

# PERFORMANCE MANAGEMENT

Network Instruments Solutions from Professionals



**IT-Union GmbH & Co. KG**

BUSINESS IT-SOLUTIONS

## NUTZEN SIE UNSER WISSEN UND UNSERE ERFAHRUNG

Die IT-Union GmbH & Co. KG (ITU) ist ein Systemhausverbund und wurde 2008 von den Gesellschaftern BMAnetworks, DANES, GORDION und INDASYS gegründet. Die Mitglieder der IT-Union sind bereits seit den frühen 90er Jahren am Markt und verfügen allesamt über ein tiefes Know-how im Bereich der Netzwerktechnik und -Analyse. Durch die langjährige Erfahrung unserer Spezialisten ist die ITU ein idealer Partner rund um das Thema Network Performance Management und unterstützt branchenübergreifend Netzwerke unterschiedlichster Größenordnung und Komplexität.

## EIN STARKER VERBUND FÜR UNSERE KUNDEN UND PARTNER

Die IT-Union ist ein Verbund von vier innovativen IT-Systemhäusern, die in ihren Spezialgebieten Datennetzwerktechnik, IT-Sicherheit, Voice over IP und Triple-Play-Metronetze zu den führenden IT-Unternehmen innerhalb Deutschlands gehören.

Der Schulterchluss dieser IT-Spezialisten erfolgte mit dem Ziel, ihren Kunden und Partnern den größtmögliche Nutzen zu bieten. So steht die IT-Union für

- Bundesweite Präsenz bei regionaler Nähe zu unseren Kunden
- Umfassendes und tiefes know how zu den fokussierten Fachgebieten
- Langjährige Erfahrung
- Schnelle Reaktionszeiten bei Support und spare parts
- Supportservices 24 Stunden an 7 Tagen der Woche
- Produkte und Lösungen, die markt-, innovations-, leistungs-, sowie qualitätsführend sind
- Kunden, die eine hohen Anspruch an Ihre IT stellen und damit an uns, die IT-Union, Ihrem IT-Versorger
- Kunden aus allen Branchen und Größenordnungen
- Die Flexibilität eines mittelständischen Unternehmens

- >> Datennetzwerktechnik
- >> IT-Sicherheit und Datenschutz
- >> Voice over IP
- >> Triple Play Metronetze

### NORD

**Kiel**  
BMAnetworks GmbH  
Preetzer Chaussee 55  
24222 Schwentinental  
Telefon 0431 97449 0  
Telefax 0431 97449 77  
Email vertrieb.ki@it-union.eu

**Hamburg**  
BMAnetworks GmbH  
Albert-Einstein-Ring 5  
Arelia-Haus, 22761 Hamburg  
Telefon 0431 97449 0  
Telefax 0431 97449 77  
Email vertrieb.hh@it-union.eu



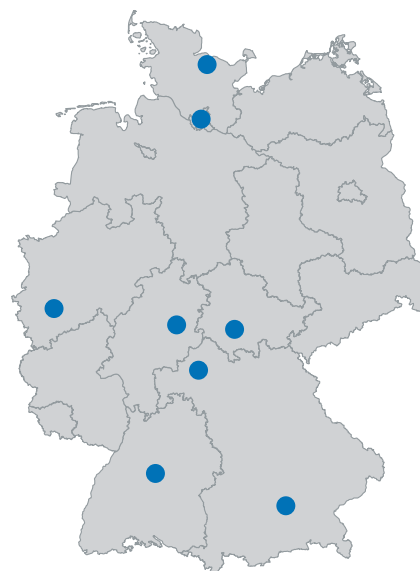
### MITTE

**Köln**  
GORDION Data Systems Technology GmbH  
Mottmannstraße 13  
53842 Troisdorf  
Telefon 02241 4904 0  
Telefax 02241 4904 90  
Email vertrieb.kln@it-union.eu

**Fulda**  
DANES Datennetzwerktechnik GmbH  
Richard-Müller-Straße 7  
36039 Fulda  
Telefon 0661 250359 0  
Telefax 0661 250359 11  
Email vertrieb.fd@it-union.eu

**Schweinfurt**  
DANES Datennetzwerktechnik GmbH  
Felix-Wankel-Straße 4  
97526 Sennfeld  
Telefon 09721 67594 10  
Telefax 09721 67594 11  
Email vertrieb.sw@it-union.eu

**Suhl**  
DANES Datennetzwerktechnik GmbH  
Schwarzwasserweg 17  
98527 Suhl  
Telefon 03681 4270 10  
Telefax 03681 4270 12  
Email vertrieb.shl@it-union.eu



### SÜD

**Stuttgart**  
indasys connectivity GmbH  
Leitzstraße 4c  
70469 Stuttgart  
Telefon 0711 896659 15  
Telefax 0711 896659 49  
Email vertrieb.st@it-union.eu

**München**  
DANES IT-Systems & Services GmbH  
Max-Planck-Straße 10  
85716 Unterschleißheim  
Telefon 089 37427 909 0  
Telefax 089 37427 909 11  
Email vertrieb.muc@it-union.eu

## VOICE OVER IP | VIDEO OVER IP

- >> VOIP Systeme
- >> IP Phones
- >> Voice over WLAN
- >> Unified Messaging
- >> Voice Mail
- >> Billing Lösungen
- >> Kamera-Management-Software
- >> Kameras für jeden Einsatzfall
- >> Integration bestehender analoger Kameratechnik

## TRIPLE PLAY METRONETZWERKE

- >> TV Versorgung mit hunderten von Programmen
- >> Zusätzlich Pay-TV möglich
- >> Video on Demand
- >> Schnelles Internet
- >> Erstklassige Telefonie
- >> Konvergenz der Dienste
- >> Telemetriatenerfassung
- >> Alles „aus einer Hand“

## OUTSOURCING UND MANAGED IT-SERVICES

- >> Systemadministration
- >> Active Monitoring /Alarming
- >> Troubleshooting
- >> Firewall Policy Backup
- >> Update Services
- >> Disaster Recovery
- >> Service Level Agreement (SLA)
- >> Logfile Analysen

## DATENNETZWERKTECHNIK

- >> Switching
- >> Routing
- >> WAN Verbindung
- >> LAN Gebäudevernetzung
- >> Bandbreitenmanagement
- >> WAN Beschleunigung
- >> Netzwerkdokumentation
- >> Netzwerkanalyse LAN/WAN/WLAN
- >> Enterprise Wireless LAN
- >> Managed WLAN
- >> WLAN Lösungen für Lager und Logistik
- >> WLAN über Laser oder Mikrowelle
- >> Application Delivery Lösungen

## IT-SICHERHEIT UND DATENSCHUTZ

- >> Firewall, Virenschutz
- >> Unified Threat Management
- >> VPN, SSL, IPsec
- >> Starke Authentifizierung
- >> Single Sign On (SSO) und Passwortmanagement
- >> Network Access Control
- >> Content Security
- >> Intrusion-Detection, -Prevention
- >> Datenschutzconsulting
- >> Externer Datenschutzbeauftragter



