Eventbasiertes Monitoring am Flughafen München

Hubert Bösl
21.10.2014

Terminals:	Terminal 1	Terminal 2
Länge:	1081 m	980 m
Fläche:	198.000 m²	271.000 m²
Förderanlage:	18 km	40 km
Vorfelder:	600.000 m²	760.000 m²

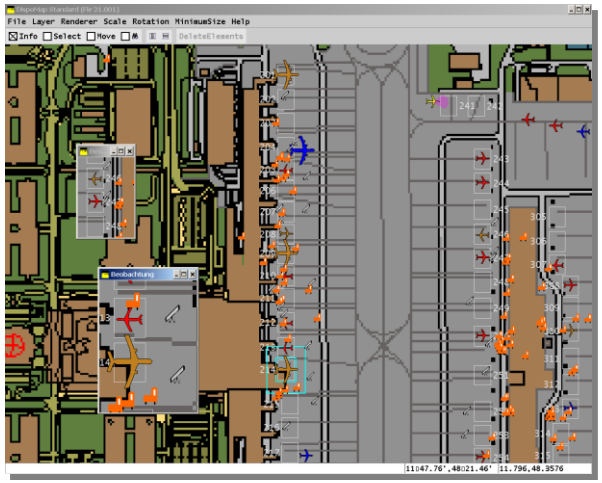
Firmengelände:	
Hangars:	90.300 m²
Treibstoff:	44.000.000 l
Geschäfte:	200
Parkplätze:	34.000

Einrichtungen:

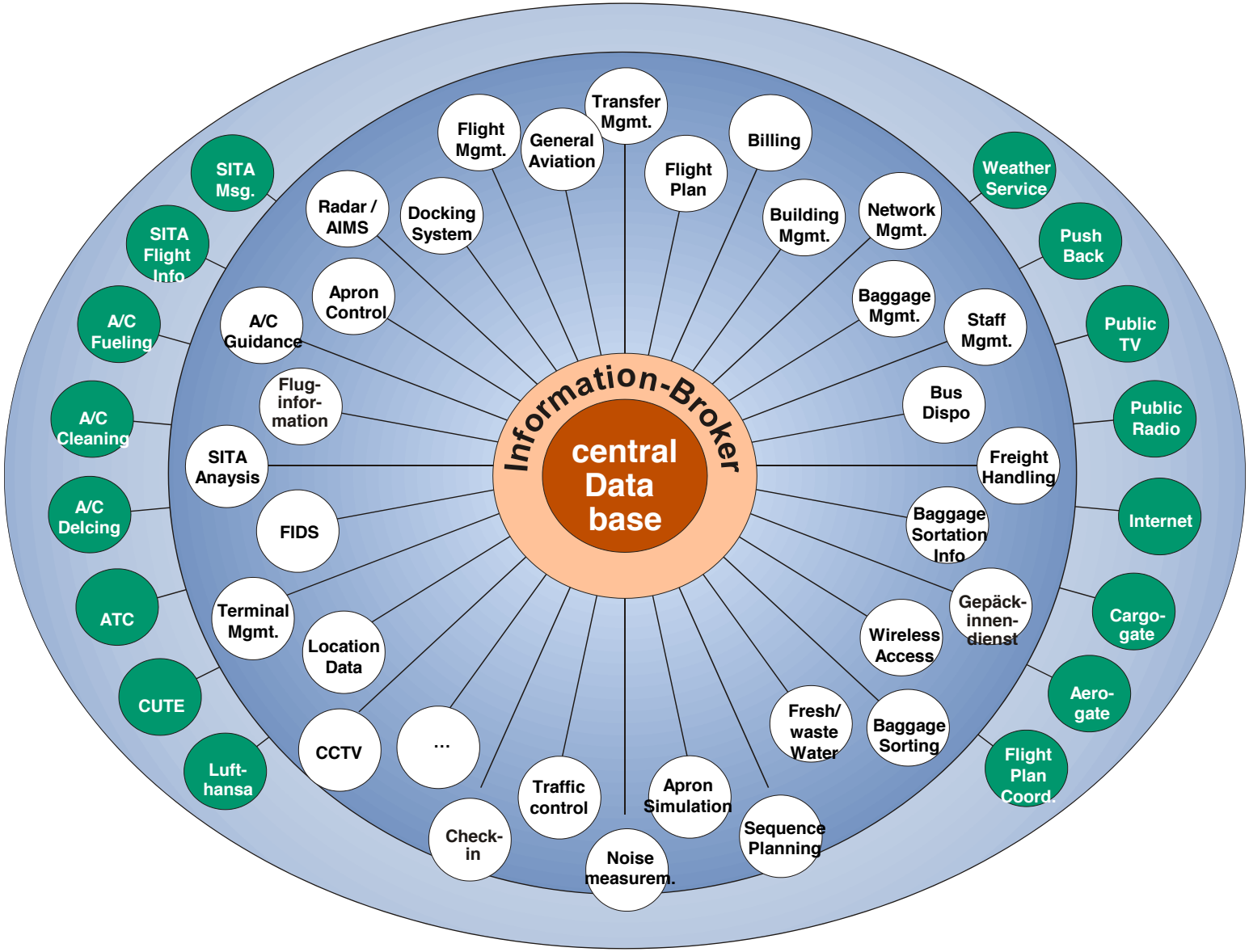
- 2 Hotels
- Tagungszentrum
- Kirchlicher Dienst
- Gebetsraum für Muslime
- Ärztezentrum und Klinik
- Kindergarten
- Feuerwehr

