Analyse und seit 1996 eigene Software zur Auswertung von Analyse-Messdaten.

- Es ist kein weiteres Unternehmen bekannt, das ausschließlich LAN-Analyse betreibt und somit als Spezialist das nötige Know-How erworben hat und finanziell unabhängig ist von großen Marktteilnehmern.
- In der Person von Frank R. Walther ist Synapse:Networks der dienstälteste Anbieter von LAN-Analyse in Deutschland in ununterbrochener persönlicher Kontinuität.
- In der Person von Frank R. Walther stellt Synapse:Networks den Autor der einschlägigen Fachliteratur: Networker's Guide (2000,2003), Registriy Guide (2001).
- Mit den Analyse-Programmen TraceCommander, **Mini:Magic** und **Trace:Magic** verfügt Synapse:Networks über einen derzeit uneinholbaren Vorsprung gegenüber sämtlichen Mitbewerbern.

Trace:Commander → Aufzeichnung von Capture-Files

Mini:Magic → Online-Analyse / Schnell-Auswertung
Trace:Magic → Offline-Analyse / Detail-Auswertung

Am Markt verfügbare bzw. übliche Mittel+Methoden

Nur wenige Marktteilnehmer bieten LAN-Analyse ähnlich lang oder länger auf dem Markt an als Synapse:Networks. Massive Einschränkungen:

- Es ist kein weiterer Dienstleister bekannt, dessen Personal 15 Jahre oder mehr an ununterbrochener Kontinuität in der Beschäftigung mit LAN-Analyse aufweisen könnte.
- Allgemein sind die auftretenden LAN-Analysten nicht mit einer Erfahrung ausgestattet, die über viele Generationen von Betriebssystemen und LAN-Verfahren hinweg reicht.
- Soweit bekannt, ist kein weiterer Dienstleister neben Synapse:Networks vollständig auf LAN-Analyse spezialisiert und somit unabhängig. Vielmehr bieten andere Dienstleister selber die Hardware/Software an, deren Fehler es zu analysieren gilt. Interessen-Konflikte können somit kaum ausgeschlossen werden.
- Andere Dienstleister verwenden am Markt verfügbare Analyse-Werkzeuge und sind von ihnen abhängig. Sie sind folglich methodisch eingeschränkt.

Die Aufzeichnung von Messdaten findet bei Synapse:Networks mit eigener Software statt, dem TraceCommander.

- TraceCommander nutzt am Markt verfügbare Hardware sowie die anerkannt guten Capture-Module WinPCap/TShark – jedoch nur auf Treiber- und Capture-Ebene, nicht auf Anwendungsebene.
- TraceCommander steuert selbst die Aufzeichnung der Messdaten durch WinPCap/TShark und verwaltet die aufgezeichneten Messdaten eigenständig, einschließlich der Online-Auswertung mittels MiniMagic.
- TraceCommander verfügt über einen „Capture Scheduler" zur genauen Steuerung der Aufzeichnungs-Zeiten. So kann beispielsweise vermieden werden, dass Backup-Streams, die nachts oder am Wochenende über den Messpunkt fließen, in die Analyse-Aufzeichnungen einfließen.
- TraceCommander verfügt über einen „Link+Capture Test", der den Messpunkt automatisch nach einer Vielzahl von Kriterien dahin gehend bewertet, ob der Messpunkt (Mirror Port) korrekt konfiguriert wurde.
- TraceCommander verfügt über sein Modul „MiniMagic" über die Fähigkeit zeitnaher Schnell-Auswertung. Etwa 60-70% der häufigsten Performance-Killer werden so bereits nach kurzer Zeit nachweisbar. „MiniMagic" ist vom eigentlichen Experten-System „TraceMagic" (s.u.) entlehnt und wurde gezielt für Schnell-Auswertungen unter Online-Bedingungen entwickelt.
- TraceCommander kann endlos (über Monate hinweg) permanent aufzeichnen und auswerten.

Die Aufzeichnung und Auswertung von Messdaten findet beim Mitbewerb erfahrungsgemäß wie folgt statt:

