

2011

IT@WORK # ProLog

EventLog Protokollierung

**Security Information Management
&
Security Event Management
nach geltendem Datenschutzgesetz**

NETZWERK #

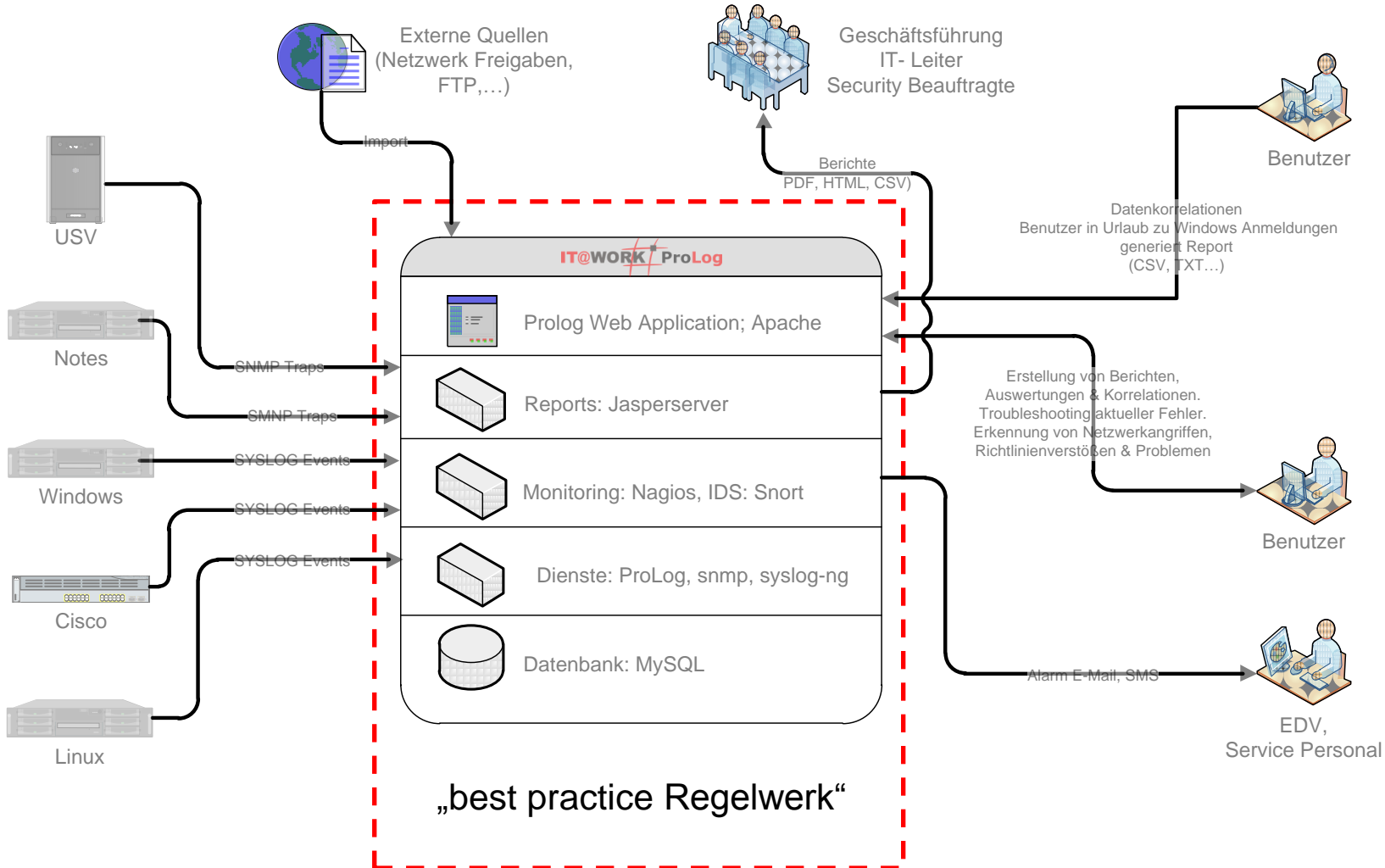
Gesetzliche Anforderungen

- „Der Vorstand hat (...) insbesondere ein Überwachungssystem einzurichten“
(§91 AktG)
- „Geschäftsführer haben (...) die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden“
(§43 GmbHG)
- „Dabei ist auch zu prüfen, ob Risiken der künftigen Entwicklung zutreffend dargestellt sind“
(§317 KonTraG)
- „Es ist darauf einzugehen, ob Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern“
(§321 KonTraG)

