Retrospektive

Netzwerk-Analyse mit GigaStor

Rewind. Review. Resolve.

Lösungen für komplexe Rechner - Netzwerke.

GORDION®

GORDION
Data Systems Technology GmbH
Mottmannstraße 13
53842 Troisdorf

Telefon: 02241 49040
Telefax: 02241 490490

Email: info@gordion.de
Internet: www.gordion.de

GORDION LAN / WAN SECURITY ANALYZING

Retrospektive Netzwerk-Analyse mit GigaStor

Selbst ein partieller Ausfall des Netzwerks für einen nur kurzen Zeitraum kann in Kosten von mehreren Tausend Euro resultieren.

Das GigaStor-System von Network Instruments ermöglicht eine Retrospektive Netzwerk-Analyse (RNA) und verkürzt Fehlersuche, Ursachen-Ermittlung und Fehlerbehebung erheblich.

Von Oliver Lindlar und Mirco Jakuszeit, GORDION.

Störungen in Netz und Applikationen können vielseitig auftreten.

Die Netzwerk-Kommunikation und damit der Zugriff auf Server, Daten und Applikationen muss heutzutage reibungslos funktionieren. Optimalerweise ohne Störungen und am besten hochverfügbar. Ein performantes und hochverfügbares Daten-Netzwerk ist branchenübergreifend die Basis für moderne Geschäftsprozesse und -Kommunikationen sowie deren Applikationen. Die Mehrheit der Dienste und Applikationen, darunter auch VoIP / Audio / Video, nutzt mittlerweile das (Ethernet-) Netzwerk als Kommunikations-Infrastruktur. Während es noch vor einigen Jahren in Unternehmen und Organisationen durchaus denkbar war, dass z.B. der Email-Dienst für einen Tag ausfällt oder eine Applikation für Mitarbeiter nicht erreichbar ist, wirken sich solche Szenarien heute meist sehr empfindlich auf die Geschäftsprozesse aus und verursachen signifikante Kosten.

Aus diesem Grund verfügen moderne Netzwerke u.a. über ein redundantes Core- und Server-Switch-System, welches im Störungsfall einer zentralen Komponente weiterhin den Zugriff auf die Server / Daten / Applikationen ermöglicht (no single point of failure, gleiches gilt analog für Firewalls u.a. unternehmenskritische Komponenten). Darüber hinaus ermöglichen Netzwerk-Management-Lösungen einen Gesamtüberblick und melden Störungen von Komponenten und Systemen umgehend an die verantwortlichen Administratoren.

Der Klassiker: „Das Netz ist langsam."

Neben den meist eindeutigen Störungsmeldungen aus dem Netzwerk-Management-System gibt es leider auch eine Vielfalt an „schwammigen" Störungsmeldungen. Oft kommuniziert durch die User, wie z.B. der Klassiker: „Das Netz ist langsam." Oder „Mein Programm ABC reagiert nicht mehr". Noch ungünstiger sind Meldungen wie „Das Netz war gestern langsam" oder „Heute morgen reagierte mein Programm ABC nicht mehr". Der Ausfall von Voice over IP (VoIP), eine nicht erreichbare Serverfarm / Datenbank oder eine stehende Produktion aufgrund einer Netzwerkanomalie sind dagegen durchaus konkrete, unternehmenskritische Störungen und verursachen sofort Ausfallkosten.

Zeigt in solchen Fällen das Netzwerk-Management-System keine korrelierende Anomalie, kann die Fehlerbehebung erheblich Zeit beanspruchen. Wie geht man dann der Ursache für kritische Störungsmeldungen auf den Grund? Wie ermittelt man ad hoc mit ein paar Mausklicks die Ursache und behebt in kürzester Zeit das Problem? Wie hoch steigern sich die Kosten für den Fall, dass eine komplette Abteilung, Produktionshalle oder Aussenstelle von einer Störung / Downtime betroffen ist?

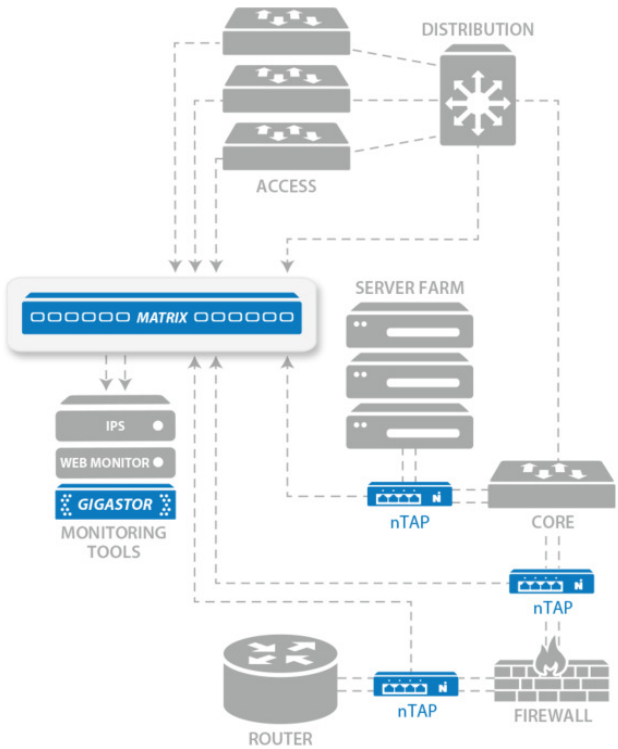


Abb.-1: Exemplarischer Einsatz von nTAPs, Matrix-Switch und GigaStor zur Retrospektiven Netzwerk-Analyse (RNA).

Netzwerk-Analyse meist erforderlich für eine schnelle Lösung

Zur schnellen Problemlösung ist meist eine Netzwerk-Analyse erforderlich, mit Fokus auf die detaillierte Datenkommunikation. Vorzugsweise retrospektiv, also mit „Blick in die Vergangenheit". Wir beleuchten daher nachfolgend das Potential einer Retrospektiven Netzwerk-Analyse (RNA) und zeigen die Möglichkeiten einer schnellstmöglichen Aufdeckung und Lösung von Netzwerk- / Server- / Applikations-Problemen. Ein entsprechendes System zur RNA bietet der Hersteller Network Instruments mit der GigaStor-Technologie. Die GigaStor ermöglicht mittels Zeitnavigation und per Drill-Down-Mausklicks die schnelle Ermittlung eines Fehlers und unterstützt durch ihre Langzeit-Datenerfassung eine proaktive Lösung von Problemen, insbesondere bei sporadischen Fehlerbildern.

Retrospektive Netzwerk-Analyse (RNA) mit GigaStor

Vergleichbar mit 24/7 Kameraüberwachung für das Netzwerk

Die GigaStor erfasst und speichert jedes übertragene Paket von geeigneten Messpunkten im Netz (vgl. Kasten rechts und Abb.-3) und ermöglicht so ein einfaches „Zurückspulen" der Datenkommunikation im Rahmen der Retrospektiven Netzwerk-Analyse (RNA) zur Ermittlung von Netz-, Applikations- oder Security-Problemen. Die RNA ist vergleichbar mit einer 24/7 Kameraüberwachung für das Netzwerk. Die RNA erlaubt ein „Zurückspulen" in problematische Szenarien und zeigt auf, was vor, während, und nach einer Netzwerk-Anomalie vorgefallen ist.