BMAnetworks GmbH

DANES Datennetzwerktechnik GmbH

GORDION Data Systems Technology GmbH

indasys connectivity GmbH

<b>Network Instruments</b> .....	<b>5</b>
<b>Network Instruments Lösungen</b> .....	<b>6</b>
<b>Observer Reporting Server (ORS)</b> .....	<b>7</b>
Unternehmensweites Performance Monitoring .....	7
Echtzeit-Reports .....	7
Per Drill-Down bis zur Paketebene .....	8
<b>GigaStor</b> .....	<b>9</b>
Retrospektive Netzwerk-Analysen .....	9
Reduzierung von Ausfallzeiten mittels proaktiver Fehlersuche .....	10
Vermeidung von Problemen bei Einführung neuer Applikationen .....	11
Überwachung von 10Gbit-Netzwerken .....	12
Erkennung von Security- und Compliance-Problemen .....	12
<b>Observer Analyse- und Monitoring-Lösung</b> .....	<b>13</b>
Übersicht .....	14
Über 600 Expert-Meldungen .....	15
Überwachung von IP-Diensten .....	15
Verbindungsanalyse mittels „Connection Dynamics“ .....	16
Unified Communications (UC) .....	16
Application Performance Monitoring .....	17
Zusätzliche Funktionen .....	18
<b>Observer Infrastructure (OI)</b> .....	<b>19</b>
Proaktives, unternehmensweites Device-Monitoring .....	19
Intuitive Netzwerk-Überwachung .....	20
Geräte-Überwachung .....	21
Überwachung von Netzwerk-Routen und SLAs .....	21
Individuelles Reporting .....	22
Alarmierung .....	23
WSD-Applikationsdaten .....	24
Nutzung von IP SLA- und NBAR-Funktionalitäten .....	24
Integration in Observer Reporting Server (ORS) .....	25

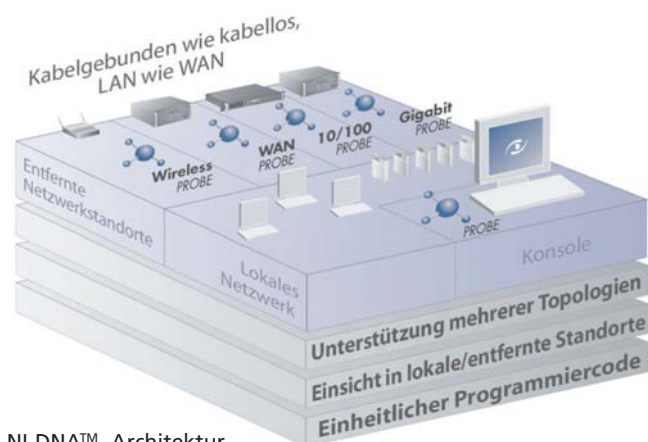
# Network Instruments

## Führend in Performance Management und Analyse

Network Instruments ist seit über 15 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 Vertriebspartnern in über 50 Ländern. Weitere Informationen zu Network Instruments finden Sie auf unserer Webseite: [www.it-union.eu](http://www.it-union.eu)

Die Lösungen von Network Instruments bieten einen umfassenden Überblick über das Netzwerk und deren Applikationen. Hierbei unterstützt eine Management- und Reporting-Plattform als ganzheitliche Lösung die Anforderung einer modernen IT:

- Performance-Optimierungen
- Kapazitätsplanungen
- Vermeidung von Ausfallzeiten
- Minimierung der Zeit zur Fehlerbehebung



NI-DNA™ -Architektur

Seit der Gründung von Network Instruments 1994 entwickelt das Unternehmen alle Produktlösungen im eigenen Haus.

Die Network Instruments „Distributed Network Analysis (NI-DNA™)“-Architektur ermöglicht umfangreiche Analysefunktionen über eine einzige Schnittstelle und damit einen attraktiven Return On Investment (ROI).



Das Netzwerk-Monitoring-Modell zeigt das Zusammenwirken der NI-Lösungen.

## Observer Reporting Server

Als zentrale Management- und Reporting-Plattform stellt der Observer Reporting Server (ORS) alle gesammelten Netzwerk-Informationen in Berichte und Dashboards zusammen und ermöglicht so ein unternehmensweites Performance-Monitoring. ORS bietet eine sofortige Problemlösung per Drill-Down und weist pro-aktiv auf Performance-Probleme hin.

## GigaStor

Als Langzeit-Analyse - System erfasst GigaStor detaillierte Netzwerk-Informationen in Echtzeit und bietet eine retrospektive Analyse durch Speicherung der erfassten Daten ohne Informationsverluste. Zurückliegende Ereignisse können somit sofort analysiert werden, eine zeitaufwendige Reproduktion eines Fehlerszenarios entfällt.

## Observer

Die Observer-Lösung sammelt Netzwerk-Informationen und bietet Expert-Analysen zur effizienten Fehlersuche und Problemlösung an.

## Observer Infrastructure

Während Observer und GigaStor insbesondere das Kommunikationsverhalten im Netz analysieren, unterstützt die Observer Infrastructure - Lösung (OI) die Überwachung der Netzwerk-Systeme (Server, Switches, Router, etc.). OI ermöglicht eine grafische Darstellung der Netzwerk-Topologie und der gesammelten Statistik-Daten (SNMP, WMI, WSD, NBAR, IP SLA, WAAS).

# Observer Reporting Server (ORS)

## Unternehmensweites Performance Monitoring mit direktem Drill-Down zur Fehleranalyse.

Als zentrale Management- und Reporting-Plattform stellt der Observer Reporting Server (ORS) alle gesammelten Netzwerkinformation in Berichte und Dashboards zusammen und ermöglicht so ein permanentes und unternehmensweites Performance-Monitoring. Das ORS bietet eine sofortige Problemlösung per Drill-Down bis zur Paketebene und weist pro-aktiv auf Performance-Probleme hin.



ORS-Dashboard

## Echtzeit-Reports

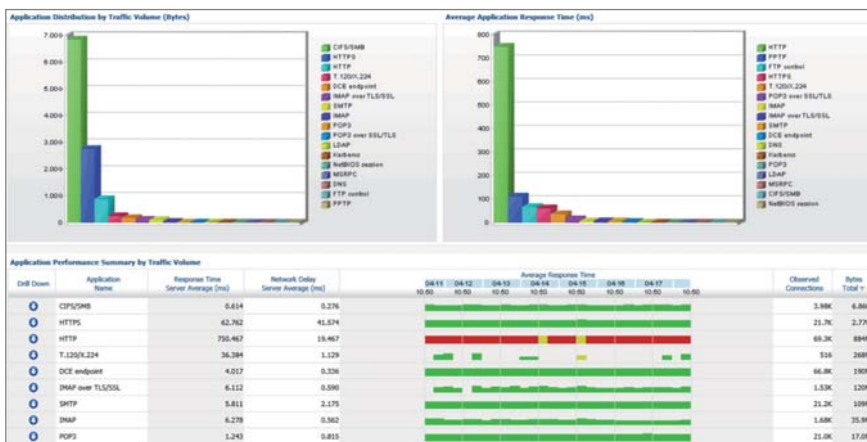
ORS bietet die Analyse des Datenverkehrs einzelner Verbindungen oder Benutzer. Reports werden in Echtzeit mit korrespondierenden Observer Suite-, GigaStor- und Probe-Lösungen aktualisiert und liefern u.a. folgende Möglichkeiten:

- Drill-Down zur sofortigen Analyse einzelner Verbindungen und Benutzer
- Eingrenzung der Fehlerursache mittels wichtiger Applikationsmetriken
- Erkennung langfristiger Trends



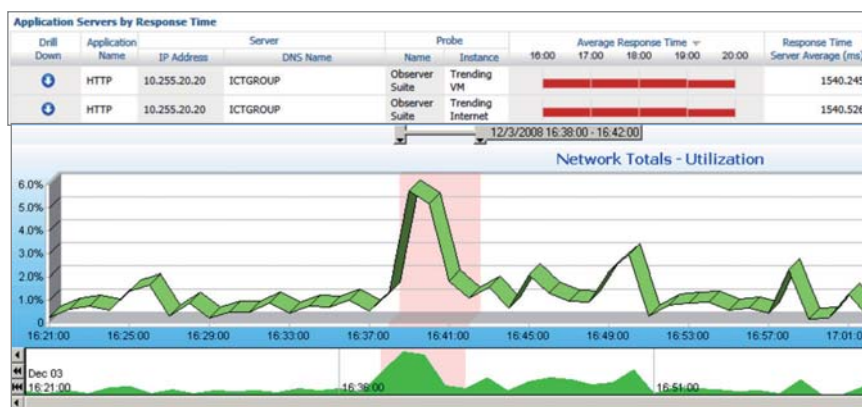
## Per Drill-Down bis zur Paketebene

In Verbindung mit GigaStor ermöglicht der Observer Reporting Server eine sofortige Bewertung aufgetretener Ereignisse, auch wenn sie bereits länger zurückliegen. Aus dem ORS heraus können per Drill-Down die Expert-Analysen mit den gesammelten Paketdaten der GigaStor direkt durchgeführt werden. Eine solche retrospektive Analyse unterstützt die Untersuchung des Netzwerkverkehrs vor, während und nach einem Ereignis.