Betriebliche Anforderungen

- Schutz des geistigen Eigentums
- Aufbereitung von Daten für Revisionen/Audits/TÜV-Zertifizierungen/...
- Einhaltung des deutschen Datenschutzgesetzes
- Frühzeitige Erkennung von Systemausfällen
- Schutz vor Angriffen von Innen
- Missbrauchsfälle bedeuten Imageverlust, monetäre und zeitliche Aufwendungen

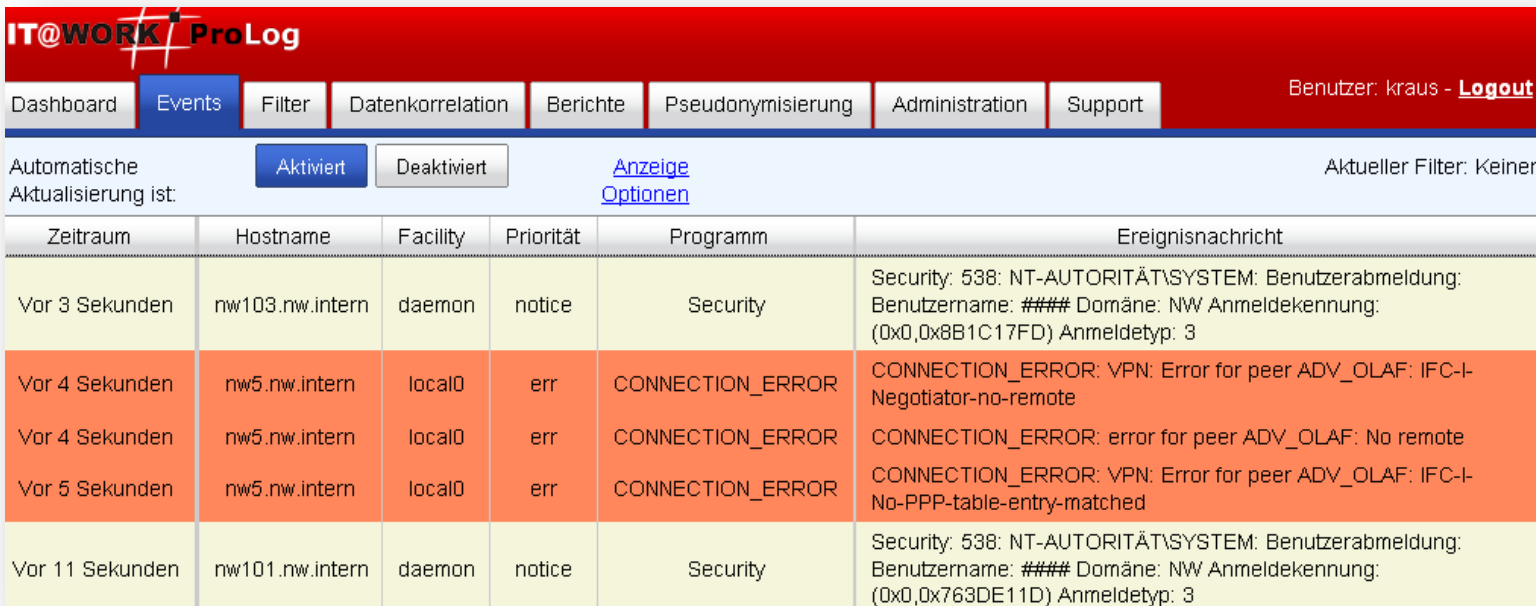
Funktionsweise von ProLog



Event Highlighting

IT@WORK ProLog									
Dashboard Events Filter Datenkorrelation Berichte Pseudonymisierung Administration								Benutzer: koch - Logout	
Automatisch Aktualisierung ist		<input type="button" value="Aktiviert"/>	<input type="button" value="Deaktiviert"/>	<<<< << 1 2 3 4 5 6 7 8 9 10 >>>>					Aktueller Filter: Cisco_Port_Security_Policy_Verletzungen
ID	Ereignistyp	IP-Adresse	Hostname	Facility	Priorität	Programm	Datum	Ereignisnachricht	
20112428	syslog	10.1.1.159		local7	notice	436	16.02.10 17:37:35	436: 18w4d: %SYS-5-CONFIG_I: Configured from console by vty0 (10.1.1.215)	
20109427	syslog	10.1.1.159		local7	err	435	16.02.10 17:28:39	435: 18w4d: %LINK-3-UPDOWN: Interface FastEthernet0/36, changed state to down	
20109423	syslog	10.1.1.159		local7	notice	434	16.02.10 17:28:38	434: 18w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/36, changed state to down	
20109284	syslog	10.1.1.159		local7	err	433	16.02.10 17:27:56	433: 18w4d: %LINK-3-UPDOWN: Interface FastEthernet0/37, changed state to down	
20109281	syslog	10.1.1.159		local7	notice	432	16.02.10 17:27:55	432: 18w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/37, changed state to down	
20109278	syslog	10.1.1.159		local7	crit	431	16.02.10 17:27:54	431: 18w4d: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0017.423b.2abd on port FastEthernet0/37.	
20109271	syslog	10.1.1.159		local7	warning	430	16.02.10 17:27:53	430: 18w4d: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/37, putting Fa0/37 in err-disable state	
20109018	syslog	10.1.1.159		local7	notice	429	16.02.10 17:27:25	429: 18w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/37, changed state to up	
20109017	syslog	10.1.1.159		local7	err	428	16.02.10 17:27:25	428: 18w4d: %LINK-3-UPDOWN: Interface FastEthernet0/37, changed state to up	
20108812	syslog	10.1.1.159		local7	notice	427	16.02.10 17:27:03	427: 18w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/36, changed state to up	