Flughafen IT

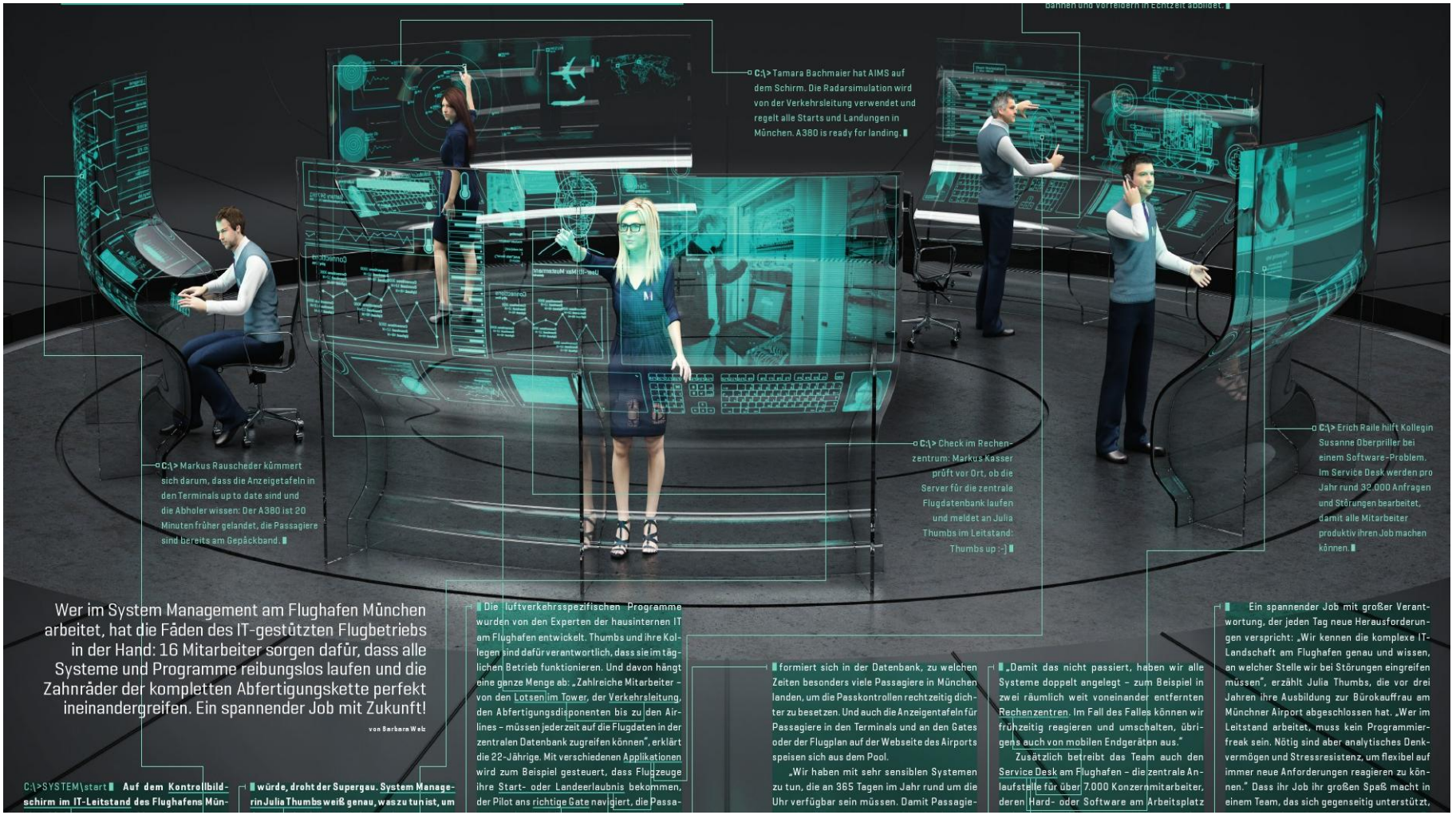
• PC‘s & Workstations	3.500
• LAN-Ports	18.000
• Phones	12.500
• FIDS Displays	1.850
• FIDS Accounts	2.800
• CCTV Cameras	2.150
• Server (in 2 Data Centers)	750
• SAN/NAS-Storage	1500 TB
• Applications	600
• Employes (IT)	200
• Customers	500
• External revenue	14 Mio Eur



FMG IT die Informationsdrehscheibe



IT Leitstand Flughafen München



C:\> Tamara Bachmaier hat AIMS auf dem Schirm. Die Radarsimulation wird von der Verkehrsleitung verwendet und regelt alle Starts und Landungen in München. A380 is ready for landing.

C:\> Markus Rauscheder kümmert sich darum, dass die Anzeigetafeln in den Terminals up to date sind und die Abholer wissen: Der A380 ist 20 Minuten früher gelandet, die Passagiere sind bereits am Gepäckband.

C:\> Check im Rechenzentrum: Markus Kasser prüft vor Ort, ob die Server für die zentrale Flugdatenbank laufen und meldet an Julia Thumbs im Leitstand: Thumbs up :-)

C:\> Erich Raile hilft Kollegin Susanne Oberpriller bei einem Software-Problem. Im Service Desk werden pro Jahr rund 32.000 Anfragen und Störungen bearbeitet, damit alle Mitarbeiter produktiv ihren Job machen können.

Wer im System Management am Flughafen München arbeitet, hat die Fäden des IT-gestützten Flugbetriebs in der Hand: 16 Mitarbeiter sorgen dafür, dass alle Systeme und Programme reibungslos laufen und die Zahnräder der kompletten Abfertigungskette perfekt ineinandergreifen. Ein spannender Job mit Zukunft!

von Barbara Welz

C:\>SYSTEM\start **Auf dem Kontrollbildschirm im IT-Leitstand des Flughafens Mün-**

würde, droht der Supergau. System Managerin Julia Thumbs weiß genau, was zu tun ist, um

Die luftverkehrsspezifischen Programme wurden von den Experten der hausinternen IT am Flughafen entwickelt. Thumbs und ihre Kollegen sind dafür verantwortlich, dass sie im täglichen Betrieb funktionieren. Und davon hängt eine ganze Menge ab: „Zahlreiche Mitarbeiter – von den Lotsen im Tower, der Verkehrsleitung, den Abfertigungsdisponenten bis zu den Airlines – müssen jederzeit auf die Flugdaten in der zentralen Datenbank zugreifen können", erklärt die 22-Jährige. Mit verschiedenen Applikationen wird zum Beispiel gesteuert, dass Flugzeuge ihre Start- oder Landeerlaubnis bekommen, der Pilot ans richtige Gate navigiert, die Passa-

formiert sich in der Datenbank, zu welchen Zeiten besonders viele Passagiere in München landen, um die Passkontrollen rechtzeitig dichter zu besetzen. Und auch die Anzeigentafeln für Passagiere in den Terminals und an den Gates oder der Flugplan auf der Webseite des Airports speisen sich aus dem Pool.

„Wir haben mit sehr sensiblen Systemen zu tun, die an 365 Tagen im Jahr rund um die Uhr verfügbar sein müssen. Damit Passagie-

„Damit das nicht passiert, haben wir alle Systeme doppelt angelegt – zum Beispiel in zwei räumlich weit voneinander entfernten Rechenzentren. Im Fall des Falles können wir frühzeitig reagieren und umschalten, übrigens auch von mobilen Endgeräten aus."

Zusätzlich betreibt das Team auch den Service Desk am Flughafen – die zentrale Anlaufstelle für über 7.000 Konzernmitarbeiter, deren Hard- oder Software am Arbeitsplatz

Ein spannender Job mit großer Verantwortung, der jeden Tag neue Herausforderungen verspricht: „Wir kennen die komplexe IT-Landschaft am Flughafen genau und wissen, an welcher Stelle wir bei Störungen eingreifen müssen", erzählt Julia Thumbs, die vor drei Jahren ihre Ausbildung zur Bürokauffrau am Münchner Airport abgeschlossen hat. „Wer im Leitstand arbeitet, muss kein Programmierfreak sein. Nötig sind aber analytisches Denkvermögen und Stressresistenz, um flexibel auf immer neue Anforderungen reagieren zu können." Dass ihr Job ihr großen Spaß macht in einem Team, das sich gegenseitig unterstützt,

Anforderungen Systemmonitoring

- Alle wichtigen Systeme überwachen
- Ausfall möglichst schnell bemerken
- Wichtige Themen hervorheben
- Unwichtige Meldungen unterdrücken
- Zusatzinformationen
- Zeitliche Abläufe erkennen