Übersicht der meistgenutzten Applikationen in ORS (Anomalien rot markiert).

Der Observer Reporting Server ist als Stand-Alone-Lösung verfügbar und kann in Verbindung mit Observer Suite gleichzeitig Netzwerkdaten aus weiteren Observer Probes, NetFlow-Geräten und anderen Quellen im gesamten Netzwerk sammeln.



Anomalie-Analyse per Drill-Down von ORS in GigaStor.

## Retrospektive Netzwerk-Analysen reduzieren den Zeitaufwand einer Fehlersuche (Mean Time To Repair – MTTR)

Schon ein partieller Ausfall der IT-Infrastruktur für einen kurzen Zeitraum kann in Kosten von mehreren Tausend Euro resultieren. Im Fehlerfall ist es entscheidend, die Ursache des Problems schnell einzugrenzen respektive zu beheben. GigaStor ermöglicht mittels Zeit-Navigation eine schnelle Ermittlung des relevanten Fehler-Zeitraums und unterstützt durch Langzeit-Datenerfassung eine proaktive Lösung des Problems (insbesondere bei sporadischen Fehlern).



**GigaStor Portable**  
 • Transportable design  
 • 2 and 4 TB capacity  
 • 1 and 10 Gb networks



Rack Size 2U Storage 2 TB

**GigaStor Standard**  
 • Remote branch/network edge  
 • 2 TB capacity for 1 Gb networks  
 • 4 TB capacity for 1 and 10 Gb networks



Rack Size 3U Storage 4 TB



Rack Size 4U Storage unlimited

**GigaStor SAN**  
 • Data center, long-term retention  
 • SAN capacity virtually unlimited  
 • 1 and 10 Gb networks

All appliances use the Network Instruments-designed Gen2™ capture card



Rack Size 5U Storage 8 TB - 48 TB

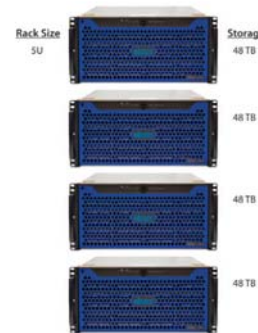
**GigaStor Upgradeable**  
 • Data center/branch facilities  
 • Field upgradeable without removal from rack  
 • 8 to 48 TB capacity  
 • 1 and 10 Gb networks



Rack Size 5U Storage 48 TB  
 +48 TB

**GigaStor Expandable**  
 • Data center/large branch  
 • Field expandable  
 • 48 to 96 TB capacity  
 • 1 and 10 Gb networks

**GigaStor SAS**  
 • 576 TB capacity  
 • 1 and 10 Gb networks



Rack Size 5U Storage 48 TB  
 48 TB  
 48 TB  
 48 TB

**GigaStor 10 Gb Wire Speed**  
 • Large data center/enterprise core  
 • World's fastest 10 Gb write-to-disk appliance  
 • 192 TB capacity  
 • 10 Gb line rate

Übersicht der GigaStor-Lösungen.

GigaStor ermöglicht aufgrund ihrer großen Speicherkapazität (bis zu 576 TB) die Aufzeichnung des kompletten Datenverkehrs. In Kombination mit der Zeit-Navigation kann unmittelbar mit der Fehler-Analyse begonnen werden. Eine zeitaufwändige Nachstellung von Problemen entfällt.

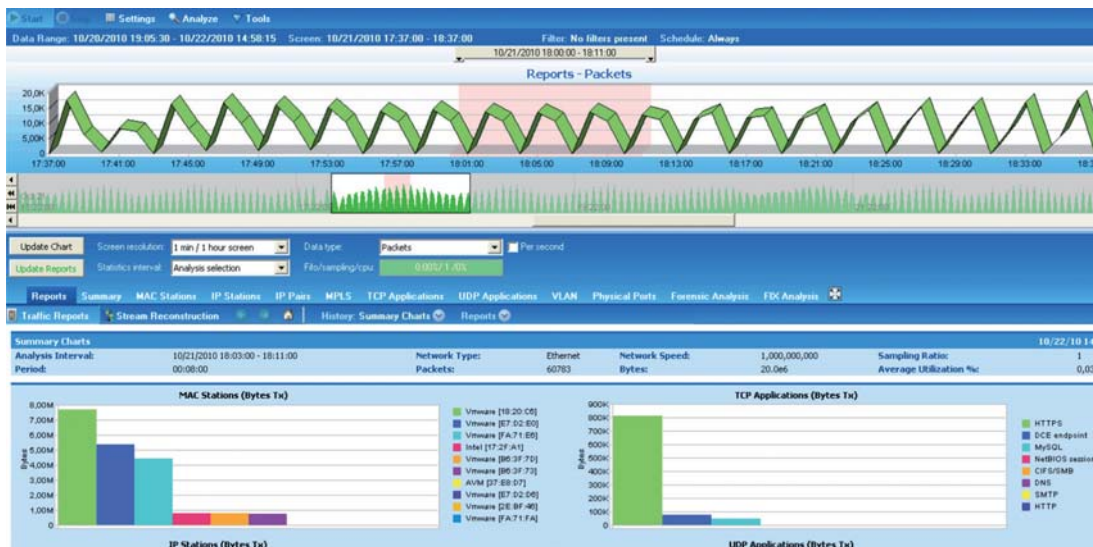
**GigaStor unterstützt u.a. folgende Schnittstellen:**

- Ethernet
- Gigabit-Ethernet
- 10 Gigabit-Ethernet
- STM1/4
- Fiber Channel.



## Reduzierung von Ausfallzeiten mittels proaktiver Fehlersuche

GigaStor unterstützt die ständige Erfassung von Netzwerk-Daten und ermöglicht mittels retrospektiver Analyse, die Zeit zurückzudrehen und eine mögliche Problem-Ursache schnell zu finden.



GigaStor-Control-Panel: Auswahl eines Zeitbereichs zur retrospektiven Analyse.

### Per Drill-Down zur Problemlösung

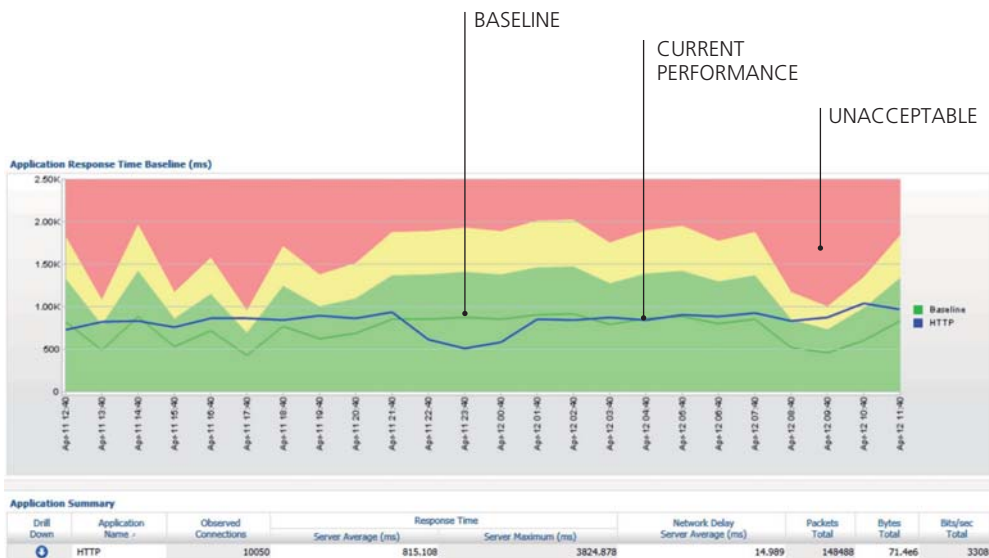
Die integrierte Expert-Analyse ermöglicht eine kurzfristige Problemlösung. Ausgehend von einer unternehmensweiten Netzwerk-Performance – Übersicht unterstützt GigaStor die Überwachung der Auslastung, Top Talker, Applikations-Performance, NetFlow-Daten, VoIP-Qualität, u. a..