- Die zur Aufzeichnung verwendeten LAN-Analyzer können zwar für die Aufzeichnung großer Datenmengen eingesetzt werden, verfügen aber über keinerlei Fähigkeit, die Messdaten online oder offline im Umfang 5-6 stelliger GB-Volumina auszuwerten.
- Online findet allgemein eine um leichte logische Funktionen verbesserte Statistik statt, die nicht wirklich als Experten-Analyse bezeichnet werden kann.
- Offline kann immer nur 1 (!) Aufzeichnungs-Datei zur selben Zeit ausgewertet werden, was angesichts von Mengen von oft 1.000 Dateien und mehr an Ineffizienz kaum mehr zu überbieten ist.
- Die am Markt gängigen Analyzer sind überwiegend (oder gar sämtlich) nicht in der Lage, bestimmte Tages- oder Wochenzeiten auszusparen, um z.B. Backup-Streams auszuschließen.
- Die sog. Experten-Systeme enthalten teils kaum, teils so gut wie nie Erkennungs-Mechanismen aktueller Fehler insbesondere aus dem Microsoft/Windows-Umfeld. Bei einem Entwicklungs-Zyklus von 18 Monaten und mehr „lohnt" es sich nicht für die Hersteller (Open-Source-Entwickler eingeschlossen), z.B. ServicePack-bezogene Fehler-Erkennungs-Bibliotheken zu entwickeln, da zum Zeitpunkt ihres Erscheinens (nach aufwendiger Projektierung, Programmierung, Beta-Testung) Microsoft allgemein schon einige ServicePacks oder Betriebssystems-Stufen weiter ist. Damit geht aber der Wert dieser Analyzer in der Fehler-Situation praktisch vollständig verloren.

- TraceCommander kann mit seinem Modul „MiniMagic" praktisch unbegrenzt Messdaten bis in den Terabyte-Bereich hinein auswerten; hierbei können Filter gesetzt und Reports erzeugt werden.

- TraceCommander erzeugt HTML-Reports, die (je nach Konfiguration) von außen abfragbar sind.

- TraceCommander, MiniMagic und TraceMagic werden zeitnah in ihren Fehler-Erkennungs-Bibliotheken ergänzt, um aktuelle Fehler-Szenarien nachweisen zu können.

Die Auswertung von Messdaten findet bei Synapse:Networks teils online statt (TraceCommander mit MiniMagic), teils offline mit TraceMagic.

- TraceMagic ist laut Loseblatt-Sammlung „LAN-Analyse & Troubleshooting" (WEKA/Interest 2005) das führende Werkzeug:

  <<Das momentan am Markt beste Expertensystem nach Meinung des Autors ist (..) TraceMagic.>> (3/5.6 S.4 - 2005)

- TraceMagic verfügt über genau die Fähigkeiten, die sonstigen LAN-Analyzern fehlen: TraceMagic kann extreme Mengen von MessDaten automatisch verarbeiten und automatisch ebenso extrem umfangreiche und genaue Reports erzeugen.

- TraceMagic wird sehr zeitnah den Fehler-Zyklen angepasst, die sich in Hardware (z.B. Adapter-Teaming) und Software (z.B. Microsoft/Windows-Umgebung) ergeben. Es verfügt somit über Fähigkeiten, völlig neu aufkommende Fehler zu erkennen, wo andere Entwickler/Hersteller gezielt davon Abstand nehmen, derlei Aktualisierungen der Experten-Systeme vorzunehmen (zu lange Entwicklungs-Zyklen).

- Die Abhängigkeit von manueller Durchsicht von Messdaten bzw. das Fehlen automatischer Auswertung von Langzeit-Messungen macht es bei herkömmlichen Verfahren kaum möglich, Fehler zu identifizieren, die nur sporadisch auftreten. Viele Fehler insbesondere der Microsoft/Windows-Umgebung treten jedoch nicht ständig auf, sondern sind von bestimmten (wechselnden) Betriebszuständen abhängig. Manuelles Durchsuchen mikroskopisch kleiner Stichproben darf getrost als praktisch hoffnungslos angesehen werden.

- Die am Markt gängigen Analyzer erzeugen keine Reports, mit denen die Ergebnisse von Langzeit- und/oder Detail-Auswertungen belegt werden könnten. So gut wie alle Ergebnisse müssen entweder mündlich vermittelt werden oder in Form von ScreenShots.

- Folglich sieht es so aus: Es wird automatisch nur mit wenig aussagekräftigen Statistiken gearbeitet, und Experten-Analyse findet manuell in mikroskopisch kleinen Stichproben statt – was kaum geeignet ist, zu repräsentativen Befunden zu kommen, und was nur selten die Frage der Verantwortlichen beantwortet, ob größere Finanzmittel für umfangreiche Reparatur-Vorhaben auch wirklich als gerechtfertigt angesehen werden dürfen.

(TraceMagic hat keine Entsprechung beim Mitbewerb)

Praxis der Messung: Synapse:Networks ist leistungsfähiger - und trotz scheinbar höherer Honorare oft günstiger im Preis-Leistungs-Verhältnis.

- Synapse:Networks kann mit einem einzigen LAN-Analysten vor Ort 6-8 Messpunkte errichten und bereits am Ende des ersten Tages sehr umfangreiche und in die Tiefe gehende Berichte von allen Messpunkten vorlegen.