Einhaltung der Service Level

SL_Platin

ID	Icons	Last	Cnt.	Rule	State	Host	Level	Host	Application	Message
310847		60 min	1	nagios	WARN	fmg-le06	SL_Platin	fmg-le06	DHCP Pool 134.247.201.112	WARN - Addresses Free: 1, Used: 10, Pending: 0
305686		27 hrs	1	nagios	CRIT	ctv-rz2-vnx898a	SL_Platin	ctv-rz2-vnx898a	Disks	Bus 1, Enclosure 0, Disk 0 is Rebuilding, Bus 1, Enclosure 1, Disk 11 is Removed, 223 physical disks are OK. 8 Hotspares are ready.
305665		27 hrs	1	nagios	CRIT	ctv-rz2-vnx898a	SL_Platin	ctv-rz2-vnx898a	Faults	Faulted Subsystem: ctv-rz2-vnx898
290126		2014-09-25 08:38:58	1	live-check	CRIT		SL_Platin			Expected message did not arrive since 2014-09-25 08:30:00
224847		2014-09-18 17:26:57	1	nagios	WARN	vdbb-vprod	SL_Platin	vdbb-vprod	ORA vprod.USERS Tablespace	WARN - ONLINE, size 12.21 GB, used 8.58 GB, no autoextend, only 3.63 GB left (levels at 30.0%/10.0%), 1 data files (1 avail, 0 autoext)
76407		2014-09-05 10:37:04	1	nagios	WARN	vdbb2	SL_Platin	vdbb2	fs_/vdbb/oradata2	WARN - 91.1 % used (23.31 of 25.59 GB), (levels at 90.00/100.00 %), trend: +178.69 MB / 24 hours

SL_Gold_RB

ID	Icons	Last	Cnt.	Rule	State	Host	Level	Host	Application	Message
285708		2014-09-25 00:34:08	1	nagios_gol_rb	CRIT	extDNS	SL_Gold_RB	extDNS	HOST	CRITICAL - 134.247.251.215: rta nan, lost 100%

SL_Silber

ID	Icons	Last	Cnt.	Rule	State	Host	Level	Host	Application	Message
306781		19 hrs	1	nagios	WARN	xtimedb-xtprod47	SL_Silber	xtimedb-xtprod47	LOG /oracle/db/diag/rdbms /xtprod47/xtprod47/trace /alert_xtprod47.log	WARN - 1 WARN messages (Last worst: "ORA-00060: Deadlock detected. More info in file /oracle/db/diag/rdbms/xtprod47 /xtprod47/trace/xtprod47_ora_14961.trc.")
298284		2014-09-26 19:12:32	2	nagios	CRIT	cus-nas01	SL_Silber	cus-nas01	fs_/vol/sw_fs02_eco_data1/	CRIT - 90.6 % used (1291.45 of 1425.00 GB), (levels at 80.00/90.00 %), trend: +646.19 GB / 24 hours
297712		2014-09-26 14:40:46	1	nagios	CRIT	lx-dataexchange1	SL_Silber	lx-dataexchange1	ESX Guest Tools	CRIT - VMware Tools has never been installed
297713		2014-09-26 14:40:46	1	nagios	WARN	lx-dataexchange1	SL_Silber	lx-dataexchange1	ESX Heartbeat	WARN - No VMWare Tools installed, outdated or not running
268474		2014-09-24 23:57:45	2	nagios	WARN	uds4	SL_Silber	uds4	VN-Log-Messages	WARN - WARNING - VN-Log-Messages per Min: 19 (26 Msgs in 82 Sec)

SL_Bronce

ID	Icons	Last	Cnt.	Rule	State	Host	Level	Host	Application	Message
1112		3 min	1490	r9991	WARN		SL_Bronce	bv140	smartd	Device: /dev/sda, 11 Currently unreadable (pending) sectors
1113		3 min	1490	r9991	WARN		SL_Bronce	bv140	smartd	Device: /dev/sda, 11 Offline uncorrectable sectors

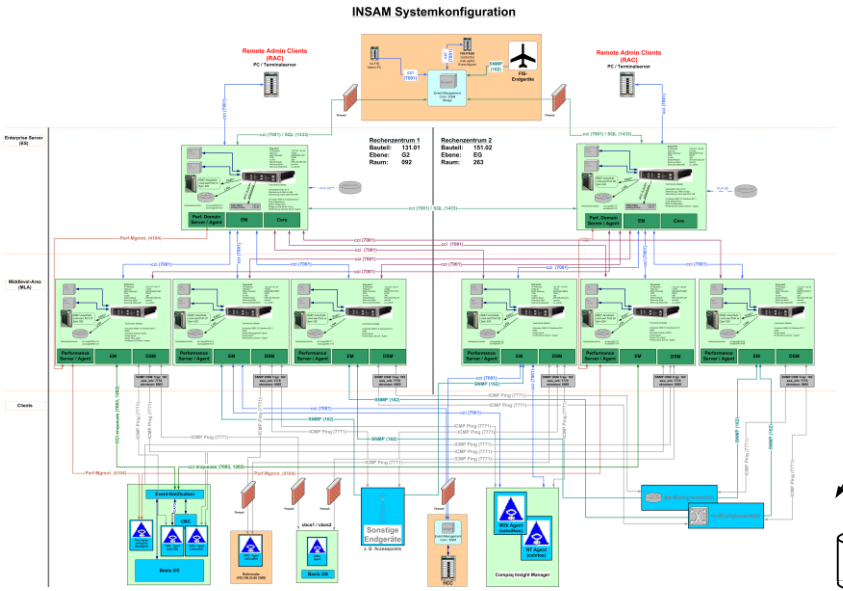
Entwicklung Systemmonitoring am Flughafen München

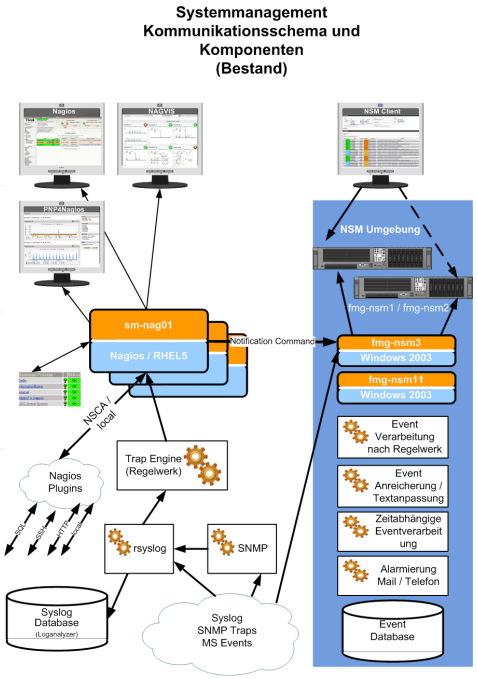
1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014

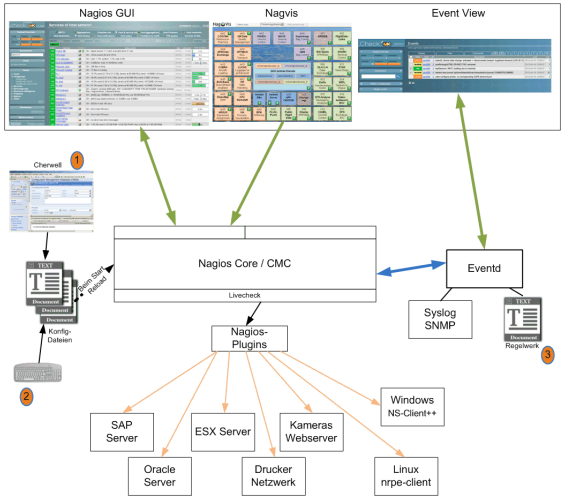
INSAM
(Integrated Network, System and Applikation Monitoring)

Einführung Nagios
(CA Eventkonsole)

Ablösung Eventkonsole
(Einführung check_mk)