20108811	syslog	10.1.1.159		local7	err	426	16.02.10 17:27:03	426: 18w4d: %LINK-3-UPDOWN: Interface FastEthernet0/36, changed state to up	
20108689	syslog	10.1.1.159		local7	err	425	16.02.10 17:26:55	425: 18w4d: %LINK-3-UPDOWN: Interface FastEthernet0/35, changed state to down	
20108687	syslog	10.1.1.159		local7	notice	424	16.02.10 17:26:54	424: 18w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/35, changed state to down	
20108681	syslog	10.1.1.159		local7	crit	423	16.02.10 17:26:53	423: 18w4d: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0017.423b.2abd on port FastEthernet0/35.	
20108678	syslog	10.1.1.159		local7	warning	422	16.02.10 17:26:52	422: 18w4d: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/35, putting Fa0/35 in err-disable state	
20108587	syslog	10.1.1.159		local7	err	421	16.02.10 17:26:35	421: 18w4d: %LINK-3-UPDOWN: Interface FastEthernet0/34, changed state to down	
20108584	syslog	10.1.1.159		local7	notice	420	16.02.10 17:26:34	420: 18w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/34, changed state to down	
20108578	syslog	10.1.1.159		local7	crit	419	16.02.10 17:26:33	419: 18w4d: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 001a.e807.5c77 on port FastEthernet0/34.	

ProLog Pseudonymisierung



Zeitraum	Hostname	Facility	Priorität	Programm	Ereignisnachricht
Vor 3 Sekunden	nw103.nw.intern	daemon	notice	Security	Security: 538: NT-AUTORITÄT\SYSTEM: Benutzerabmeldung: Benutzername: ##### Domäne: NW Anmeldeerkennung: (0x0,0x8B1C17FD) Anmeldetyp: 3
Vor 4 Sekunden	nw5.nw.intern	local0	err	CONNECTION_ERROR	CONNECTION_ERROR: VPN: Error for peer ADV_OLAF: IFC-I-Negotiator-no-remote
Vor 4 Sekunden	nw5.nw.intern	local0	err	CONNECTION_ERROR	CONNECTION_ERROR: error for peer ADV_OLAF: No remote
Vor 5 Sekunden	nw5.nw.intern	local0	err	CONNECTION_ERROR	CONNECTION_ERROR: VPN: Error for peer ADV_OLAF: IFC-I-No-PPP-table-entry-matched
Vor 11 Sekunden	nw101.nw.intern	daemon	notice	Security	Security: 538: NT-AUTORITÄT\SYSTEM: Benutzerabmeldung: Benutzername: ##### Domäne: NW Anmeldeerkennung: (0x0,0x763DE11D) Anmeldetyp: 3

- ProLog ist das einzige System mit einer BDSG konformen Pseudonymisierung.
- Freigabe auf Wunsch nur nach N-Augen Prinzip

ProLog Webadministration

- keine Eingriffe im System nötig

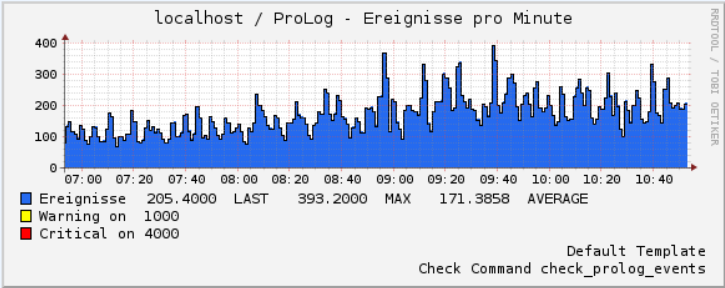
IT@WORK ProLog
Benutzer: kraus - [Logout](#)

Dashboard Events Filter Datenkorrelation Berichte Pseudonymisierung Administration Support