- Über die Technik der sog. „TC:PingNotes" können Anwender während der Messung Fehler-Meldungen versenden, die u.a. als „Lesezeichen" direkt in die Messdaten hinein geschrieben werden.

- Falls Zeit=Geld ist, wenn also die Geschwindigkeit einer umfassenden Analyse eine Rolle spielt, hat Synapse:Networks eine sonst nicht erreichte Leistungsfähigkeit.

- Diese Methode und Fähigkeit, vor Ort schnellstmöglich binnen weniger Stunden bereits 70-80% der später insgesamt vorgelegten Befunde zu erkennen, hat eine von Synapse:Networks beim Deutschen Marken- und Patentamt eingetragene Schutzmarke:

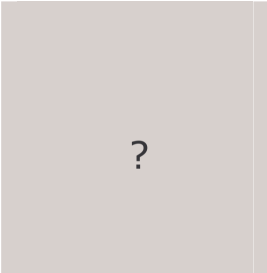
  Prima Vista Analyse *-> auf den ersten Blick sehen, was ist*

Am Markt tätige Mitbewerber sind nur auf den ersten Blick preiswerter; auf den zweiten Blick offenbaren sich schwere Zweifel am Preis-Leistungs-Gefüge.

- Da Analyse jenseits der wenig aussagefähigen Online-Statistiken wesentlich auf manueller Handarbeit beruht, müssen entweder vor Ort mehrere Techniker pro Tag anwesend sein, um die verschiedenen Messpunkte zu betreuen (was die Zahl der Techniker pro Tag erhöht), oder ein einziger Techniker kann nur 1-2 Messpunkte betreuen (was die Zahl der Tage pro Techniker erhöht).

- Anwender können sich bestenfalls telefonisch oder per Mail bemerkbar machen; die Fundstellen in den Messdaten müssen aufwendig identifiziert werden.

- Falls Zeit=Geld ist, verstreicht auf diese Weise zu viel Zeit, wodurch andauernde Fehler zusätzliches Geld kosten.



Praxis der Berichte: Analyse ist nicht alles. Die Ergebnisse müssen vermittelt werden, um Wirkung zu zeigen.

Synapse:Networks hat hier eine eigene, hoch wirksame Methode entwickelt.

- An jedem Tag vor Ort wird Bericht erstattet, jeweils nachmittags.
- Die Bericht-Erstattung findet in Konferenz-Räumen mit Video-Beamer statt. Neben den Netzwerk-Administratoren sind Client/Server-Admins, Datenbank-Admins etc. anwesend. Nur integriertes Wissen ist gutes Wissen.
- Alle betroffenen Kollegen bringen ihr Wissen ein, es fließt unmittelbar in den per Beamer gezeigten Bericht ein.
- Umfangreiche Datenbank-, Filter- und Suchfunktionen der Software TraceMagic erlauben es, sofort auf Zuruf beliebigen Fragen nachzugehen und Vermutungen zu bestätigen oder zu widerlegen.
- Durch die Teilnahme aller relevanten Kollegen auf seiten des Kunden hat der resultierende Bericht volle Akzeptanz und wird sofort umgesetzt. (Kein Schwarze-Peter-Spiel.)
- Jeder Teilnehmer kann per USB-Stick den Bericht im sog. TraceMagic-„MemoReader"-Format mitnehmen.

Am Markt tätige Mitbewerber legen Berichte allgemein nicht nur Tage, sondern Wochen später als Synapse:Networks vor, wobei nur Stichproben der Messdaten untersucht wurden. Doch welche Bedeutung haben die Berichte?

- Umfangreiche, auf einer breiten Datenbasis beruhenden Berichte gibt es entweder gar nicht, oder erst Wochen später (bei Synapse:Networks sofort am ersten Tag vor Ort).
- Die Berichte sind überlicherweise in MS-Word geschrieben, hier und da sind Statistiken und ScreenShots aufgenommen. Eine Berichtsform, die datenbank-gestützt mit Tabellen-, Filter- und Suchfunktionen arbeiten würde und freies Assoziieren erlauben würde, ist nicht gegeben.
- Da die Berichte erst lange nach der Messung vorgelegt werden, ist es allgemein schwierig, zur Besprechung die erforderlichen Kollegen kundenseitig einzubinden: Während im Zuge der Messung die verantwortlichen Administratoren erfahrungsgemäß anwesend sind (und folglich zur Berichts-Diskussion zur Verfügung stünden), muss erneut um Termine und Zeiten gerungen werden.
- Da die MS-Word-Berichte nicht interaktiv sind, können kaum das Wissen und die Ansichten der Kollegen eingebunden werden. Entsprechend niedrig fällg oft die Akzeptanz der Berichte aus.
- Folge: Oft werden die Ergebnisse nicht oder nur kaum umgesetzt.