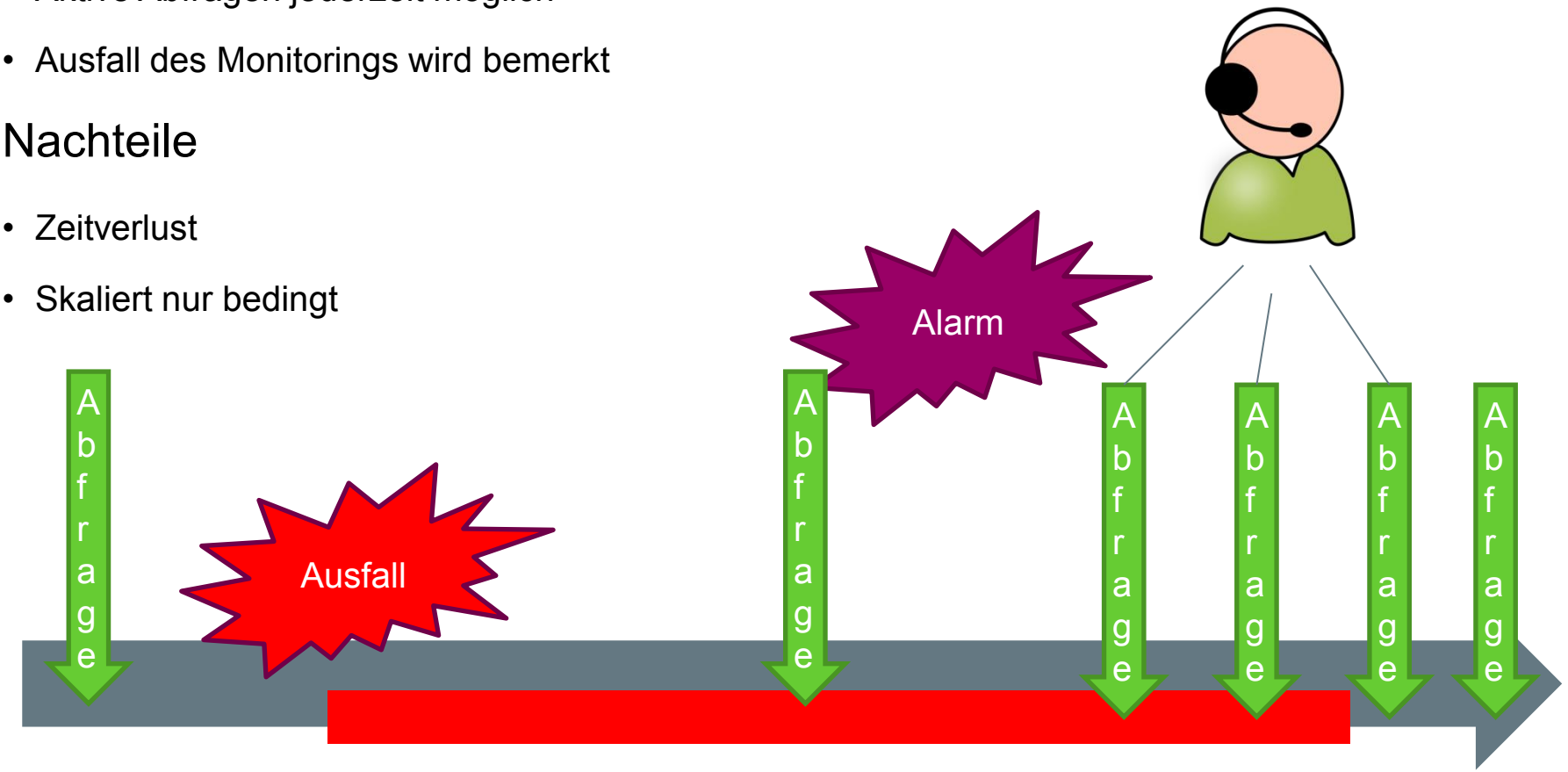






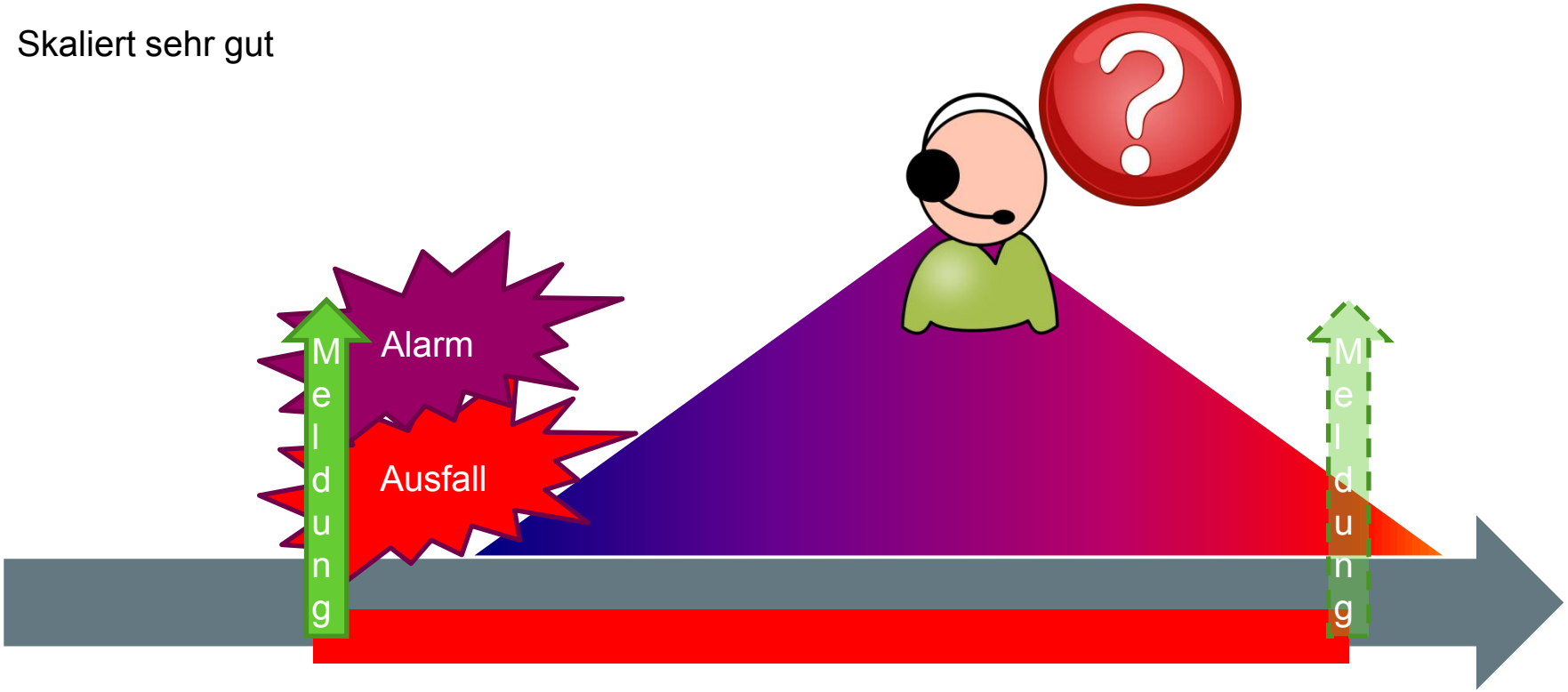
Status orientiertes Monitoring

- Vorteile
  - Aktive Abfragen jederzeit möglich
  - Ausfall des Monitorings wird bemerkt
- Nachteile
  - Zeitverlust
  - Skaliert nur bedingt