Die GigaStor-Technologie unterstützt Ethernet-Schnittstellen bis 40Gbps auf Basis einer eigenentwickelten Gen2-Erfassungskarte und ermöglicht eine Aufzeichnungskapazität von bis zu 576 TB. In Kombination mit der GigaStor-Zeitnavigation kann unmittelbar nach einer Problemmeldung mit der Fehler-Analyse begonnen werden. Eine zeitaufwändige Nachstellung von Problemen entfällt (vgl. auch Übersicht in Abb.-4 und Abb.-5 auf Seite 7/8).

Beispiel mit GigaStor

Neun Schritte zur Lösung — per Drill-Down

In dem folgenden Beispiel wird exemplarisch beschrieben, wie mittels GigaStor und RNA innerhalb von nur neun Schritten eine typische Störung identifiziert und lokalisiert werden kann. Im folgenden Beispiel erhält der Netzwerk-Verantwortliche an einem Nachmittag die „schwammige" Fehler-Meldung eines Users: „Meine Web-Anwendung ist seit ca. 12:30 Uhr langsam". Das Unternehmen verfügt über das o.g. GigaStor Analyse-System von Network Instruments, welches die Netzwerkdaten an vorab definierten Messpunkten permanent aufzeichnet.

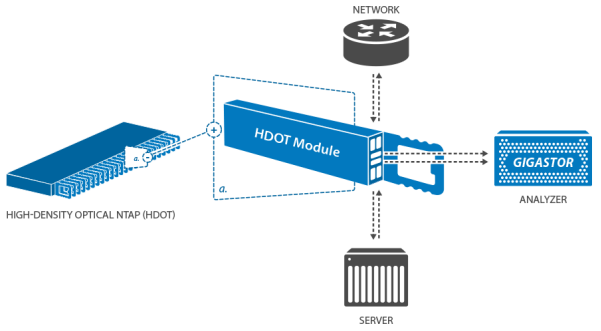


Abbildung-2: Traffic-Schema für High Density Optical nTAP (HDOT)

Zugriff auf Daten — Geeignete Messpunkte für Analysedaten

Die Analyse von Netzwerkdaten bedingt notwendigerweise einen Zugriff auf die Datenkommunikation. Einen geeigneten Zugriff auf die spezifischen Parameter der Netzwerkkommunikation, welche Aufschluss darüber geben, ob, wo und welche Fehler im Netz auftreten.

Geeignete Messpunkte sind insbesondere Punkte zwischen Servern und Clients oder am Übergabepunkt RZ↔Router. Oft werden SPAN- (Mirror-/ Spiegel-) Ports der Switches genutzt, um einen zu analysierenden Datenstrom mittels Analysator „abzuzapfen". Besser geeignet sind jedoch fest installierte TAPs, welche im Gegensatz zu SPAN-Ports die Abnahme eines Full-Duplex-Datenstroms zum Analysator ermöglichen und insbesondere auch evtl. physikalische Fehler der Leitung übertragen (vgl. Abbildung-2).

Vorteile durch Messpunkt-Realisierung mit TAPs (Test Access Ports)

- TAPs fungieren als permanenter Zugang zum Messpunkt
- TAPs ermöglichen Analysen in Full-Duplex, ohne Überbuchung
- TAPs geben physik. Fehler der Leitung an den Analyzer weiter
- TAPs arbeiten transparent und werden im Netzwerk nicht erkannt

High Density nTAP (Test Access Port)

- 1HE Rack für bis zu 24 Fiber nTAPs
- für 1, 10, oder 40 Gbps nTAPs (Fiber only)
- nTAP Module werden variabel eingesetzt
- kein Stromanschluss notwendig

Messpunktrealisierung mit nTAPs & Matrix Network Monitoring Switch

Die nTAPs (Test Access Ports) ermöglichen eine leistungsstarke Erstellung von Netzwerk-Analyse-Zugriffspunkten und sind in drei Varianten (Inline – Aggregation – Conversion) sowohl für Copper- als auch für Fiber-Anbindungen verfügbar. Der Matrix-Switch 1024 verfügt über 24 SFP/SFP+ Ports, welche skalierbar bestückt werden können. Insbesondere die einfache Administration per Web-GUI (u.a. mit Filter-Definition via Icon und zentralisiertem Regelmanagement) reduziert den Konfigurationsaufwand erheblich.

Motivation für den Einsatz von Matrix-Switches

Der Matrix – Switch 1024 unterstützt die Zusammenführung von Messpunkten mit unterschiedlichen Geschwindigkeiten. Eine Vorfilterung und Aggregation der Datenströme erfolgt einfach mittels Web-GUI. Der Matrix-Switch ermöglicht:

- Messpunkte für mehrere (parallele) Monitoring-Tools
- Nutzung von 1G-Monitoring-Tools an 10G-Messpunkten
- Vorfilterung für Monitoring-Tools zur Datenreduzierung

Network Instruments nTAP in drei Varianten
Inline — Aggregation — Conversion
Für Copper und Fiber

Feature-Set Matrix 1024

- Einfache Bedienung per Web-GUI (HTML5)
- 1U für 24x SFP/SFP+ Ports
- Skalierbar per Lizenzfreischaltung
- “Ingress / Egress” pro Port frei wählbar
- Replication, Aggregation (one-to-many, many-to-one, any-to-any)
- Speed Conversion, Filtering, De-Duplication
- Port / Time-Stamping, Packet-Trimming
- Load-Balancing