# Vermeidung von Problemen bei Einführung neuer Applikationen



Performance-Übersicht zu mehreren Applikationen.

Bei der Einführung neuer Applikationen wie z.B. Unified Communications empfiehlt es sich, im Vorfeld ein Netzwerk-Baselining durchzuführen, um eventuelle Probleme und Veränderungen nach der Implementation schnell erkennen zu können. Mit GigaStor Trending-Reports kann man einfach und schnell Netzwerkstatistiken und Applikationsleistungen einsehen sowie eine Baseline (Normalzustand) ermitteln. Durch die Konfiguration von Alarm-Definitionen informiert das GigaStor-System, wann und wie die neue Applikation die bisherigen Netzwerkkennzahlen beeinträchtigt.



Baseline der Applikation HTTP.

Nach einer Alarmierung von Performance-Problemen durch GigaStor kann man sofort eine tiefer gehende Applikationsanalyse mit dem integrierten Expert-System durchführen.

- Isolierung von Transaktions-Problemen
- Darstellung von Laufzeit-Problemen
- Ermittlung langer Server-Antwortzeiten
- Überwachung von Applikations-spezifischen Störungen

## Überwachung von 10 GBit-Netzwerken

Network Instruments verfügt mit der eigenentwickelten Gen2 – Capture Card über eine der leistungsfähigsten Datenerfassungskarten für Gigabit- und 10 Gigabit-Netzwerke. Unterstützt werden bis zu acht Gigabit-Ports und vier 10Gigabit-Ports. Zur Vermeidung von unnötigem Datenverkehr im Netzwerk werden die erfassten Daten direkt auf der GigaStor-Probe gespeichert, indiziert und analysiert. Somit müssen die Daten nicht erst für eine detaillierte Analyse übertragen werden.

- Optimiert für 10 GBit-Analysen
- 16-Lane PCI-Express Karte
- Hardware-Filter und Statistikerfassung direkt auf der Gen2-Datenerfassungskarte
- Datenerfassung und Analyse direkt in der GigaStor-Probe



10 GBit Gen2 - Capture Card

## Erkennung von Security- und Compliance-Problemen

Sessions	Client IP	Server IP	Type	Bytes	StartTime	Duration	Description
	66.249.67.179	10.0.1.170	HTTP	22311 bytes	2008-12-03 16:59:35.973	05m:24.379s	<a href="http://www.networkinstruments.com">http://www.networkinstruments.com</a>
	209.85.238.8	10.0.1.170	HTTP	15732 bytes	2008-12-03 16:59:38.031	00.343s	<a href="http://www.networkinstruments.com">http://www.networkinstruments.com</a>
	94.213.66.133	10.0.1.170	HTTP	589000 bytes	2008-12-03 16:59:58.732		
	194.114.135.78	10.0.1.170	HTTP	255295 bytes	2008-12-03 16:59:59.229		
	85.65.221.172	10.0.1.170	HTTP	1665 bytes	2008-12-03 17:00:34.894		
	209.120.207.254	10.0.1.170	HTTP	483682 bytes	2008-12-03 17:00:42.534		
	201.192.231.50	10.0.1.170	HTTP	200641 bytes	2008-12-03 17:00:55.483		
	80.197.138.7	10.0.1.170	HTTP	1045264 bytes	2008-12-03 17:01:12.956		
	193.47.80.48	10.0.1.170	HTTP	10322 bytes	2008-12-03 17:01:24.907		

GigaStor ermöglicht Data-Mining und unterstützt tiefgehende Security-Analysen sowie die Überwachung der Einhaltung von Unternehmensregeln. Mit Hilfe der GigaStor kann man den Netzwerk-Verkehr im Original anschauen und wiedergeben und somit Sessions und Transaktionen genau untersuchen. GigaStor stellt nicht nur die Kommunikations-Verbindungen dar, sondern kann auch komplette Webseiten, VoIP-Gespräche, Dokumente oder E-Mails wiederherstellen und anzeigen.



Rekonstruktion von Web-Sessions.

# Observer Analyse- und Monitoring-Lösung

Die Observer-Lösung sammelt Netzwerk-Informationen und bietet Expert-Analysen zur effizienten Fehlersuche und Problemlösung an.

Der Observer bietet umfassende Analyse- und Monitoring-Features, u.a.:

- Detaillierte Analysen mit Drill-Down-Möglichkeiten
- Zeit-basierende Analysen
- Reporting
- Trending
- Alarme
- Applikations-Analysen
- VoIP-Analysen (UC)
- Überwachung von Netzwerkverbindungen
- Rekonstruktion von Daten und Verbindungen

Observer ist eine passive Lösung und benötigt insbesondere keine Agenten.

Mit Observer erhält man alle nötigen Werkzeuge zur Verkürzung einer Fehlersuche und Optimierung der Netzwerkverfügbarkeit.



Observer Expert Summary (Auflistung der analysierten Fehler).

# Übersicht

Mit der Observer-Lösung können Probleme schnell und sicher lokalisiert und deren Ursache mittels Expert-Hilfe bewertet werden. Dies kürzt signifikant die Zeit zur Fehlerbehebung. Die Expert-Hilfe unterstützt die automatische Interpretation von Netzwerk-Auffälligkeiten.



Expert Summary								
Packets: 49,488    Packets Processed: 49,488    %Packets Processed: 100,0%    Connections: 255								
Expert Data								
Compacted Connections    Selected Pair Individual Connections								
	Station1/Port (Connections) ->	<- Station2/Port	Protocol	Status	Packets ->	<- Packets	Response Time (ms) ->	<- Response Time (ms)
TCP Events	10.98.100.253/1152	194.77.76.28/443	HTTPS	🔴	219	2046	...	208.829
UDP Events	192.168.0.101/1891	207.46.108.30/1863	MSN	🔴	0	3	...	...
ICMP Events	10.98.100.12 (2)	212.184.6.14/80	HTTP	🔴	0	55	...	...
IPX Events	10.98.100.160/1124	213.73.102.28/110	POP3	🔴	112	89	...	341.079
	10.98.100.160 (2)	212.227.126.9/443	HTTPS	🔴	186	56	...	...
NetBIOS Events	10.98.100.160 (2)	212.227.15.131/110	POP3	🔴	28	3	...	50.346
	192.168.0.101 (2)	192.168.0.1/5678		🟢	0	4	...	...
VoIP Events	192.168.0.101/1978	80.239.144.22/80	HTTP	🟢	0	8	...	...
	192.168.0.100/2371	82.81.211.46/13176		🟢	0	1	...	...
Wireless Events	192.168.3.192/4415	84.114.131.163/27701		🟢	1	0	...	...
	10.98.100.53/2212	213.191.32.247/80	HTTP	🟢	0	1	...	...
Analysis	10.98.100.53/2175	140.124.32.202/443	HTTPS	🟢	1	0	...	...
Connection Dynamics	192.168.0.100/1584	128.6.73.73/27454		🟢	1	0	...	...
	192.168.0.100/1614	140.113.214.110/16881		🟢	0	1	...	...
Reconstruct Streams	192.168.0.100/1616	221.244.87.61/47947		🟢	1	0	...	...
TCP Dump	10.98.100.81/2676	66.186.66.240/28441		🟢	1	0	...	...
	10.98.100.81/2680	219.167.15.115/27317		🟢	1	0	...	...
Time Interval Analysis	10.98.100.81/2610	164.8.253.150/46935		🟢	1	0	...	...
Server Analysis	10.98.100.53/2186	81.218.13.17/443	HTTPS	🟢	1	0	...	...
	10.98.100.53/2192	82.43.141.47/443	HTTPS	🟢	1	0	...	...
What-If Analysis	10.98.100.53/2193	213.217.243.56/443	HTTPS	🟢	2	0	...	...
	10.98.100.53/2194	163.143.137.119/443	HTTPS	🟢	1	0	...	...
	10.98.100.53/2195	128.12.76.136/443	HTTPS	🟢	1	0	...	...
	10.98.100.53/2198	62.95.52.12/46926		🟢	1	0	...	...