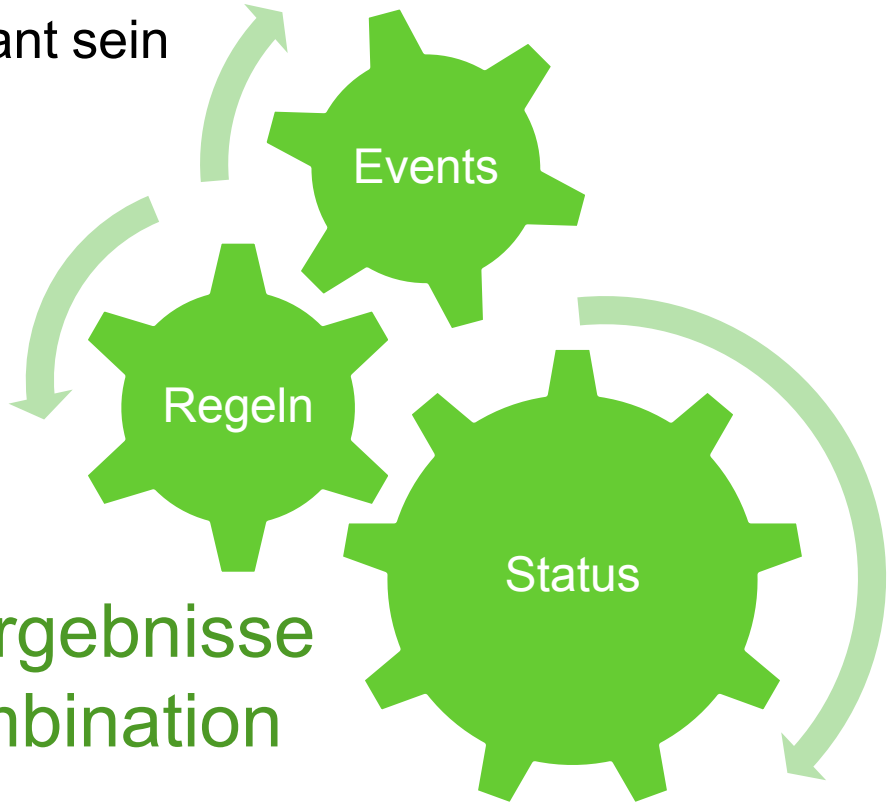
Event orientiertes Monitoring

- Vorteile
  - Bei vielen Produkten integriert
  - Schelle Alarmierung
  - Skaliert sehr gut
- Nachteile
  - Verlust von Meldungen möglich
  - Oft keine OK Meldung vorgesehen



Warum Eventbasiertes Monitoring

- Nicht alle Quellen können aktiv abgefragt werden
- Eine statusbasierte Überwachung kann nie alle Aspekte abdecken
- Auch OK Meldungen können interessant sein



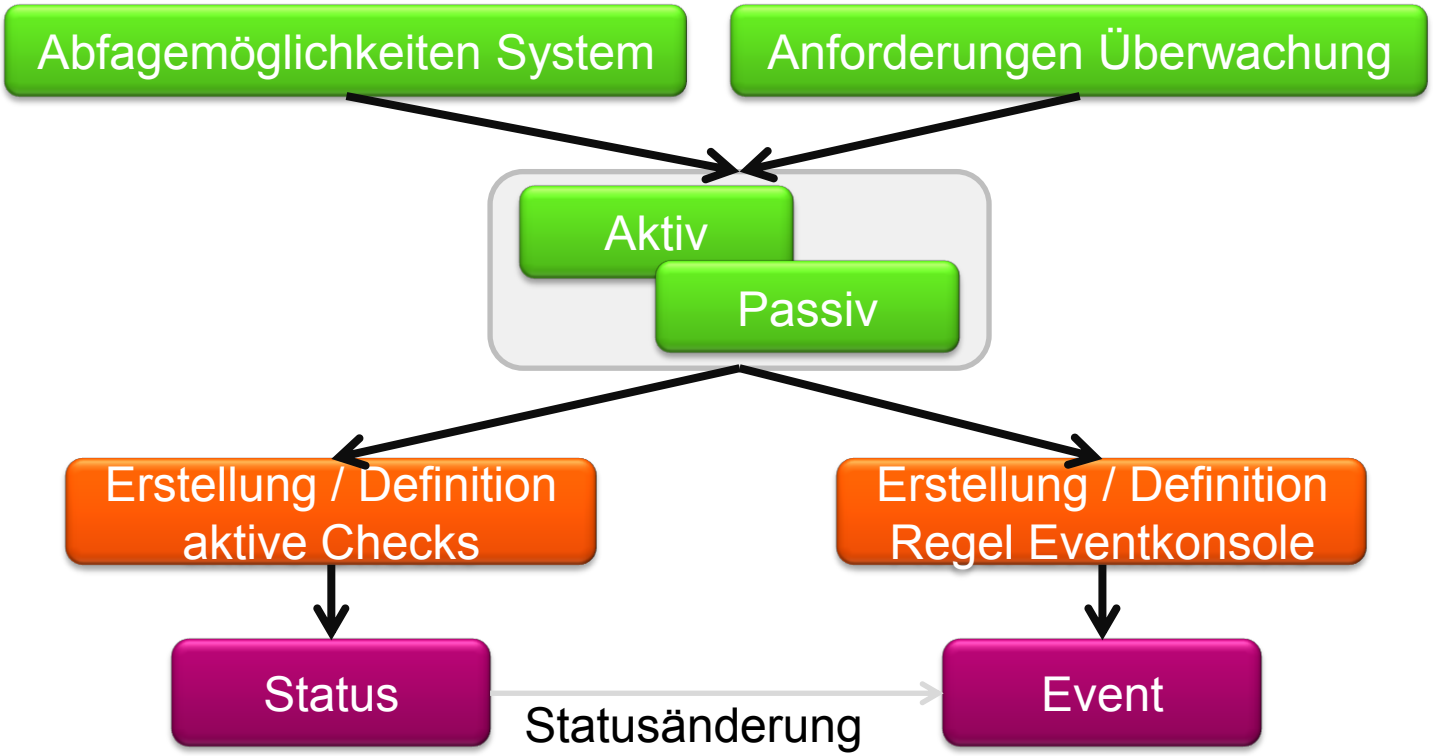
Optimale Ergebnisse
durch Kombination

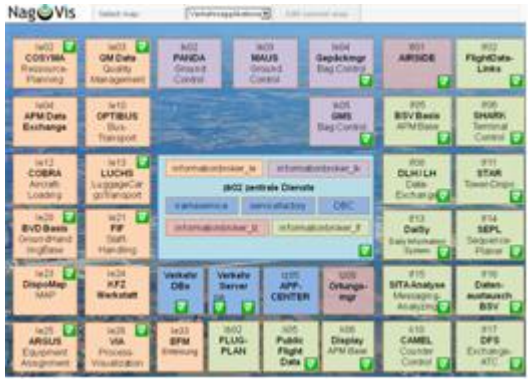
Kombination

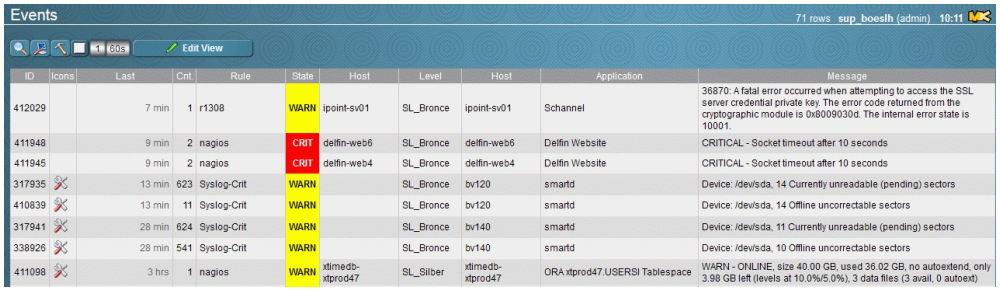
Die Kombination ist besser als die Summer der Einzelteile

Richtig gut wird es, wenn es aus einem Guss ist.