Network Instruments Matrix 1024 mit 24x SFP/SFP+ Ports

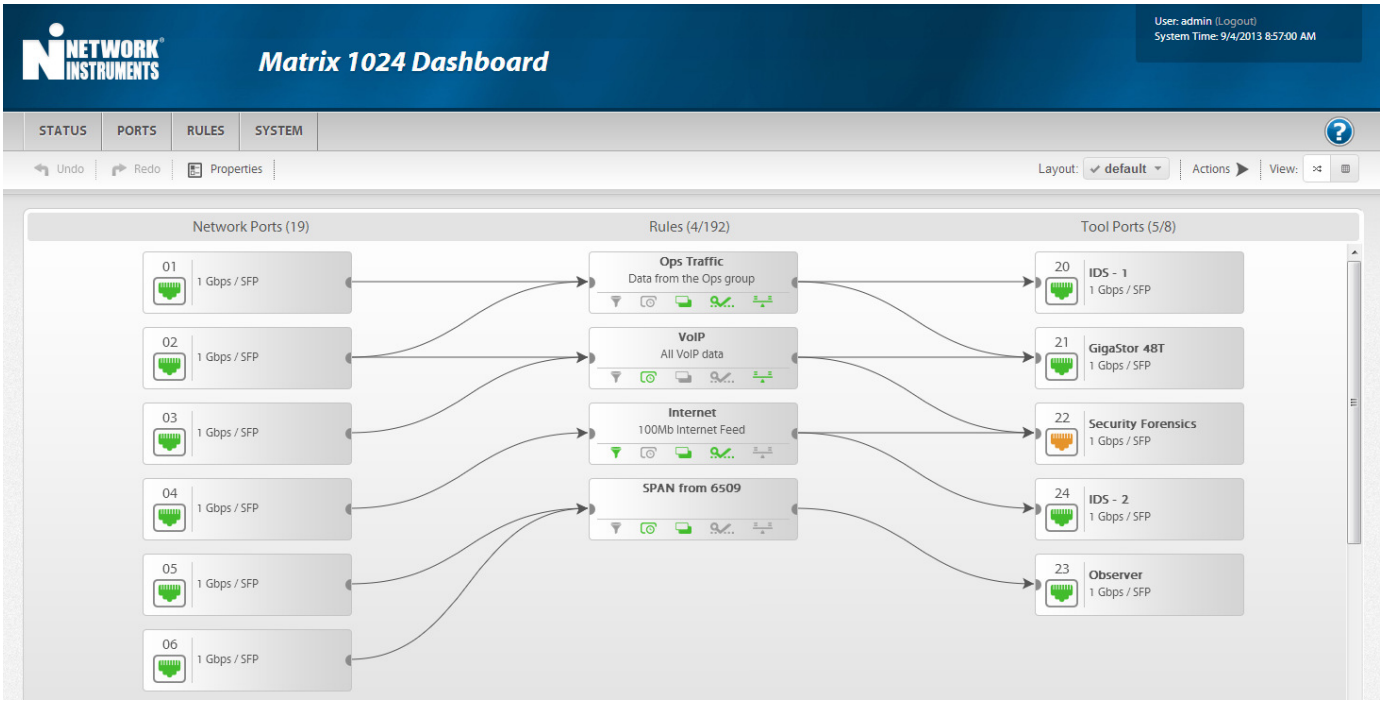
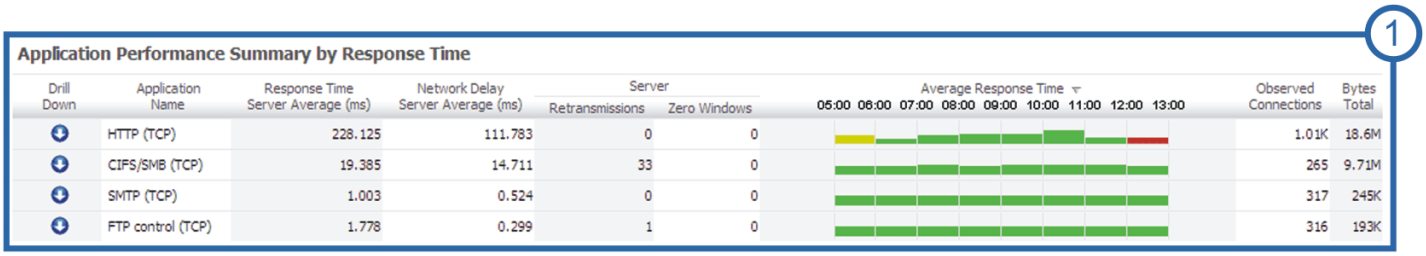


Abbildung-3: Messpunktrealisierung mit nTAPs und Matrix Network Monitoring Switch mit einfacher Administration per Web-GUI

Schritt-1: Erster Überblick in der Application Performance Summary

Da eine langsame Web-Anwendung gemeldet wurde, prüft der Netzwerk-Verantwortliche im ersten Schritt in der GigaStor-Weboberfläche die Performance der Applikationsprotokolle (u.a. FTP, SMTP, CIFS/SMB, HTTP). Das System zeigt für den Zeitbereich von 12:00 bis 13:00 Uhr eine rot markierte Anomalie im Übertragunsprotokoll HTTP (vgl. nachfolgende Abbildung zu Schritt-1).

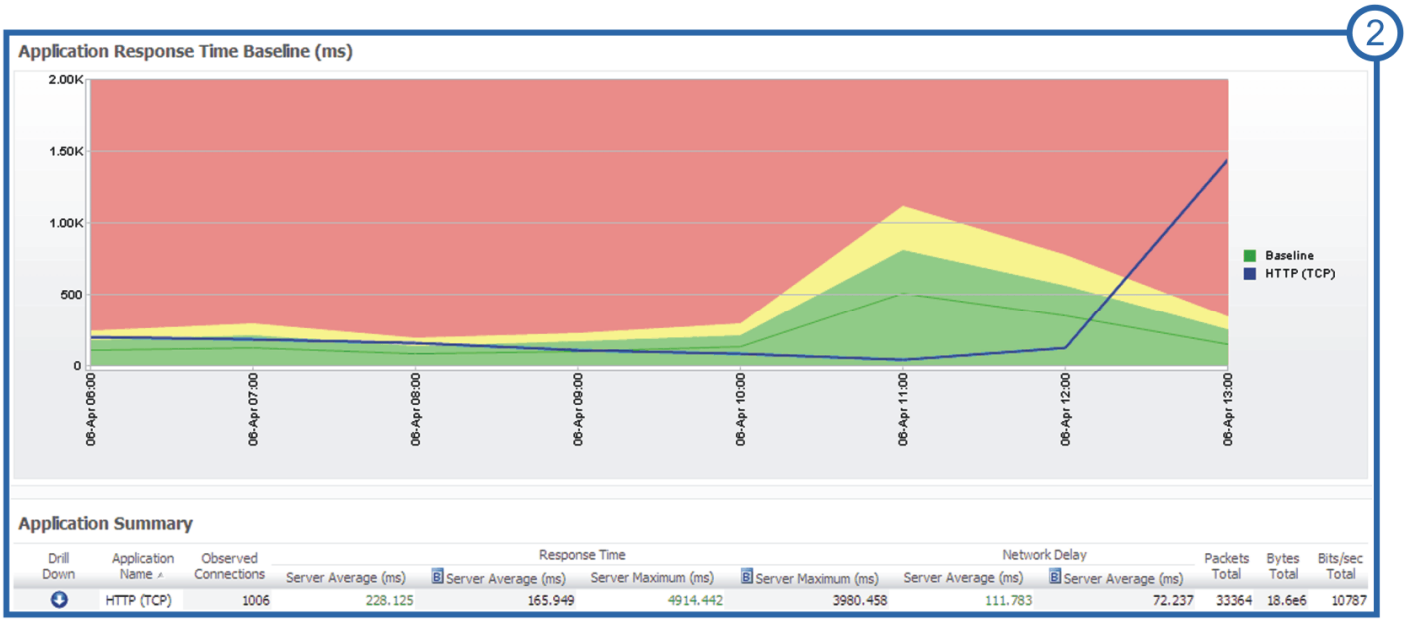


Drill Down	Application Name	Response Time Server Average (ms)	Network Delay Server Average (ms)	Server Retransmissions	Server Zero Windows	Observed Connections	Bytes Total
	HTTP (TCP)	228.125	111.783	0	0	1.01K	18.6M
	CIFS/SMB (TCP)	19.385	14.711	33	0	265	9.71M
	SMTP (TCP)	1.003	0.524	0	0	317	245K
	FTP control (TCP)	1.778	0.299	1	0	316	193K

Abb. zu Schritt-1: Übersicht zu Applikations-Antwortzeiten — für HTTP wird eine rot markierte Anomalie angezeigt

Schritt-2: Blick auf die HTTP-Antwortzeiten — Vergleich mit der Baseline

Der Administrator möchte im zweiten Schritt die gezeigte Anomalie mit der Baseline vergleichen. Die GigaStor ermöglicht mittels Baselining einen Vergleich der aktuellen Werte mit den Werten der gespeicherten Ergebnisse aus der Vergangenheit (Tage / Wochen / Monate). Die Baseline dient hierbei zur Orientierung im Sinne von „Vergleich mit dem normalen Verhalten der Applikationen im Netz“. Der Drill-Down-Report „Application Response Time Baseline“ zeigt per Mausklick die Baseline (grün) sowie einen signifikanten Anstieg der HTTP-Antwortzeiten ab 12:00 Uhr (blau), welche deutlich über dem Baseline-Wert liegen (vgl. Abb. zu Schritt-2). Die gemeldete langsame Web-Anwendung ist demnach definitiv eine akute Störung im Netz- oder im Serverbereich.