Expert Analysis  
Client: 10.98.100.253/1152    Server: 194.77.76.28/443 [HTTPS]  
Client analysis: Client delay information is not available.  
Server analysis: Network connection is slow due to excessive retransmissions. Slow server and network connection.  
Right click on a column for a Expert Explanation about that item.

Analytisierte Fehler in TCP-Verbindungen.

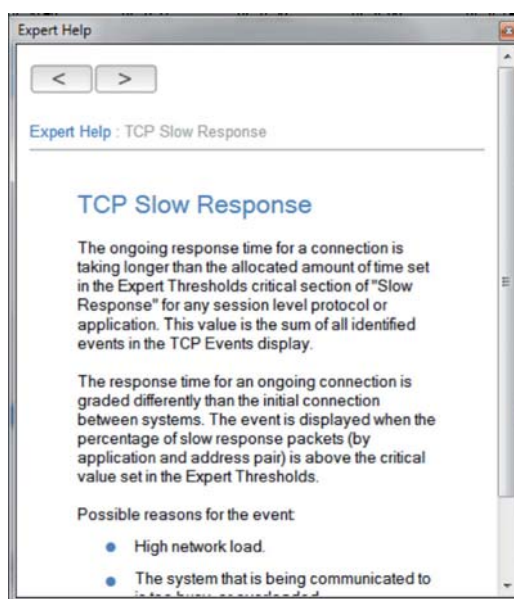
Darüber hinaus bietet die Observer-Lösung eine Applikations-Analyse bis OSI Layer-7. Die integrierte Applikations-Performance – Lösung überwacht geschäftskritische Anwendungen und ermöglicht eine frühzeitige Anomalie-Erkennung.

Weitere Analyse-Module sind im Paket enthalten:

- VoIP-Analysen (UC)
- Netflow-Analysen
- Applikations-Analysen
- Multi-Hop – Analysen  
(Analysen zur Isolierung auffälliger Netzwerksegmente)

## Über 600 Expert-Meldungen

Die Observer Expert-Hilfe enthält über 600 Expert-Ereignisse und unterstützt die automatische Interpretation von Netzwerk-Auffälligkeiten. Das Expert-System hilft, Fehler automatisch zu erkennen, zu alarmieren und schnellstmöglich zu beheben.



Fehlerbeschreibung im Expert-System.

Die Expert-Hilfe arbeitet in Echtzeit oder analysiert bereits aufgezeichnete Daten. Hierdurch erhält man die volle Flexibilität, Probleme bereits zu bearbeiten, während sie entstehen. Erkennt das Expert-System ein Problem, bietet es wahrscheinliche Ursachen und Hilfsmittel zur Lösung an.

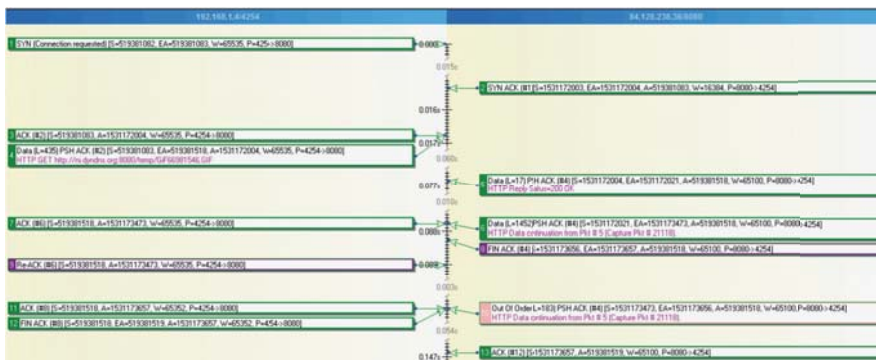
## Überwachung von IP-Diensten

Observer ermöglicht die genaue Überwachung von IP-Diensten, u.a:

- Frühzeitige Erkennung von problembehafteten Verbindungen
- Überwachung von Port-basierenden Applikationen (u.a. auf langsame Antwortzeiten)
- Unterscheidung von Netzwerk- und Anwendungs-Problemen
- Differenzierung zwischen LAN- und WAN - (Internet) Verkehr

## Verbindungs-Analyse mittels „Connection Dynamics“

Observer bietet die Darstellung „Connection Dynamics“ und ermöglicht so eine effiziente Verbindungsanalyse. Innerhalb der Connection Dynamics werden IP-basierte Kommunikations-Verbindungen graphisch dargestellt, sodass Latenz- und Antwortzeiten sofort erkennbar sind (Retransmissions und Dropped Packets werden farblich hervorgehoben). Observer ermöglicht so eine schnelle und sichere Eingrenzung von Verzögerungs- und Applikations-Problemen.

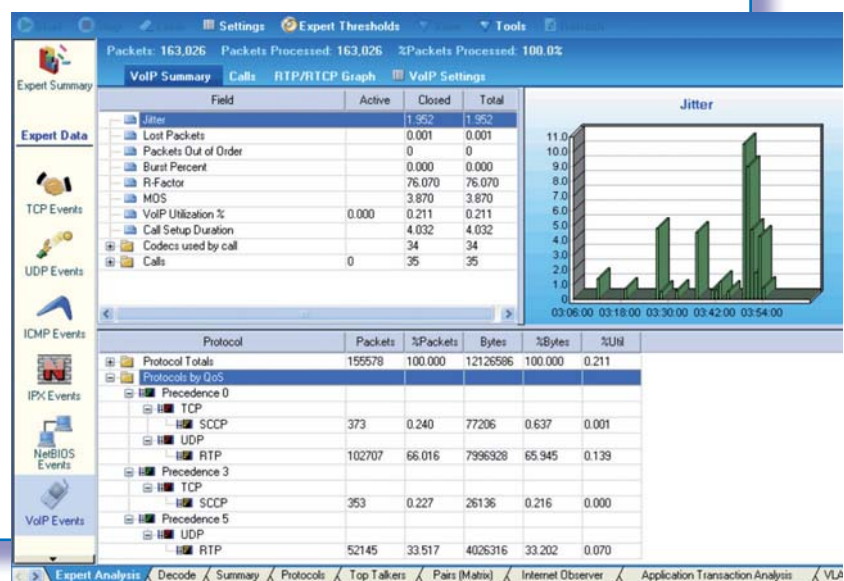


Ablaufdiagramm einer TCP-Verbindung (Connection Dynamics).