Der Weg zum Monitoring



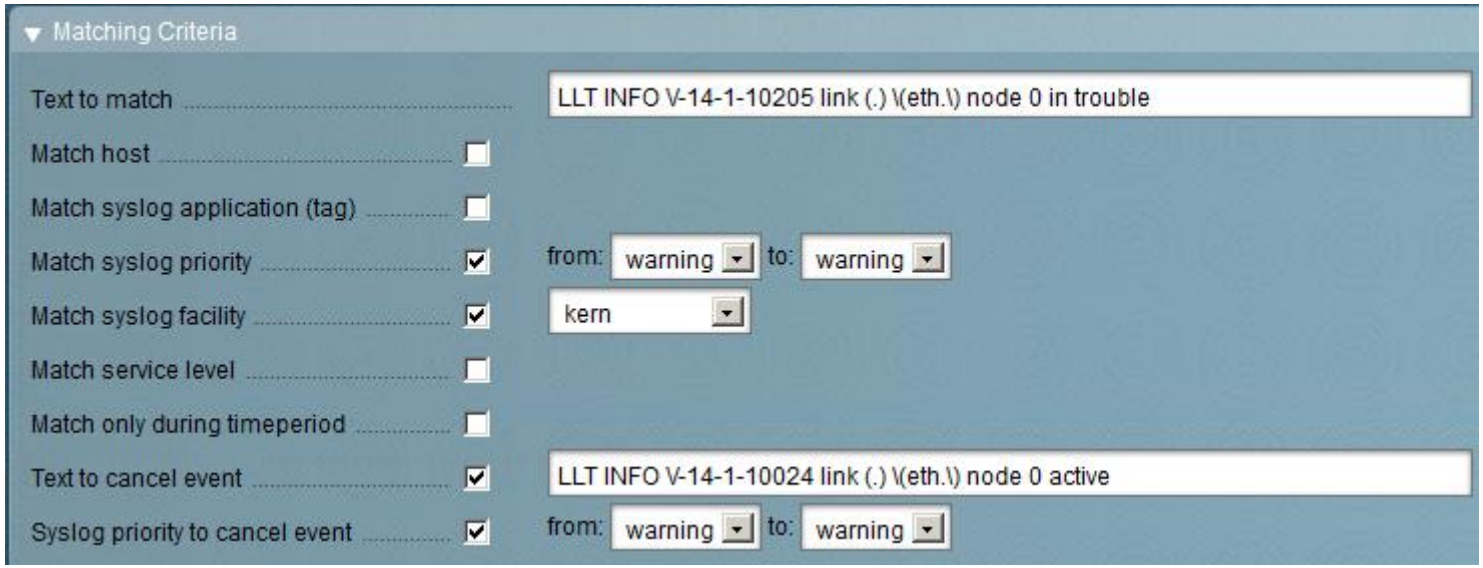




Der Weg zur Eventkonsole

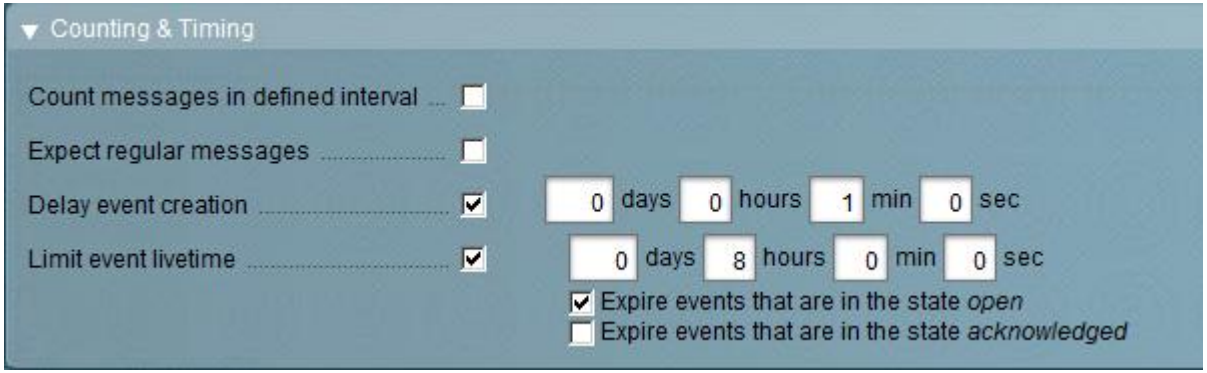
- Ende 2011 stand die Erneuerung der CA Unicenter Konsole an
- Vergleich zwischen kommerziellen Produkten und Open Source
  - Es war keine Open Source Lösung verfügbar, die den Anforderungen genügte
  - Einholung von kommerziellen Angeboten
  - Erarbeitungen von Open Source Konzepten
- Das Konzept von Mathias Kettner überzeugte und war finanziell umsetzbar
- Ausschlaggebend war die einfache Bedienbarkeit und geringe Ressourcenanforderungen
- Im Juni 2012 stand das Konzept und Pflichtenheft
- Im Oktober 2012 übernahm die check_mk Eventkonsole die Führungsrolle

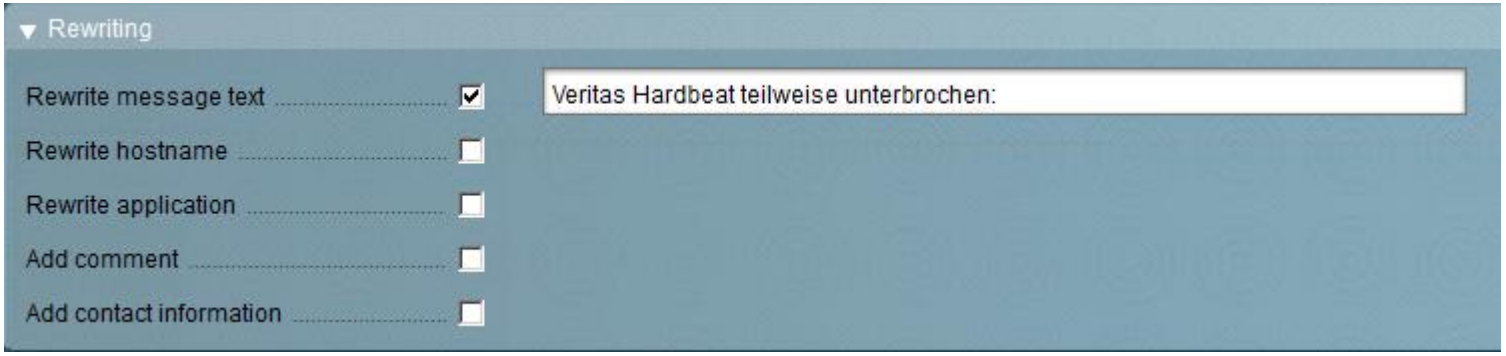
Event - generieren und löschen



Events können beim auftreten der OK Meldung auch automatisch archiviert werden.