System Status Allgemeine Einstellungen Berechtigungen Überwachung Updates Share Verwaltung Backup Share

ProLog Datenbank Informationen

Datenbankgröße (Live):	277.41 MB	Gesamtanzahl der Events:	608.426	Neue Events innerhalb der letzten 24 Stunden:	221.711
Datenbankgröße (Archiv):	257.34 MB	Freier Speicherplatz DB-Partition:	31.42 GB		



Status der System Dienste

Dienst	Beschreibung	Erwarteter Status	Aktueller Status	Aktion
mysqld	MySQL Datenbank	Gestartet	Gestartet	
syslog-ng	Syslog Server	Gestartet	Gestartet	
prolog2file.pl	Schnittstelle zwischen Syslog und dem File Puffer	Gestartet	Gestartet	
prolog2db.pl	Schnittstelle zwischen den File Puffer und der ProLog Datenbank	Gestartet	Gestartet	

Inline-Edit

IT@WORK ProLog Benutzer: bartelzki - Logout

Dashboard Events **Filter** Datenkorrelation Berichte Pseudonymisierung Administration N-Augen Anfragen Support

Filter anzeigen Filter anlegen Filter importieren

Anzeige Optionen

Filtername	Beschreibung	Berichte	Im Dashboard anzeigen
A_MS_Security_538	MS Security 538 Zeitraum: letzte 7 Tage		
A_MS_Security_540			
Cisco_Security_Event_Port	Cisco Portsecurity Event in % Port		
Kiwi			
MegaLog			
MS_Security_12294_Versuch_Konto_zu_sperren	Es wurde versucht, ein Konto zu sperren.		
MS_Security_512_Windows_wird_gestartet	Windows wird gestartet.		
MS_Security_513_Windows_wird_heruntergefahren	Windows wird heruntergefahren.		
MS_Security_514_Authentifizierungspaket_geladen	Ein Authentifizierungspaket wurde durch die lokale Sicherheitsinstanz geladen.		
MS_Security_515_Vertrauenswuerdiger_Ameldevorgang	Ein vertrauenswürdiger Anmeldevorgang wurde bei der lokalen Sicherheitsinstanz registriert.		
MS_Security_516_Verlust_von_Sicherheitseignismeldungen	Die für die Warteschlangenverarbeitung von Sicherheitsereignismeldungen reservierten internen Ressourcen sind ausgelastet. Der Verlust von einigen Sicherheitsereignismeldungen ist eingetreten.		
MS_Security_517_Ueberwachungsprotokoll_wurde_geloescht	Das Überwachungsprotokoll wurde gelöscht.		
MS_Security_520_Systemzeit_wurde_geaendert	Die Systemzeit wurde geändert. Hinweis: Diese Überwachung wird in der Regel zweimal durchgeführt.		
MS_Security_521_Es_koennen_keine_Ereignisse_aufgezeichnet_werden	Es können keine Ereignisse aufgezeichnet werden.		
MS_Security_528_Erfolgreiche_Benutzeranmeldung	Ein Benutzer hat sich erfolgreich bei einem Computer angemeldet.		
MS_Security_529_gescheiterte_Benutzeranmeldung			
MS_Security_530_Ameldefehler_unzulaessige_Zeit	Anmeldefehler: Ein Anmeldeversuch wurde außerhalb der zulässigen Zeit unternommen.		
MS_Security_531_Ameldefehler_deaktiviertes_Konto	Anmeldefehler: Ein Anmeldeversuch mit einem deaktivierten Konto wurde unternommen.		

Datenkorellationen

IT@WORK ProLog

Dashboard | Events | Filter | Datenkorrelation | Berichte | Pseudonymisierung | Administration | N-Augen Anfragen | Support
Benutzer: bartetzki - [Logout](#)

Datenquellen anzeigen | Datenquellen anlegen | Datenkorellation anlegen | Datenkorrelationen anzeigen

1. Name der Korrelation

Benutzernamen

2. Auswahl der Datenquellen

Filter:

Datenquelle:

3. Bedingungen

WENN [+ Bedingung hinzufügen](#)
UND [+ Bedingung hinzufügen](#) [- Bedingung Entfernen](#)
UND [+ Bedingung hinzufügen](#) [- Bedingung Entfernen](#)
UND [+ Bedingung hinzufügen](#) [- Bedingung Entfernen](#)

IT@WORK ProLog
Version: 1.2.502
 Lizenziert für: ksk test
 Netzwerk GmbH, Kurze Strasse 40, 70794 Filderstadt-Bonlanden