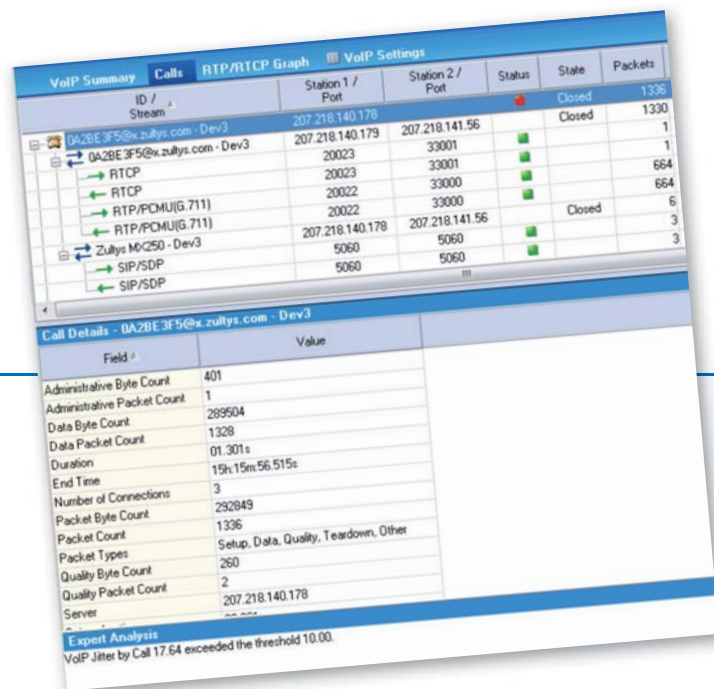
## Unified Communications (UC)

Observer unterstützt die Qualitätssicherung (Quality of Service / QoS) im Hinblick auf Unified Communications (UC):

- VoIP
- IPTV
- Video
- Instant Messaging



Übersicht zu UC-Verbindungen (VoIP-Statistiken).



Übersicht eines VoIP-Calls im Detail.

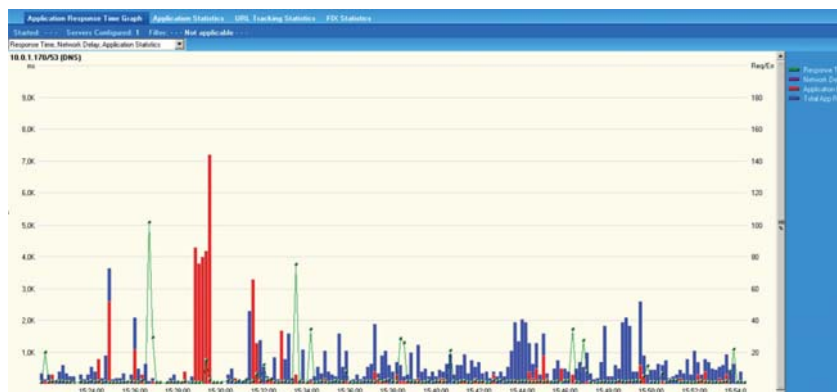
Zur Überwachung und Analyse der QoS-Kriterien (u.a. MOS, R-Factor, Jitter) stellt Observer u.a. folgende Funktionen zur Verfügung:

- Darstellung der Qualitäts- und Verkehrs-Daten in Echtzeit
- Detaillierte Einzel-Gesprächsansicht
- Konfiguration von Alarm-Meldungen
- Trace-File-Aggregation

## Application Performance Monitoring

Observer beinhaltet ein umfassendes Application Performance Monitoring – System und unterstützt beide Performance-Metriken:

- Überwachung des Antwortzeitverhaltens von Applikationen
- Darstellung von Layer-7 Informationen (z.B. SMB/Cifs - Fehlermeldungen)



Performance-Statistik zu einem DNS-Dienst.

## Zusätzliche Funktionen

Observer unterstützt noch eine Reihe weiterer Funktionen, u.a.:

### *Multi-Hop-Analysen*

Die Multi-Hop-Analyse ermöglicht die Ermittlung eines problembehafteten Netzwerkabschnittes. Observer analysiert gleichzeitig mehrere Netzwerkabschnitte, z.B. vor und nach einem Load-Balancer. So wird eine effiziente Lokalisierung und Eingrenzung von Fehlern unterstützt. (z.B. Netzwerkengpässe, Fragmentierung, Verzögerung, abreißende Verbindungen oder Paketverluste).

### *MPLS-Analyse*

Observer unterstützt eine tiefgehende Analyse von MPLS-Netzwerken und ermöglicht so z.B. die Überwachung einer MPLS-Migration.

### *Time-Interval-Analyse*

Observer unterstützt eine Ergebnis-Darstellung in einem vorgegebenen Zeitintervall. Die Time-Intervall-Analyse ermöglicht so z.B. eine schnelle Ermittlung von Antwortzeit-Spitzen.

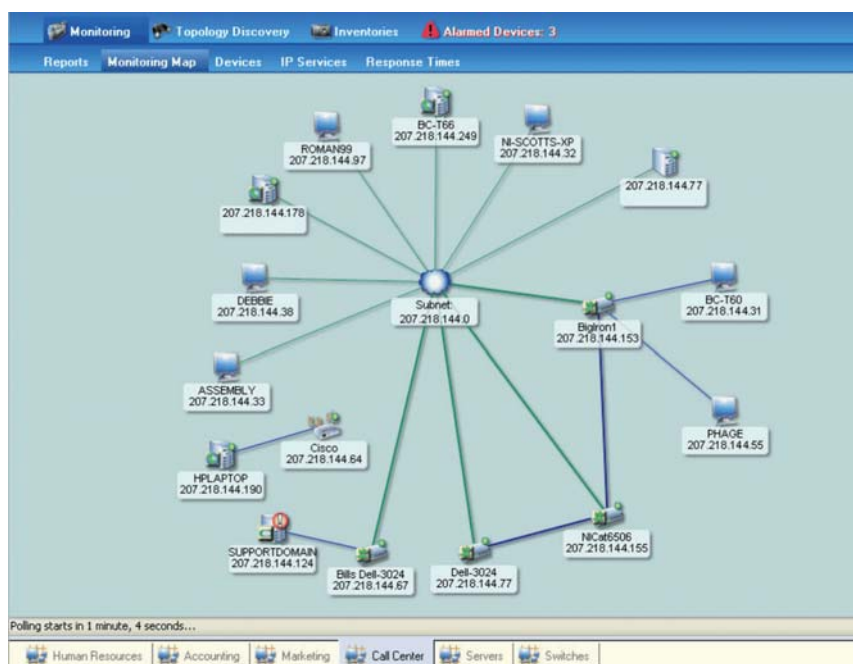
### *Stream-Reconstruction*

Observer ist in der Lage, erfasste Daten (wie z.B. Webseiten oder E-Mails) wieder herzustellen und in Klartext anzuzeigen. Dies erleichtert eine Analyse in sensiblen Bereichen und unterstützt eine Überwachung von Richtlinien (z.B. SOX).

# Observer Infrastructure (OI)

## Proaktives, unternehmensweites Device-Monitoring

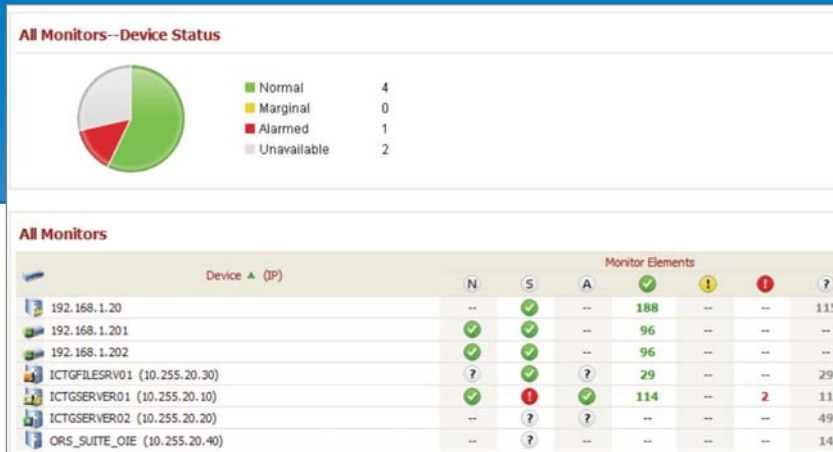
Observer Infrastructure (OI) ist eine umfassende Netzwerk-Überwachungs – Lösung, welche eine durchgehende Überwachung der Netzwerk-Geräte (Switches, Router, Server, etc.) ermöglicht. OI hilft, Ausfallzeiten zu reduzieren, Leistung zu optimieren sowie Ressourcen besser einzuplanen.