Drill Down	Application Name	Observed Connections	Response Time Server Average (ms)	Response Time B Server Average (ms)	Response Time Server Maximum (ms)	Response Time B Server Maximum (ms)	Network Delay Server Average (ms)	Network Delay B Server Average (ms)	Packets Total	Bytes Total	Bits/sec Total
	HTTP (TCP)	1006	228.125	165.949	4914.442	3980.458	111.783	72.237	33364	18.6e6	10787

Abb. zu Schritt-2: Baseline der HTTP-Applikationen

Schritt-3: Ist es der Netzwerk- oder der Serverbereich ?

Schritt-3 soll klären, ob die Ursache der Störung im Netz- oder im Serverbereich liegt. Hierzu vergleicht der Administrator die Verzögerungszeiten des Netzwerks (Network Delay) mit den Antwortzeiten der HTTP-Server (Server Response Time). Dies ermöglicht die GigaStor ebenfalls per Drill-Down-Report, welcher zu hohe Server-Antwortzeiten zeigt. Die HTTP-Applikation antwortet offenbar zu langsam. Ursache des Fehlers ist also nicht der Netzwerk-, sondern der Serverbereich.

Die nachfolgende Abbildung zu Schritt-3 verdeutlicht dies. Der blaue Bereich zeigt die durchschnittliche Verzögerung durch das Netzwerk (Delay). Diese ist nahezu unverändert und unauffällig. Der grüne Bereich zeigt einen signifikanten Anstieg der HTTP-Server-Antwortzeiten. Die Ursache der Störung liegt also im Serverbereich. Mit ein paar weiteren Klicks geht man der Sache auf den Grund.

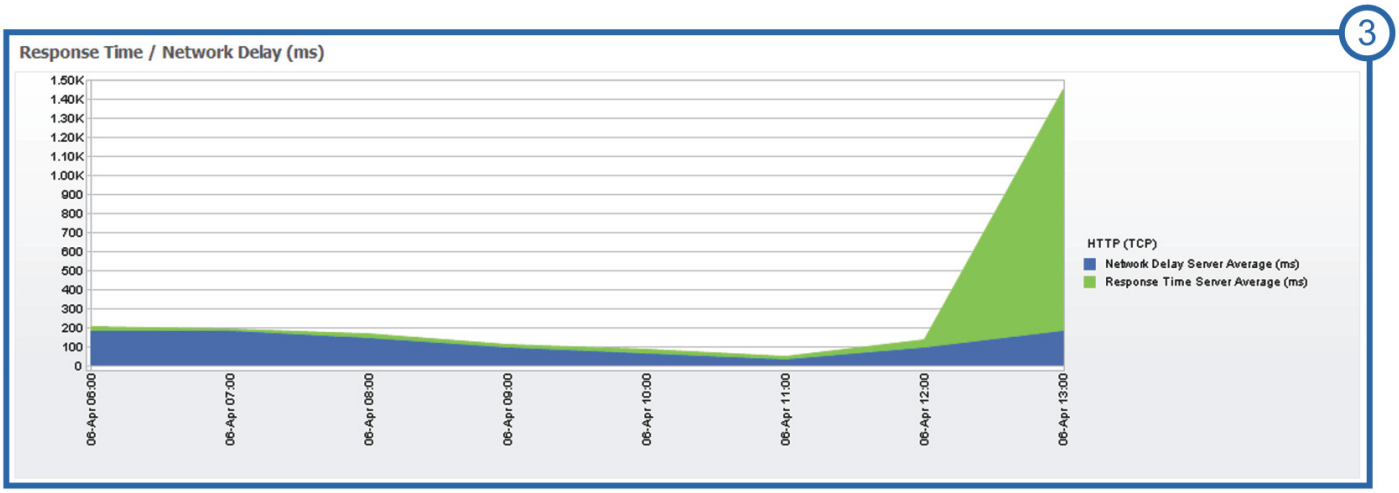
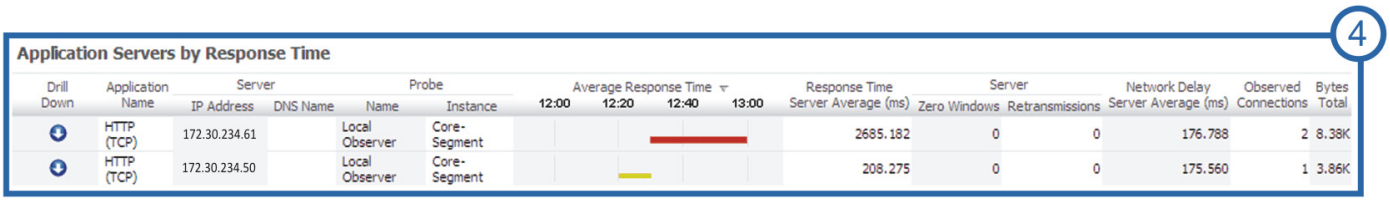


Abb. zu Schritt-3: Durchschnittliche Verzögerung im Netz (blau) im Vergleich zu den HTTP-Server-Antwortzeiten (grün)

Schritt-4: Welcher Server ist langsam ?

Die ersten drei Schritte haben gezeigt, dass der Fehler im Serverbereich liegt und es stellt sich die Frage, welcher Server genau langsam ist. Der Admin nutzt hierzu, ausgehend vom Report „Application Performance Summary" aus Schritt-1, den Drill-Down-Report „Application Servers by Response Time", welcher einen auffälligen Server mit der IP „172.30.234.61" anzeigt. Dieser Server beinhaltet das Web-Frontend der auffälligen Anwendung. Der Report zeigt eine durchschnittliche Server-Antwortzeit (Response Time Server Average, vgl. Abb. zu Schritt 4) von 2.685,182ms. Eine solche Antwortzeit, über zwei Sekunden, ist allerdings sehr hoch.

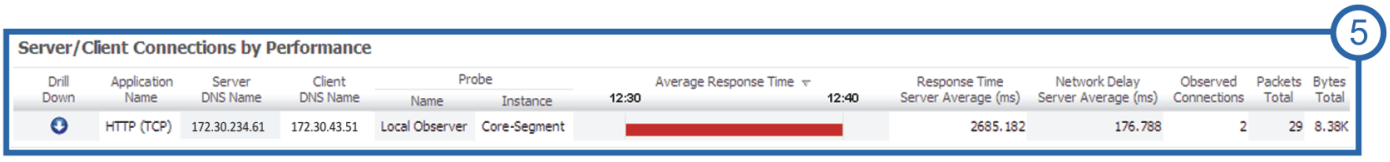


Drill Down	Application Name	Server IP Address	Server DNS Name	Probe Name	Probe Instance	Average Response Time (12:00 12:20 12:40 13:00)	Response Time Server Average (ms)	Server Zero Windows	Server Retransmissions	Network Delay Server Average (ms)	Observed Connections	Bytes Total
	HTTP (TCP)	172.30.234.61		Local Observer	Core-Segment		2685.182	0	0	176.788	2	8.38K
	HTTP (TCP)	172.30.234.50		Local Observer	Core-Segment		208.275	0	0	175.560	1	3.86K

Abb. zu Schritt-4: HTTP-Server mit IP-172.30.234.61 zeigt eine zu hohe Antwortzeit (rot markiert)

Schritt-5: Welche Clients sind betroffen ?