PA - ProLog Appliance

Hardware:
Fujitsu Technology Solutions



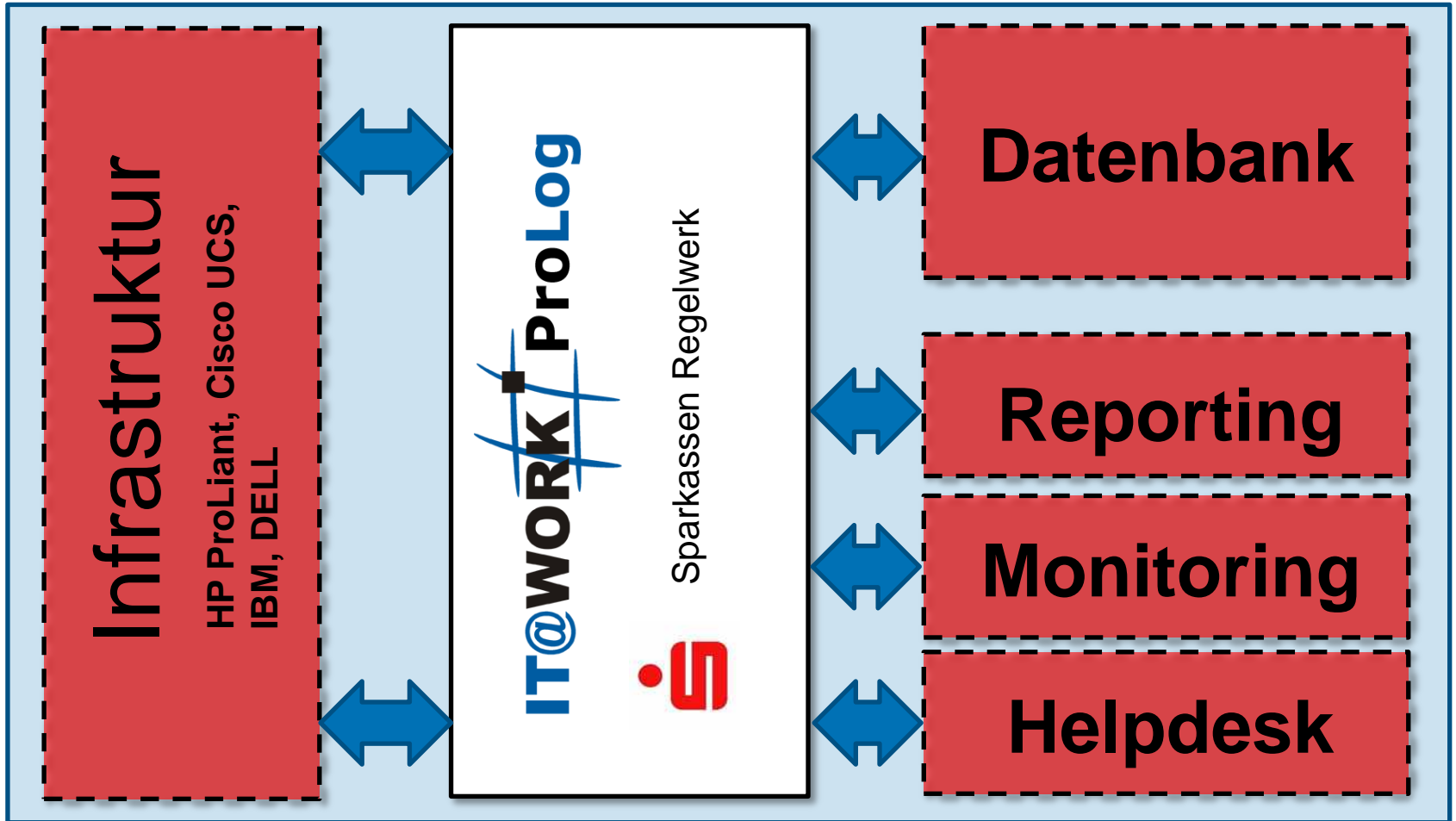
Modell	RX300 Sx (ab S5)
CPU:	2 x QuadCore CPU
RAM:	48 GB
RAID:	SAS 6G RAID 5/6 512MB + BBU
Festplatte:	6 x 450GB SAS 15K Hot Plug (2 x 450 im RAID 1; 4 x 450GB im RAID 10)
Netzwerk :	4 x 1Gbit Intel Ethernet