Topologie-Übersicht in Observer Infrastructure.

### OI beinhaltet:

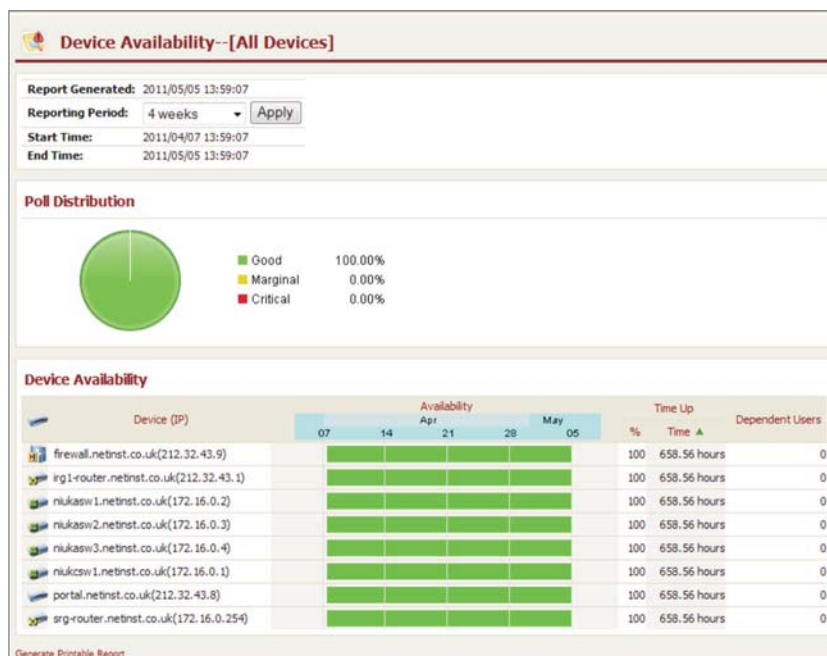
- Geräte - Überwachung (SNMP, WMI und WSD)
- Aktive IP SLA-Tests
- NBAR- und WAAS-Datensammlung
- Server-Überwachung
- Alarmierung
- Automatische Geräte-Identifizierung und -Mapping
- Aktive Geräte-Suche



Status-Übersicht der überwachten Geräte.

## Intuitive Netzwerküberwachung

Observer Infrastructure unterstützt die Suche nach Netzwerk-Geräten. OI stellt dar, um welche Geräte es sich handelt respektive wo und wie die Geräte im Netzwerk verbunden sind. OI ermöglicht die graphische und tabellarische Darstellung z.B. des gesamten Netzwerks, eines Segmentes oder auch einer über WAN angebotenen Lokation. OI stellt so eine intuitive Überwachung von Antwortzeit- und Leistungs-Metriken aller Geräte im Netzwerk zur Verfügung.



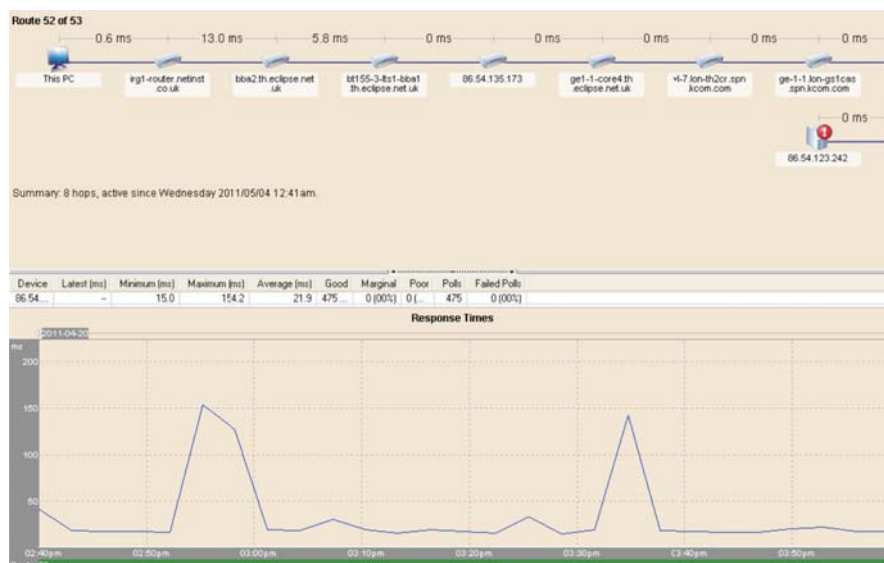
Übersicht zur Verfügbarkeit der überwachten Geräte.

## Geräte-Überwachung

Observer Infrastructure nutzt SNMP-, WMI- und WSD-Daten zur Sammlung und Bericht-Erstellung der Geräte-Informationen. Des Weiteren bietet OI auch die Konfiguration von Alarmen und Schwellwerten.

- Priorisierung von Problem-Meldungen, z.B. gemäß Auswirkung auf Geschäftsprozesse
- Überwachung der Verfügbarkeit von IP-Adressen, Ports, und weiterer Netzwerkressourcen
- Ermittlung von nicht erlaubten und unbekanntem Netzwerk-Geräten (Geräte-Inventur, auch per Scheduler)

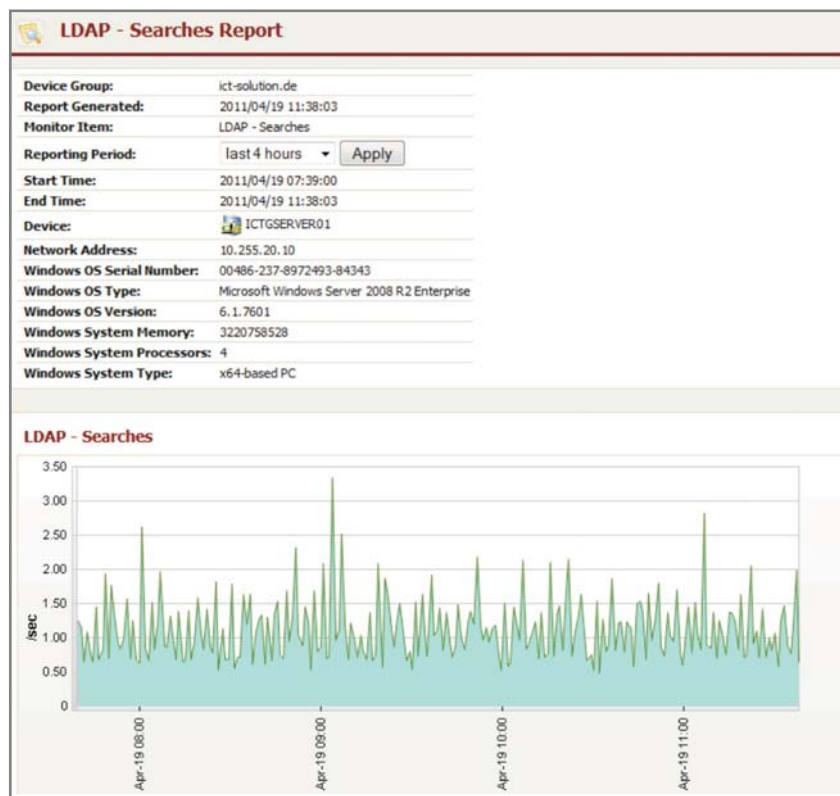
## Überwachung von Netzwerkrouten und SLAs



DELAY-Übersicht zu einer Netzwerkroute (7 Router).