Nach der Identifizierung des problematischen Servers möchte der Administrator wissen, welche Clients von der Störung betroffen sind. Der Drill-Down-Report „Server/Client Connections by Performance" zeigt ihm sämtliche Clients, die im gemeldeten Fehlerzeitraum mit dem Server kommuniziert haben. Der Report meldet nur einen betroffenen Client für den Zeitraum, welcher auch die Störung gemeldet hatte (IP „172.30.43.51", vgl. Abbildung zu Schritt 5).



Drill Down	Application Name	Server DNS Name	Client DNS Name	Probe Name	Probe Instance	Average Response Time (12:30 12:40)	Response Time Server Average (ms)	Network Delay Server Average (ms)	Observed Connections	Packets Total	Bytes Total
	HTTP (TCP)	172.30.234.61	172.30.43.51	Local Observer	Core-Segment		2685.182	176.788	2	29	8.38K

Abb. zu Schritt-5: Server-Antwortzeit der Client/Server HTTP-Verbindung

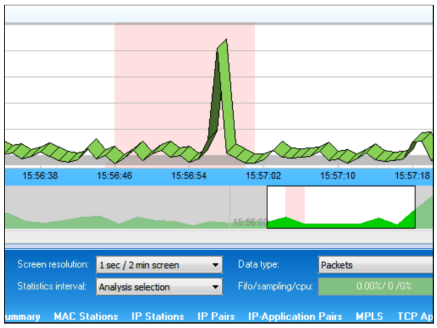
GigaStor™ — Rewind. Review. Resolve.

Die GigaStor erfasst und speichert jedes übertragene Paket an definierten Messpunkten im Netz und ermöglicht so ein einfaches „Zurückspulen“ der Datenkommunikation im Rahmen der Retrospektiven Netzwerk-Analyse zur Ermittlung von Netzwerk-, Applikations- oder Security-Problemen.

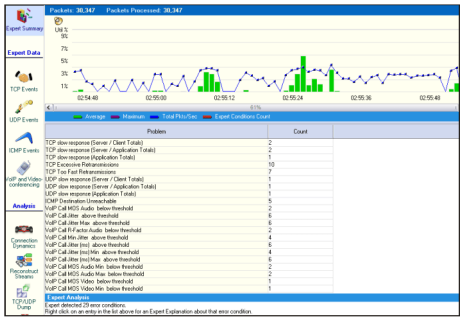
Die Retrospektive Netzwerk-Analyse (RNA) ist vergleichbar mit einer 24/7 Kameraüberwachung für das Netzwerk. Die RNA erlaubt ein „Zurückspulen“ in kritische Szenarien und zeigt, was vor, während, und nach einer Netzwerk-Anomalie vorgefallen ist.

- Erhebliche Reduzierung der Mean Time To Resolution (MTTR) bei Störungen / Ausfällen
- Unterstützt Kapazitätsplanung & Rollouts
- Ermittlung von sporadischen Problemen, ohne Nachstellung
- Isolierung von Applikations-Problemen

1 — Rewind



2 — Review



Network Troubleshooting

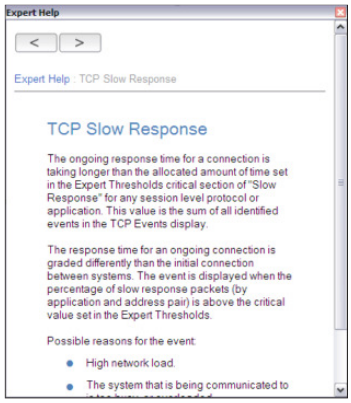
Die GigaStor unterstützt die Ermittlung von Netzwerk-Anomalien innerhalb von wenigen Schritten.

- Isolierung von Zeitfenster und User
- Drill-Down bis auf Paketebene
- Expert-Analyse

Expert-Analyse

- Über 600 Expert-Metriken
- Zur Identifizierung von Netzwerk-Anomalien
- Differenzierung zwischen Netzwerk- und Applikations-Problemen
- Unterstützt Echtzeit- und Post-Capture-Analysen
- Grafische Darstellung zur schnellen Identifizierung von Retransmissions, Dropped Packets, Latency und Antwortzeiten
- Nanosekunden-genaue Analysen zur Erkennung von Microbursts

3 — Resolve

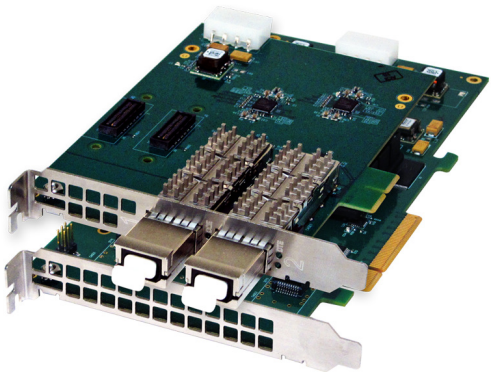


Network & Security Forensics

- Vergleich von aufgezeichneten Daten gegen Snort® Rules zur Identifizierung von Attacken und Anomalien
- Identifizierung von kompromitierten Netzteilnehmern und –Segmenten
- Drill-Down zur Determinierung von Quelle und Zeit eines Vorfalls
- Sicherstellung von Compliance und Unternehmens-Policies

GigaStor™ Erfassungskarte — Gen2™ Technology

- Nanosekunden-genaue Zeitstempel für präzise Analysen
- Flexibles Packet Deduplication reduziert doppelte Daten
- Hardware-Filter und Statistikerfassung direkt auf der Gen2 Card
- Datenerfassung und Analyse direkt in der GigaStor
- Verfügbar für 1 / 10 / 40 Gbps Ethernet
- Bis zu vier Ports pro Gen2 Card — bis zu zwölf Ports pro GigaStor



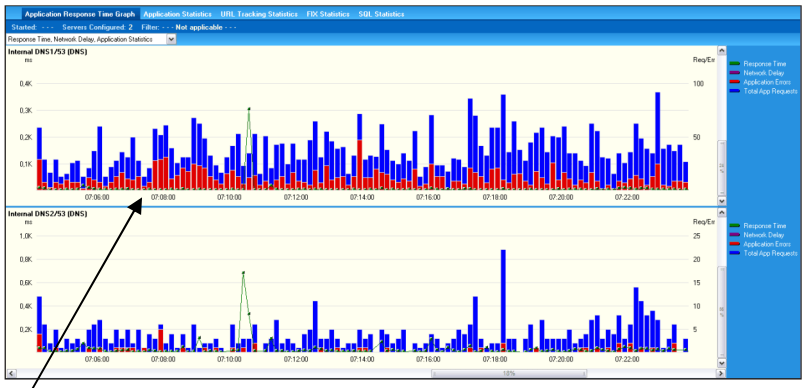
Gen2™ Erfassungskarte

Abbildung-4: Übersicht zur GigaStor-Technologie (Teil 1 /2)

Application Performance Monitoring

- Ermittlung des normalen Applikations-Verhaltens durch Generierung von Baselines mittels Trend Reporting
- Isolation von Anomalien
- Identifizierung von Latenzen
- Integrierte Metriken zur Fehleranalyse für Applikationen:
  - Citrix
  - Email
  - File-Dienste
  - Financial
  - Oracle
  - UC / VoIP
  - Web

  u.a.