ProLog Facts*

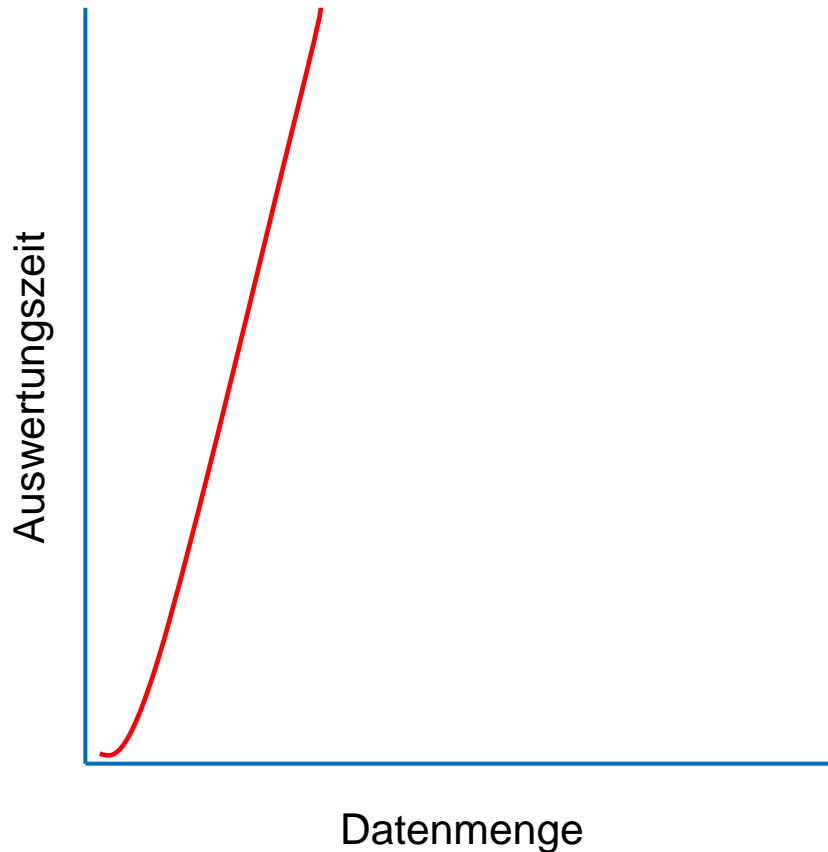
IT@WORK ProLog ist in der angebotenen Standard Version auf 35.000.000 Events/Tag, d.h. 25.000 Events/Minute ausgelegt. (Die maximale Speicherdauer bei kurzfristiger Spitzenauslastung ist vom verfügbaren Festplattenspeicher abhängig)

Maximale Speicherkapazität: ca. 400 Millionen Events
(bei empfohlener Mindestanforderung)

PCS – ProLog Customized Solution



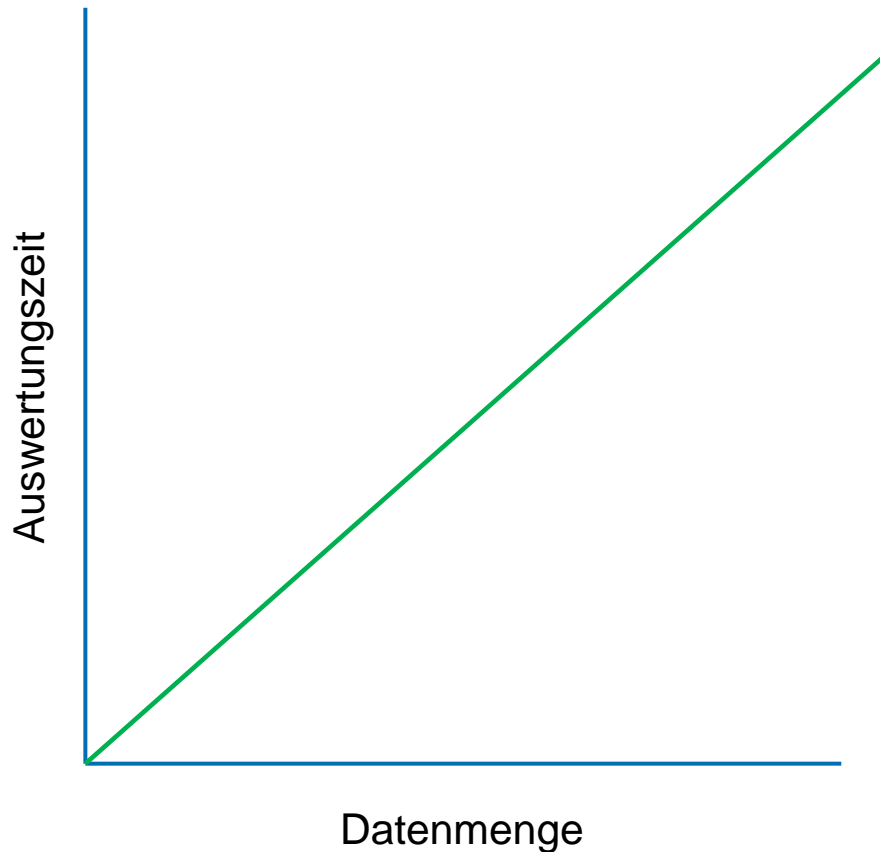
Typisches Datenbank Performance - Datenverhältnis