Observer Infrastructure unterstützt die Überwachung von Verfügbarkeit und Stabilität der Netzwerk-Verbindungen. OI entdeckt Netzwerk-Routen automatisch und ermittelt eine graphische Darstellung aller Netzwerkrouten. OI prüft permanent die Performance und alarmiert bei Änderungen oder Verzögerungen. Das Erkennen solcher Änderungen (z.B. Route-Flapping) ist u.a. notwendig zur Einhaltung von SLAs.

## Individuelles Reporting



Statistik-Report zu einem überwachten LDAP-Dienst.

Berichte beinhalten u.a.:

- Alarme
- Statistiken nach Geschäftsbereichen
- Geräte-Ereignisse
- Antwortzeiten

OI unterstützt auch die Registrierung und Dokumentation von Änderungen (z.B. bei Austausch entnehmbarer Festplatten, installierte Software, etc.). Observer Infrastructure ermöglicht Inventuren (automatisch oder ad-hoc) sowie die Alarmierung für spezifische WMI-, SNMP- und WSD-Objekte.

## Alarmierung

**Alarms Report**

Device Group: ict-solution.de  
 Report Generated: 2011/04/19 11:35:31  
 Last Poll Time: 2011/04/19 11:34:33

- There are **10** devices (**10** alarm-enabled) in Device Group
- **2** monitor elements are in **alarmed** state:
  - the **system** category: monitor elements of **1** device are in **alarmed** state

Device (IP)	Monitor Elements	Alarms
ICTGSERVER01 (10.255.20.10)	N S A Monitor alarms: LogicalDisk - % Disk Time -- E: (100.000%), LogicalDisk - % Disk Time -- HarddiskVolume1 (100.000%)	

Alarm-Report in Observer Infrastructure.

Observer Infrastructure unterstützt eine automatische Alarmierung (z.B. „Gerät nicht erreichbar“ oder „schlechte Antwortzeit“) in verschiedenen Varianten, u.a.:

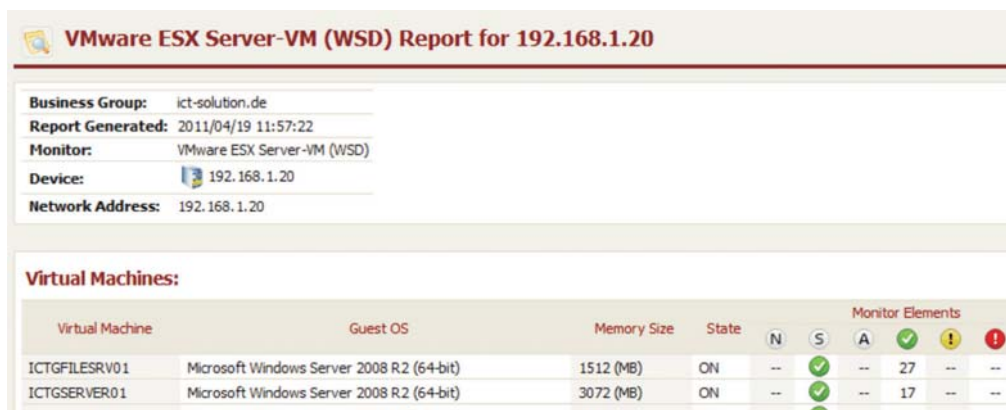
- Email- und Pager-Benachrichtigung
- Ausführung eines Skriptes oder Programms
- Versendung eines SNMP-Traps
- Start/Stop eines spezifischen Dienstes
- Log-Eintrag in einem Syslog-Server

Alarm-Berichte beinhalten:

- Alarme nach Geschäftsbereichen und / oder Netzwerkrouten
- Drill-Down zur Netzwerk-Geräte – Statistik
- Graphische Darstellung und Vergleiche über angegebene Zeiträume

## WSD-Applikationsdaten

Web Service Data (WSD) sammelt analog zu SNMP und WMI Leistungsstatistiken zu Applikationen. OI nutzt WSD zur Erstellung von Leistungsmetriken von VMware™, ESX™ Server und Cisco WAAS™.



**VMware ESX Server-VM (WSD) Report for 192.168.1.20**

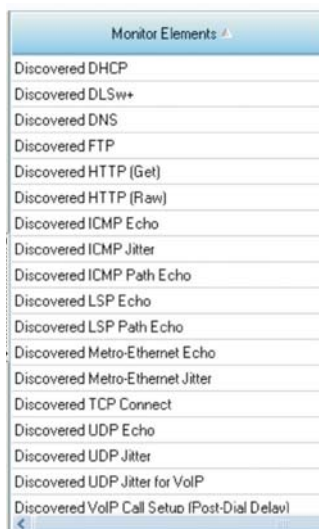
Business Group: ict-solution.de  
 Report Generated: 2011/04/19 11:57:22  
 Monitor: VMware ESX Server-VM (WSD)  
 Device: 192.168.1.20  
 Network Address: 192.168.1.20

**Virtual Machines:**

Virtual Machine	Guest OS	Memory Size	State	Monitor Elements					
				N	S	A	✓	!	✗
ICTGFILESRV01	Microsoft Windows Server 2008 R2 (64-bit)	1512 (MB)	ON	--	✓	--	27	--	--
ICTGSERVER01	Microsoft Windows Server 2008 R2 (64-bit)	3072 (MB)	ON	--	✓	--	17	--	--

WSD-Report eines ESX-Servers.

## Nutzung von IP SLA- und NBAR-Funktionalitäten



Monitor Elements
Discovered DHCP
Discovered DLSw+
Discovered DNS
Discovered FTP
Discovered HTTP (Get)
Discovered HTTP (Raw)
Discovered ICMP Echo
Discovered ICMP Jitter
Discovered ICMP Path Echo
Discovered LSP Echo
Discovered LSP Path Echo
Discovered Metro-Ethernet Echo
Discovered Metro-Ethernet Jitter
Discovered TCP Connect
Discovered UDP Echo
Discovered UDP Jitter
Discovered UDP Jitter for VoIP
Discovered VoIP Call Setup (Post-Dial Delay)

Monitor-Elemente für IP SLA.

Die IP Service Level Agreements (IP SLA™) und die Network Based Application Recognition (NBAR™) Funktion von Cisco™ ermöglichen eine Übersicht zur Applikations-Performance des gesamten Netzwerks. Diese Technologien ermöglichen eine Erweiterung der Netzwerk-Übersicht und Analyse-Möglichkeiten ohne den Einbau weiterer Probes.

- Überwachung von IP SLA-Operationen (z. B. UDP-Echo, IPv6 -Verkehr, TCP-Verbindungszeiten, DNS-Suche sowie HTTP-Get und -Response)
- Detaillierte Metriken über Cisco Router und Switches durch NBAR
- Aktive Simulation von VoIP-Gesprächen zwischen IP SLA-fähigen Geräten

## Integration in Observer Reporting Server (ORS)



ORS-Dashboard inklusive OI-Informationen.

Eine Integration von OI in den Observer Reporting Server (ORS) ermöglicht die Darstellung von Netzwerk-Infrastruktur und Geräte-Performance in Korrelation zur Applikations-Performance. Dies bietet u.a. folgende Vorteile:

- Einfache Erkennung der Geräte-Performance – Auswirkung auf die Gesamtleistung
- Integration von Reports aus weiteren Datenquellen (SNMP, WMI, WSD, WAAS, IP SLA, NBAR)
- Vergleich von Netzwerk- und Geräte-basierenden Daten in einem Report
- Verbesserte Kapazitätsplanung durch Langzeitbeobachtung der Geräte-Auslastung

OI kann mit GigaStor verlinkt werden und ermöglicht so eine signifikante Reduzierung der Fehlerbehebungszeit.





# IT UNION



**IT-Union GmbH & Co. KG**

BUSINESS IT-SOLUTIONS

[www.it-union.eu](http://www.it-union.eu)

KIEL – HAMBURG – KÖLN – FULDA – SUHL – SCHWEINFURT – STUTTGART – MÜNCHEN