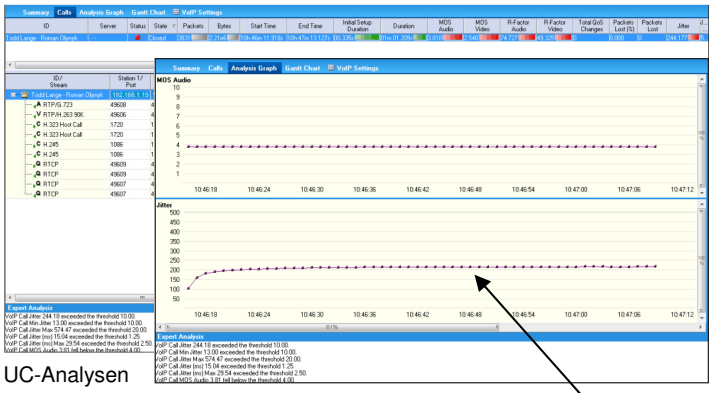
Applikations-Analysen

Tracking von Applikations-Anfragen, -Fehlern und Antwortzeiten

Unified Communications

- Performance-Überwachung mit über 70 integrierten UC-Metriken
- Bewertung der Call Quality
- Monitoring:
  - H.323
  - SIP
  - MGCP
  - SCCP
  - Avaya CCMS

  u.a.

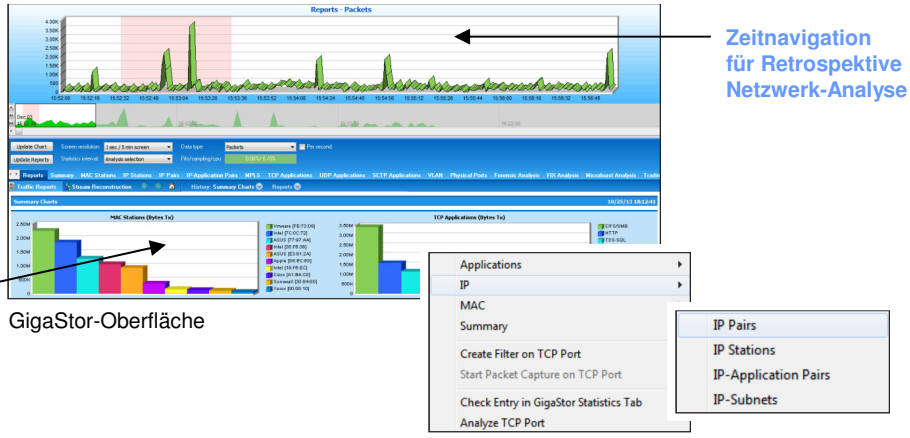


UC-Analysen

Analyse der Gesprächsqualität (z.B. zeitlicher Verlauf von MOS / Jitter)

GigaStor-Oberfläche

- Zeitbasierte Navigation ermöglicht schnelle Problem-Isolierung (RNA)
- Zeitfenster im Nanosekunden-Bereich für Microburst-Analysen
- Einfacher Zugriff auf adaptive Reports



Zeitnavigation für Retrospektive Netzwerk-Analyse

Benutzer-definierbare Workflows und Reports

GigaStor-Oberfläche

Abbildung-5: Übersicht zur GigaStor-Technologie (Teil 2 /2)

Nach nur fünf Schritten per Drill-Down in der GigaStor hat der Administrator analysiert, dass die Ursache für die gemeldete Störung nicht im Netz, sondern auf der Server-/Applikationsseite liegt. Zudem hat er ermittelt, dass der Fehler in einer HTTP-Applikation steckt und dass derzeit nur ein Client betroffen ist. Das Webfrontend der langsamen Anwendung erhält die zu visualisierenden Daten von einem Fileserver. Der Admin überprüft somit diesen Fileserver, da der Fehler genau dort liegen könnte. Eine Performance-Analyse des Fileservers analog zu den o.g. Schritten 1 bis 5 ergibt jedoch keine Auffälligkeiten. In den nächsten Schritten 6 bis 9 wird daher die Kommunikation zwischen Webfrontend ↔ Fileserver im Detail analysiert (Detail-Analyse).

Schritt-6: Eingrenzung des Zeitbereichs zur Detail-Analyse (Webfrontend ↔ Fileserver)

Die genaue Überprüfung der Kommunikations-Beziehung zwischen Webfrontend und Fileserver erfordert eine Detail-Analyse der aufgezeichneten Datenpakete (Traces). Hierzu grenzt man in der GigaStor-Oberfläche den zu untersuchenden Zeitbereich ein (vgl. Abb. zu Schritt-6, rot markierter Bereich) und wählt das gewünschte Kommunikations-Paar per Vorab-Filter aus (Datamining).

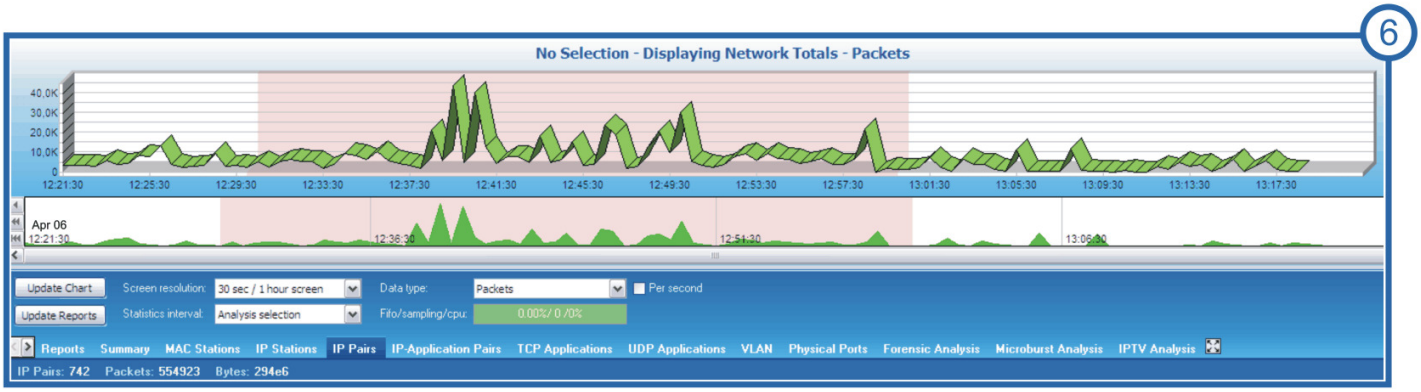
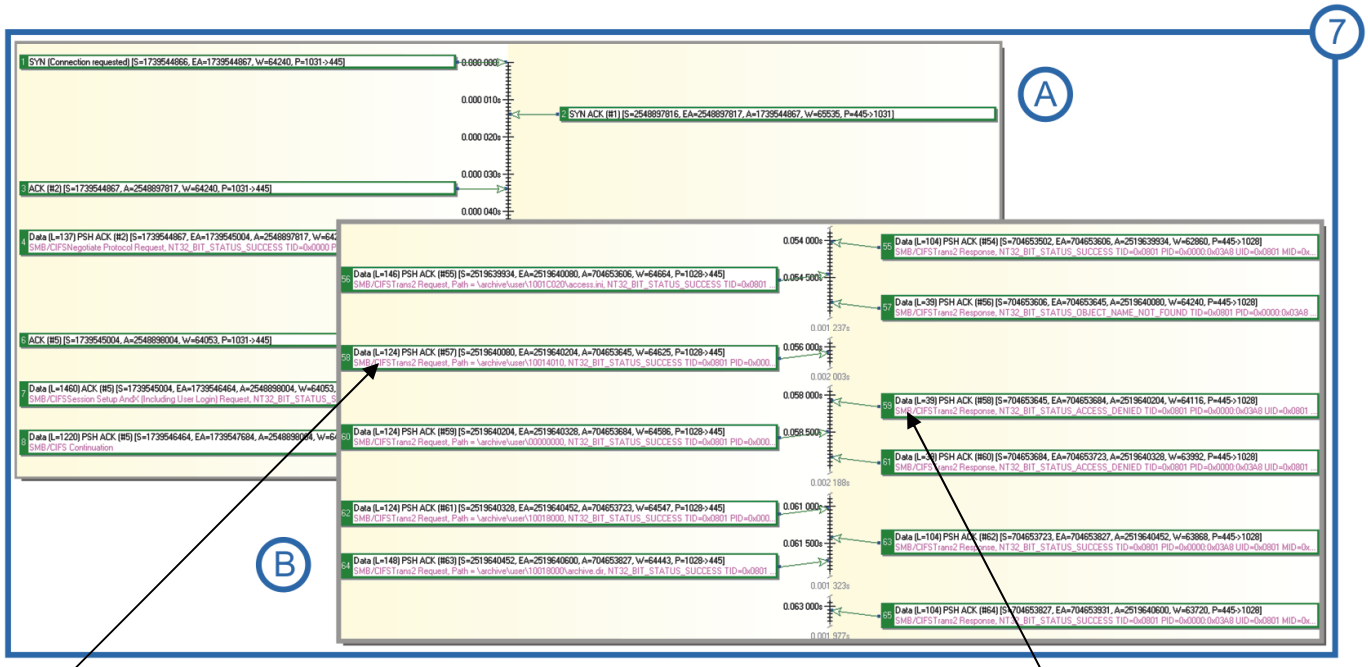