- bei stetig wachsender Datenmenge, wird permanent mehr Performance bei der Auswertung benötigt
- Längere Laufzeiten bei Auswertungen

Fazit:
Performance und Datenmenge skalieren optimaler Weise immer in Abhängigkeit

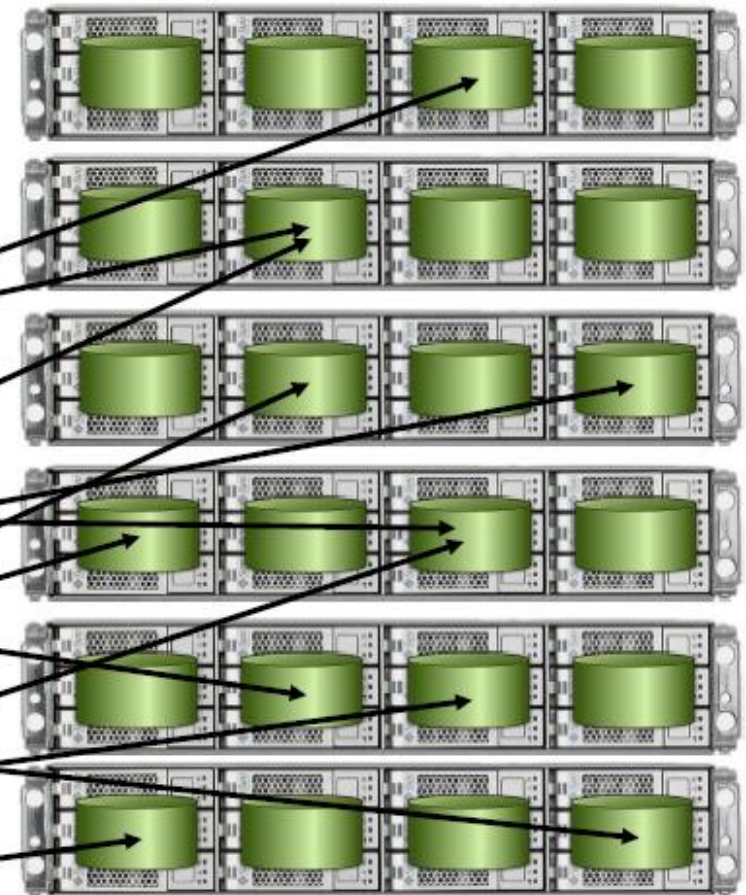
Performance – Datenverhältnis bei MPP Datenbanken



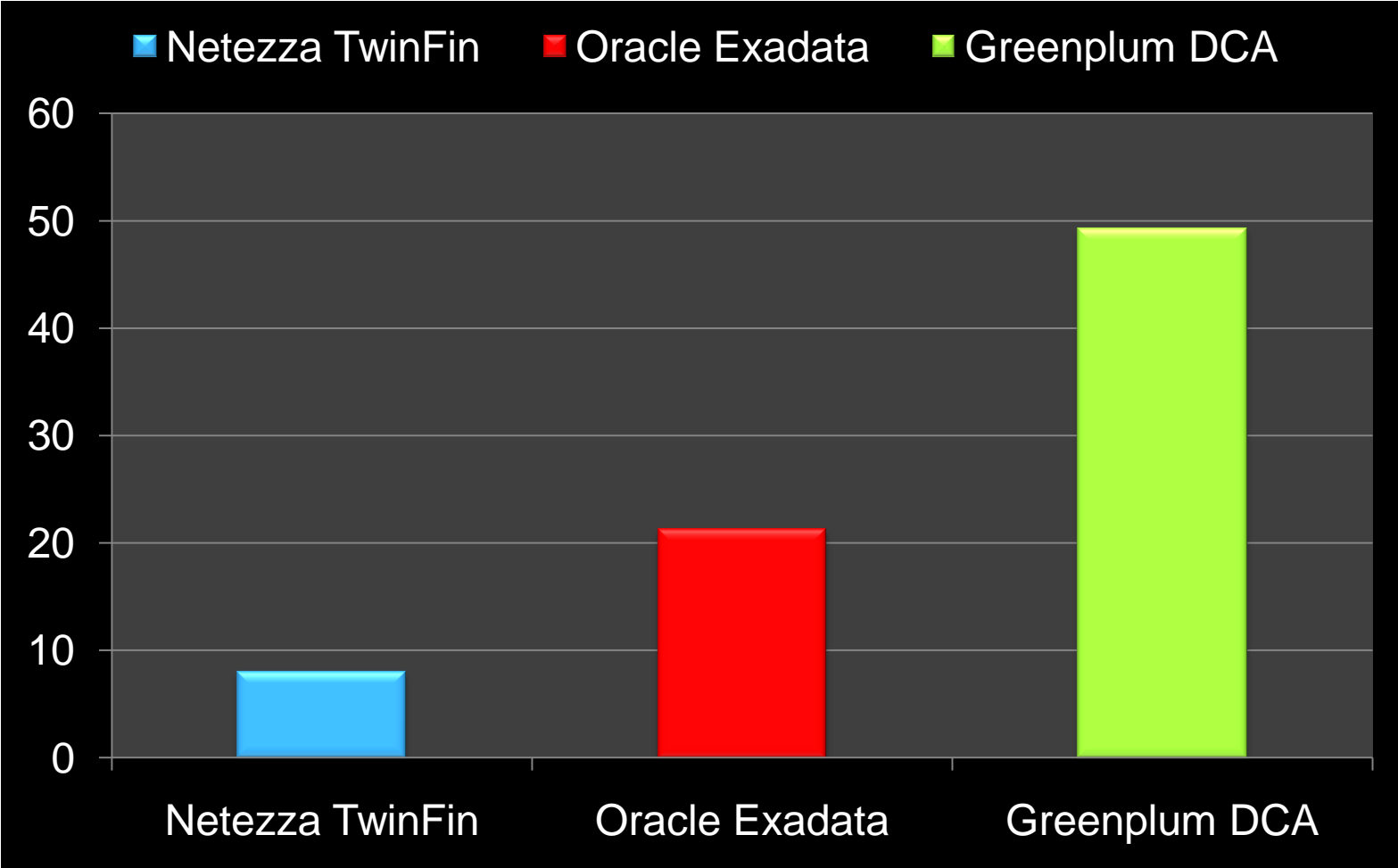
Gleichbleibendes Verhältnis
=
Gleichbleibende Leistung