Niedrige Preise? Auch das ist mit Synapse:Networks machbar, und zwar radikal niedriger als beim Mitbewerb.

- Über die mittels TraceCommander/MiniMagic und TraceMagic gegebene Fähigkeit, Messdaten offline (also nachträglich) auszuwerten, kann Synapse:Networks einmalig preisgünstige Angebote unterbreiten:
- Der Kunde zeichnet die Messdaten selber auf. Die hierzu erforderliche Software TraceCommander ist mit seinem Aufzeichnungs-Modul „Capture Wizard" kostenfrei.
- Die erste Vorab-Auswertung kann der Kunde auf Wunsch selbst vornehmen mit dem TraceCommander-Modul „MiniMagic" (Lizenz-Preise: 300 EUR bis 1.200 EUR).
- Erst bei einzelner Veranlassung sendet der Kunde die Messdaten an Synapse:Networks zwecks Auswertung durch TraceMagic und Durchsicht/Kommentierung durch die Spezialisten.
- Synpase Networks gibt den Bericht im Format des TraceMagic-MemoReaders zurück.
- Mit einer Internet-Video-Konferenz (Plattform: Netviewer) wird im Gruppen-Gespräch unter Einschluss aller Administratoren (s.o.) das Ergebnis erläutert, werden die Faktenkenntnis und Erfahrungen der Kunden-Admins zusätzlich aktiviert.
- Folge: Nicht der Mann fährt zu den Daten (keine teuren Manntage vor Ort), sondern die Daten kommen zum Mann.

Auf diese Weise kann Synapse:Networks Gründlichkeit und Effizienz zu nicht mehr schlagbaren Konditionen anbieten.

Nur beim Manntag vor Ort scheint es auf den ersten Blick so, als seien Mitbewerber preiswerter.

- Da die allgemein vom Mitbewerb verwendeten LAN-Analyzer lange Zeiträume im Datenverkehr nur online in Form der Echtzeit-Statistiken erfassen bzw. im Ergebnis aggregieren können, erfordert diese Herangehensweise in erheblichem Umfang den Einsatz von Technikern vor Ort. Folge: Teure Manntage, immer wieder.
- Die mangelnde Fähigkeit, große Datenmengen automatisch zu verarbeiten, zwingt zu manueller Durchsicht. Dies erhöht die Kosten, da Manntage teurer sind als Maschinenlaufzeiten.
- Die mangelnden Fähigkeiten der gängigen LAN-Analyzer, komplexe Fehler z.B. in Active-Directory-Umgebungen zu finden, zwingt weiterhin zu vermehrter manueller Arbeit in den Messdaten. Folge: Noch höhere Personalkosten, noch längere Wartezeiten.

Folge: In Regeldienstleistungen (also regelmäßig erbrachten Services statt sporadischen Notfall-Einsätzen) haben die am Markt gängigen Mechanismen sowohl technisch wie auch kaufmännisch/preislich das Nachsehen.

Entsprechend wird LAN-Analyse selten wirklich professionell betrieben. Die oft große Personal-Fluktuation bei Dienstleistern sorgt zudem oft noch zusätzlich dafür, dass nur wenig Expertise einfließt.

Referenzen:

Bundesministerien und Bundesbehörden
Öffentlich-Rechtliche Institute / Rundfunk+Fernsehen
Stadtverwaltungen und Stadtwerke
Polizei-Präsidien und Landeskriminalämter
Kfz-Hersteller / Zulieferer / Just-In-Time Industrie / Rüstungsbetriebe
Dt.Bundesbank; Sparkassen; Banken des In- und Auslandes
Telekom-Unternehmen / IT-Dienstleister des In- und Auslandes

… und andere mehr

Ansprechpartner:

Auf Wunsch vermitteln wir Ihnen Ansprechpartner bei einem unserer Kunden, damit Sie sich aus erster Hand ein eigenes Bild über unsere Arbeitsweisen und deren Leistungsfähigkeit machen können.

Sprechen Sie uns an!

Quellen zum Thema

http://www.synapse.de/

http://www.tracemagic.net/
http://www.tracecommander.net/
http://www.prima-vista-analyse.de/

http://www.registryguide.de/
http://www.networkersguide.de/

Rechte

Alle Rechte bei:

© 2007 Synapse:Networks GmbH / Frank R. Walther

Veröffentlichung und Wiedergabe, auch auszugsweise, nur mit Genehmigung des Autors.

Weitergabe nur in unveränderter Form (ohne Kürzungen, Erweiterungen, Änderungen) und unter Nennung der Quelle.

#