Abb. zu Schritt-6: Eingrenzung des Zeitbereichs zur Detail-Analyse (markierter Bereich)

Schritt-7: Kommunikationsverlaufs-Analyse zeigt Probleme im CIFS-Dialog

Der Verbindungsaufbau (TCP - Three-Way-Handshake) erfolgt normal. Das generelle Antwortzeit-Verhalten ist unauffällig (deutlich unter 1ms, vgl. Abbildung zu Schritt-7A). Auffällig dagegen sind CIFS-Anfragen seitens des Webfrontends mit negativer Beantwortung durch den Fileserver (*Object Name not Found, Access Denied*, vgl. Abbildung zu Schritt-7B).

Abb. zu Schritt-7: Verbindungsaufbau (A) ohne Befund. Jedoch Fehlermeldungen im CIFS-Dialog zwischen Webfrontend und Fileserver (B)



58 Data (L=124) PSH ACK (#57) [S=2519640080, EA=2519640204, A=704653645, W=64625, P=1028->445]
SMB/CIFSTrans2 Request, Path = \archive\user\10014010, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x000...

Client-Anfrage

59 Data (L=39) PSH ACK (#58) [S=704653645, EA=704653684, A=2519640204, W=64116, P=445->1028]
SMB/CIFSTrans2 Response, NT32_BIT_STATUS_ACCESS_DENIED TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 ...

Server-Antwort: Zugriff verweigert

Schritt-8: Statistik zu den verwendeten CIFS-Anfrage/Anwort-Codes mittels integrierter Applikations-Analyse

Einen Überblick zu allen Anfragen / Antworten der CIFS-Kommandos gibt die Analyse-Metrik respektive Auswerte-Schablone „Application Transaction Analysis“ im Rahmen der integrierten Applikations-Analyse. Diese zeigt die Anzahl von CIFS-Anfragen und CIFS-Antworten (für den ausgewählten Zeitbereich) an den Fileserver. Einige dieser Anfragen werden mit den Status-Codes „Access_Denied“ (≡ Zugriff verweigert) und „Object_Name_Not_Found“ (≡ Objekt-Name nicht gefunden) quittiert (vgl. Abb. zu Schritt-8).

8

CIFS/SMB (TCP)

Server	Count	Response Time		Request		Response	
		Average (ms)	Max (ms)	Packets	Bytes	Packets	Bytes
File-Server/445 (CIFS/SMB)							
Requests	93060	0.997	4.013	93060	17.4e6	93060	18.7e6
0x04 = Close File	3000	0.995	2.990	3000	309000	3000	291000
0x2E = Read AndX	2400	0.997	2.969	2400	290400	2400	2.79e6
0x32 = Trans2	85460	0.997	4.013	85460	16.3e6	85460	15.2e6
0xA2 = NT Create AndX	2200	1.002	2.950	2200	482800	2200	433400
Response Statistics	93060						
0x00000000 = STATUS_SUCCESS	88478						
0xC0000022 = STATUS_ACCESS_DENIED	597						
0xC0000034 = STATUS_OBJECT_NAME_NOT_FOUND	3985						

Abb. zu Schritt-8: Übersicht der Client-Anfragen und Server-Antworten per CIFS, inkl. Fehlermeldungen

Schritt-9: Per Mausklick weiter in das Packet Decoding – Was genau wird angefragt im CIFS-Dialog ?

Im Packet Decode ist im Detail zu erkennen, dass das Webfrontend sämtliche Archiv-Ordner für die Anwendung per CIFS abfragt. Einige Anfragen erfolgen dabei mit falschen Zugriffsrechten. Teilweise erfolgen die Anfragen mit Datei- oder Ordner-Namen, welche nicht (mehr) existieren (vgl. Abbildungen zu Schritt-9A und Schritt-9B). Das CIFS-Protokoll arbeitet normal, jedoch wird das Webfrontend aufgrund der vielen (unnötigen) Anfragen langsam. Eine Korrektur der Konfiguration sollte das Problem beheben.

9A

Pkt	Type	Size	Summary
2704	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x7982
2705	IP	206	SMB/CIFSTrans2 Request, Path = \archive\user\1001C020\archive.dir, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2706	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x79C2
2707	IP	204	SMB/CIFSTrans2 Request, Path = \archive\user\1001C020\access.ini, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2708	IP	97	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_OBJECT_NAME_NOT_FOUND TID=0x0801 PID=0x0000:0x03A8 UID=0x
2709	IP	182	SMB/CIFSTrans2 Request, Path = \archive\user\10014010, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03
2710	IP	97	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_ACCESS_DENIED TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x
2711	IP	182	SMB/CIFSTrans2 Request, Path = \archive\user\00000000, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03
2712	IP	97	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_ACCESS_DENIED TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x
2713	IP	182	SMB/CIFSTrans2 Request, Path = \archive\user\10018000, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03
2714	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x7AC2
2715	IP	206	SMB/CIFSTrans2 Request, Path = \archive\user\10018000\archive.dir, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2716	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x7B02
2717	IP	206	SMB/CIFSTrans2 Request, Path = \archive\user\10018000\archive.dir, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2718	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x
2719	IP	204	SMB/CIFSTrans2 Request, Path = \archive\user\10018000\access.ini, NT32_BIT_STATU

TCP PSH ACK, [1028] -> [445] CIFS/SMB
SMB Over TCP Message Length: 120
CIFS: Client Request - Trans2 (TID=0x0801, PID=0x0000:0x03A8, UID=0x0801, MID=0x7A42)
SMB - Trans2
SMB Trans2 - Get Info On Named File/Directory: File Basic Info (\archive\user\10014010)
Function [5] = Get Info On Named File/Directory
Byte Count 55
Padding
0000 00 00 00
Information Level [1004] = File Basic Info
Reserved (0x00000000)
File or Directory Name \archive\user\10014010