Massiv Paralleles Prinzip

Order		
Order #	Order Date	Customer ID
43	Oct 20 2005	12
64	Oct 20 2005	111
45	Oct 20 2005	42
46	Oct 20 2005	64
77	Oct 20 2005	32
48	Oct 20 2005	12
50	Oct 20 2005	34
56	Oct 20 2005	213
63	Oct 20 2005	15
44	Oct 20 2005	102
53	Oct 20 2005	42
55	Oct 20 2005	55



Leseratenvergleich



Vorteile des MPP

MPP = Massive Parallel Processing

- Zwei oder mehr Server (mit einer CPU/RAM/Disk) arbeiten gleichzeitig an einer Anfrage
- Mehrere parallelisierte Segmente arbeiten zusammen
- Parallele Datenbankabfragen
- Parallele Nutzung der CPU Ressourcen

***Segmente** = Parallele Einheiten

„Shared Nothing“ Architektur

- Jedes Segment ist eine eigene Datenbank
- Sie bearbeiten nur ihre eigene Datenmenge
- Jedes Segment ist autark
- Dedizierte CPU Last
- Desizierter lokaler Segment-Storage

ProLog Customized Solution auf MPP Basis

- **Hardware unabhängig**
(HP, IBM, FTS, CISCO ...)
- **CPU:** Bis zu 192 CPU's
- **Maximale DB Cores:** 4608
- **Maximale Scan Rate:** 24GB/s
- **Maximal Parallele Server:** 384
- **Maximale Speicherkapazität:** ca. 3,456 Billionen Events

ProLog at the Max

	ProLog auf Basis von PCS GP	Oracle Exadata X2-8 (Full Rack)	Netezza TwinFin 12 (Full Rack)	Teradata 2580 (Full Rack)
Architecture	MPP Shared-Nothing	MPP Shared-Disk	MPP Shared-Nothing	MPP Shared-Nothing
Servers	16	2 DB 14 Storage	12	4
Cores	192 Intel E5670 (2.93 GHz)	128 DB 112 Storage Intel X7560 (2.26 GHz)	96 Intel E5460 (3.16GHz) + 96 FPGA	32 Intel Nehalem (2.66 GHz)
Scan (GB/s) w/o compression	24 GB/Sec	25 GB/Sec	10 GB/Sec	10 GB/Sec
Load (TB/Hr)	>10TB/Hr	5TB/Hr	2 TB/Hr	TBD
Capacity (TB) Usable w/o Compression	36 TB (600GB)	28 TB (600 GB)	32 TB	15 TB (450 GB)
Capacity (TB) Usable w/ Compression	144 TB	112 TB	128 TB	20 TB
Largest Multi-Rack Configuration	24 racks	8 racks	10 racks	10 racks
Max DB Cores Multi-rack Configuration	4608	1024	960	352

Vielen Dank!