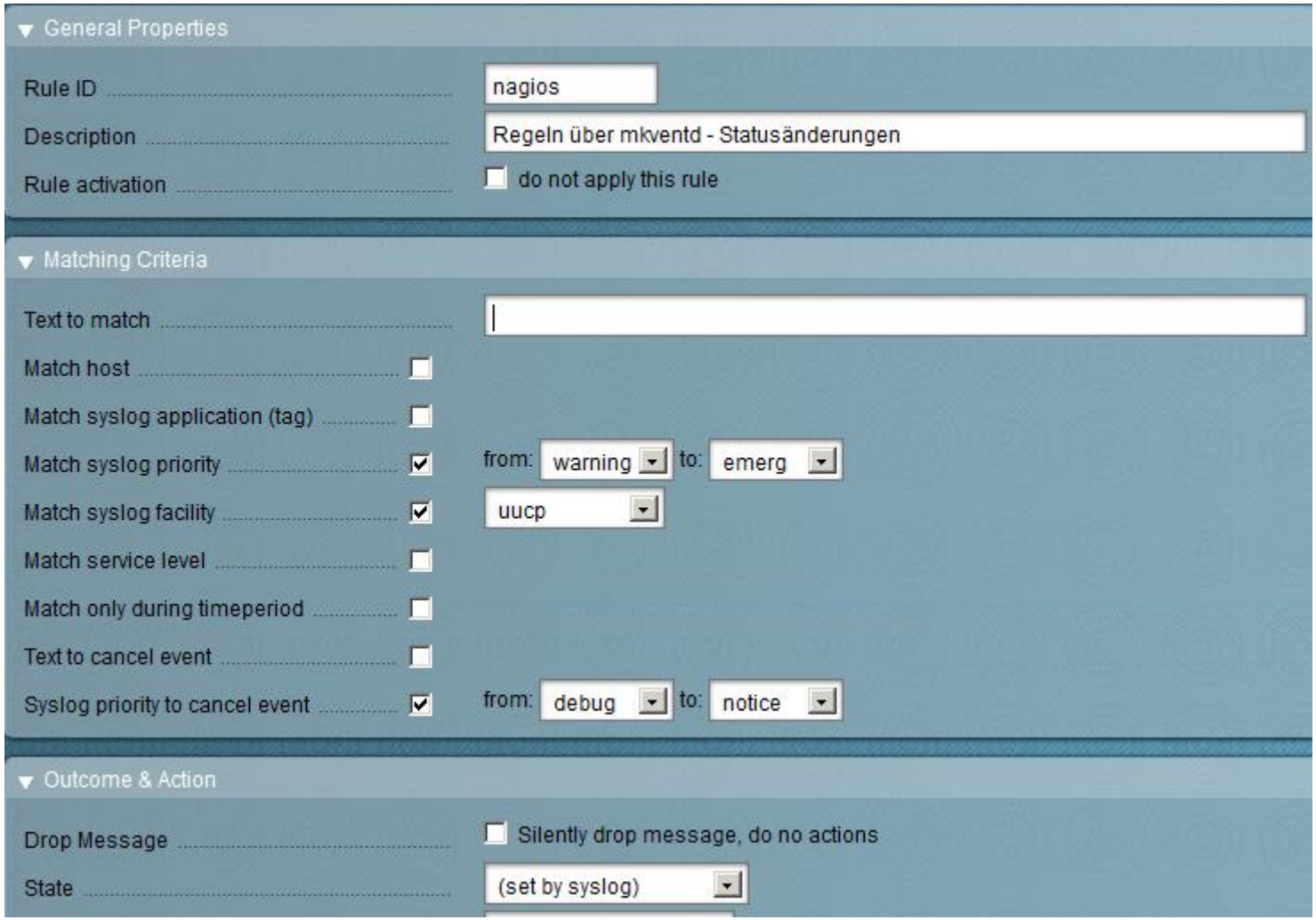
Event - Counting und Rewriting





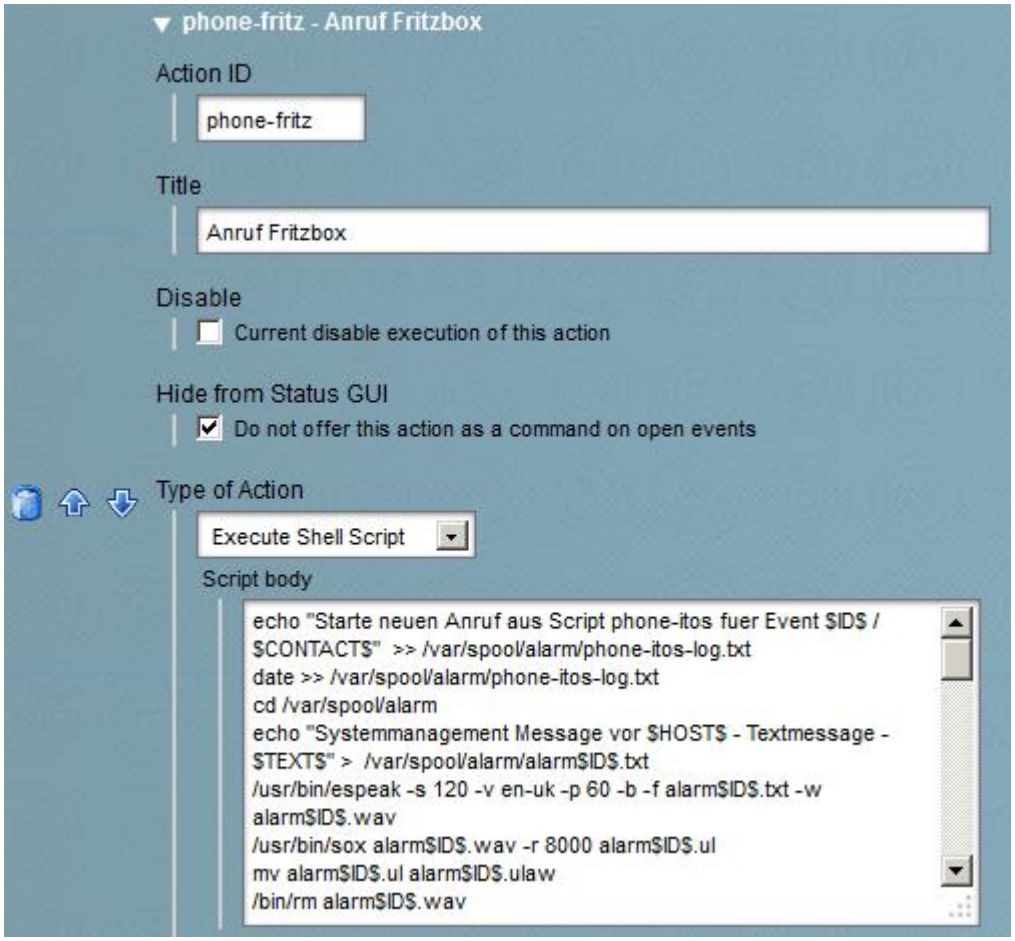
In manchen Fällen ist es sinnvoll, Events nicht sofort, oder mit anderen Text anzuzeigen.