Abb. zu Schritt 9A: Zugriffsversuch auf Archiv-Daten

9B

Pkt	Type	Size	Summary
2704	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x7982
2705	IP	206	SMB/CIFSTrans2 Request, Path = \archive\user\1001C020\archive.dir, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2706	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x79C2
2707	IP	204	SMB/CIFSTrans2 Request, Path = \archive\user\1001C020\access.ini, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2708	IP	97	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_OBJECT_NAME_NOT_FOUND TID=0x0801 PID=0x0000:0x03A8 UID=0x
2709	IP	182	SMB/CIFSTrans2 Request, Path = \archive\user\10014010, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A
2710	IP	97	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_ACCESS_DENIED TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x
2711	IP	182	SMB/CIFSTrans2 Request, Path = \archive\user\00000000, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A
2712	IP	97	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_ACCESS_DENIED TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x
2713	IP	182	SMB/CIFSTrans2 Request, Path = \archive\user\10018000, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A
2714	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x7AC2
2715	IP	206	SMB/CIFSTrans2 Request, Path = \archive\user\10018000\archive.dir, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2716	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x7B02
2717	IP	206	SMB/CIFSTrans2 Request, Path = \archive\user\10018000\archive.dir, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x
2718	IP	162	SMB/CIFSTrans2 Response, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x0000:0x03A8 UID=0x0801 MID=0x7B42
2719	IP	204	SMB/CIFSTrans2 Request, Path = \archive\user\10018000\access.ini, NT32_BIT_STATUS_SUCCESS TID=0x0801 PID=0x

CIFS: Server Response - Trans2 (TID=0x0801, PID=0x0000:0x03A8, UID=0x0801, MID=0x7A42)
SMB Header Command [50] = Trans2
CIFS Protocol Marker ÿSMB = SMB
Command [50] = Trans2
NT32_Bit Status STATUS_ACCESS_DENIED (0xC0000022)
Flags SD=F, GB=F, PC=T, CA=T, OL=F, SN=F, SR=T
(SD) Supports Sub-Dialect = False
(GB) Client Guarantees Receive Buffer = False
Reserved (must be zero)
(PC) All Pathnames are Caseless = True
(CA) All Paths Sent are Already Canonicalized = True
(OL) Requesting File Be Opportunistically Locked = False

Abb. zu Schritt 9B: Fileserver verweigert den Zugriff auf angeforderte Archiv-Daten

Mit fünf Schritten in der GigaStor konnte ermittelt werden, dass der Fehler nicht im Netz, sondern auf der HTTP-Applikationsseite liegt. Mit weiteren vier Schritten wurde analysiert, dass es Probleme mit Zugriffsrechten und nicht aktuellen Datei- und Ordnernamen gibt.

Zusammenfassung

Heutzutage ist es allgemein nachvollziehbar, dass das Netzwerk und die Kommunikation darüber in Unternehmen und Organisationen stabil und ohne Störungen funktionieren muss. Zuviele unternehmenskritische Prozesse, Anwendungen und Kommunikationen sind davon abhängig. Ebenso ist es nachvollziehbar, dass Störungen de facto nicht komplett ausgeschlossen werden können, und dass Anomalien im Netzwerk durchaus empfindliche Kosten zur Folge haben. Dies gilt mittlerweile branchenunabhängig. Es empfiehlt sich, optimalerweise sowohl Werkzeug als auch eine Vorgehensweise zur Hand zu haben, um im Ernstfall schnell eine Lösung zu finden.

Neben einem modernen und belastbaren Netzwerk-Design (inkl. Redundanzen, no single point of failure, etc.) ist es empfehlenswert, auch strategische Messpunkte im Netzwerk zu definieren und vorzubereiten (z.B. per TAP), um so jederzeit den Datenstrom einsehen und mögliche Anomalien analysieren zu können. Optimalerweise wird eine Restrospektive Netzwerk-Analyse (RNA) ermöglicht, vergleichbar mit einer 24/7 Kameraüberwachung im Netz, welche ein „Zurückspulen“ der Datenkommunikation in kritische Szenarien unterstützt und in wenigen Schritten aufzeigt, was vor, während und nach einer Netzwerk-Anomalie vorgefallen ist.

Die beschriebene GigaStor-Technologie ermöglicht die Retrospektive Netzwerk-Analyse und verkürzt mit wenigen Analyse-Schritten Fehlersuche, Ursachen-Ermittlung und Fehlerbehebung erheblich.

Network Instruments

Network Instruments ist seit über 18 Jahren ein führender Entwickler von Performance Management- und Analyse-Lösungen. Hierbei unterstützen die durchgängig eigenentwickelten Lösungen insbesondere die Gewährleistung eines reibungslosen Betriebs von geschäftskritischen Applikationen und Netzwerken. Network Instruments hat seinen Hauptsitz in Minneapolis, Minnesota (USA), mit Niederlassungen weltweit und Partnern in über 50 Ländern.

Retrospective Network Analyzer

Manage with edge-to-core vision.

Rewind. Review. Resolve.

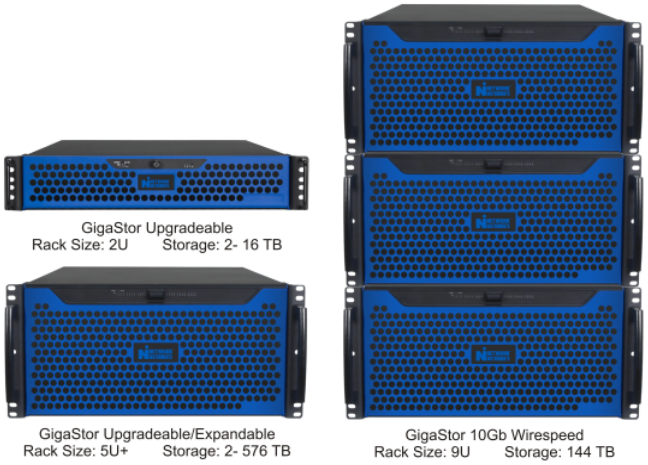
Stop Missing Critical Network Events.

GigaStor™

Als Langzeit-Analyse - System erfasst GigaStor detaillierte Netzwerk-Informationen in Echtzeit und bietet eine Retrospektive Netzwerk-Analyse durch Speicherung der erfassten Daten ohne Informationsverlust. Zurückliegende Ereignisse können somit ad hoc analysiert werden, eine zeitaufwendige Reproduktion von Fehlerszenarien entfällt.

Key Features

- Portable Option
- Root-Cause Analysen
- Latenz-Zeiten-Analyse
- Server-Delay-Tracking
- Integrierte Experten-Analyse
- Speicherkapazität bis zu 576 TB
- Gen2 Packet Capture Technologie
- Für 1 / 10 / 40 Gbps, bis zu zwölf Ports
- Applikations-spezifisches Error-Monitoring



Weitere Informationen

www.gordion.de • www.networkinstruments.com

Copyright © 2013 GORDION Data Systems Technology GmbH. Alle Rechte vorbehalten. Alle Logos, Marken, Firmennamen und Produktdesigns gehören ihren jeweiligen Eigentümern.

GORDION®

Lösungen für komplexe Rechner-Netzwerke.

Network Consulting

LAN / WAN • Security • Analyzing