Übernahme der Statusänderungen aus check_mk



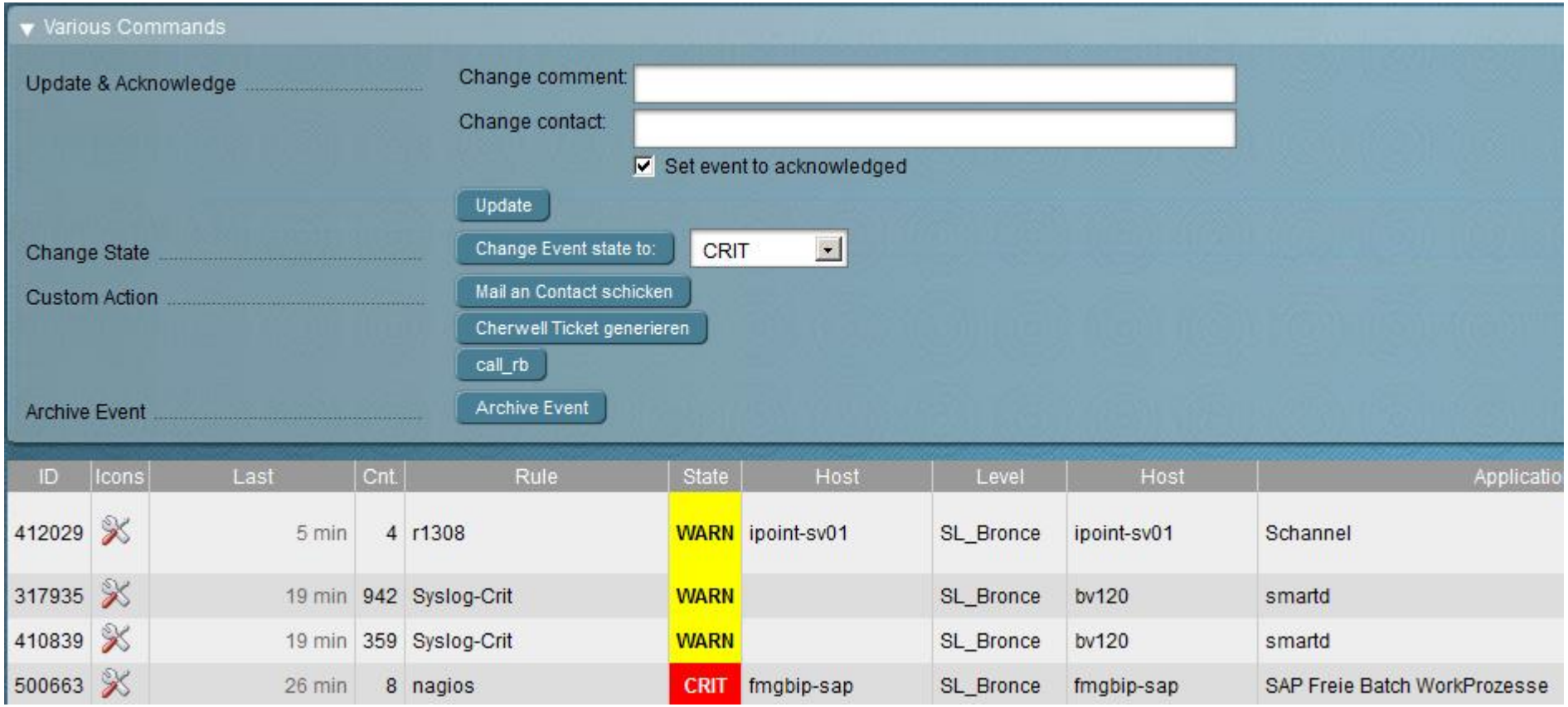
Fast alle Statusänderungen aus check_mk werden mit nur einer Regel bearbeitet

Actions – Call Rufbereitschaft



Bei sehr kritischen Events wird die Rufbereitschaft aus dem System heraus angerufen.

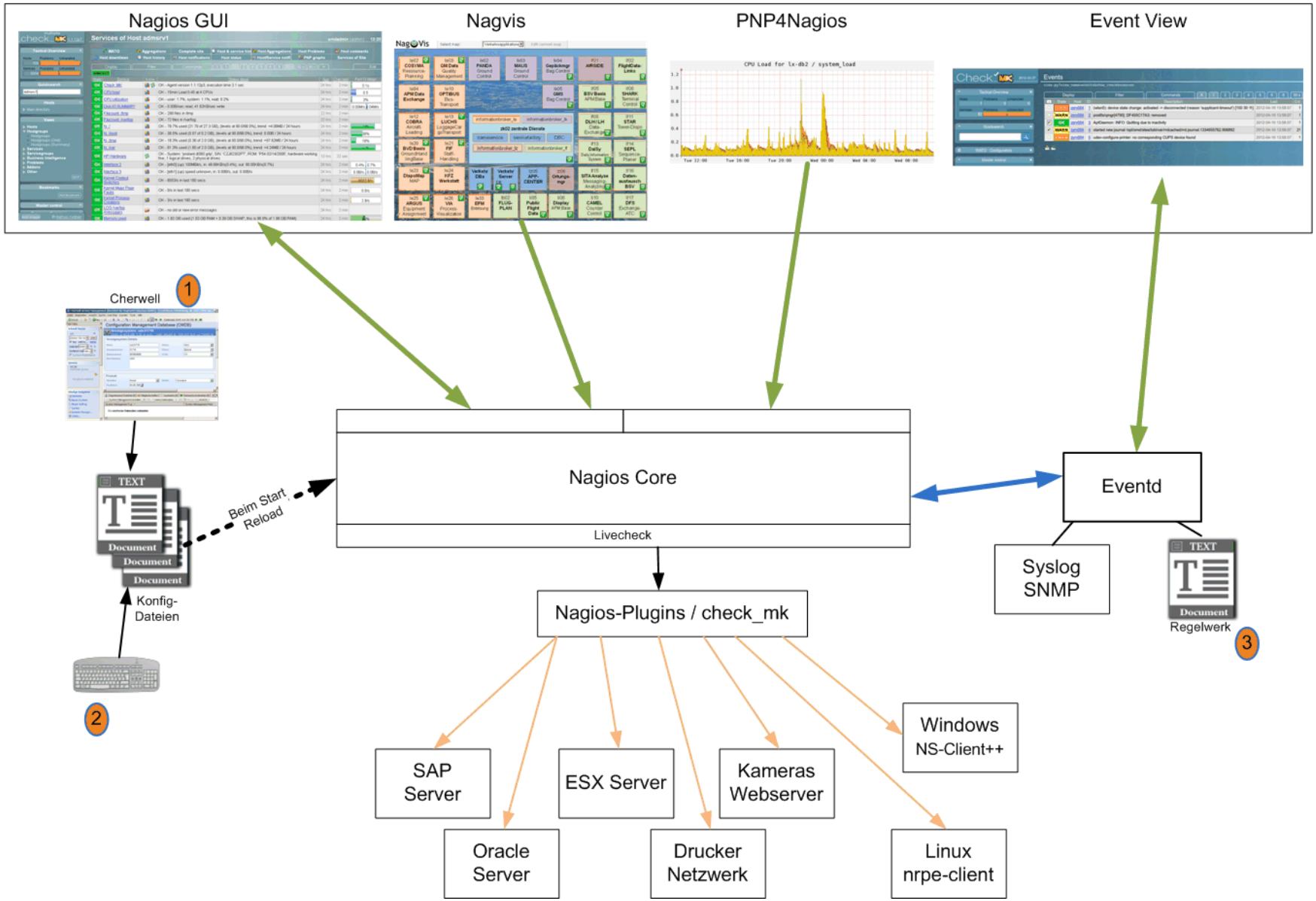
Eventkonsole - Aktionen



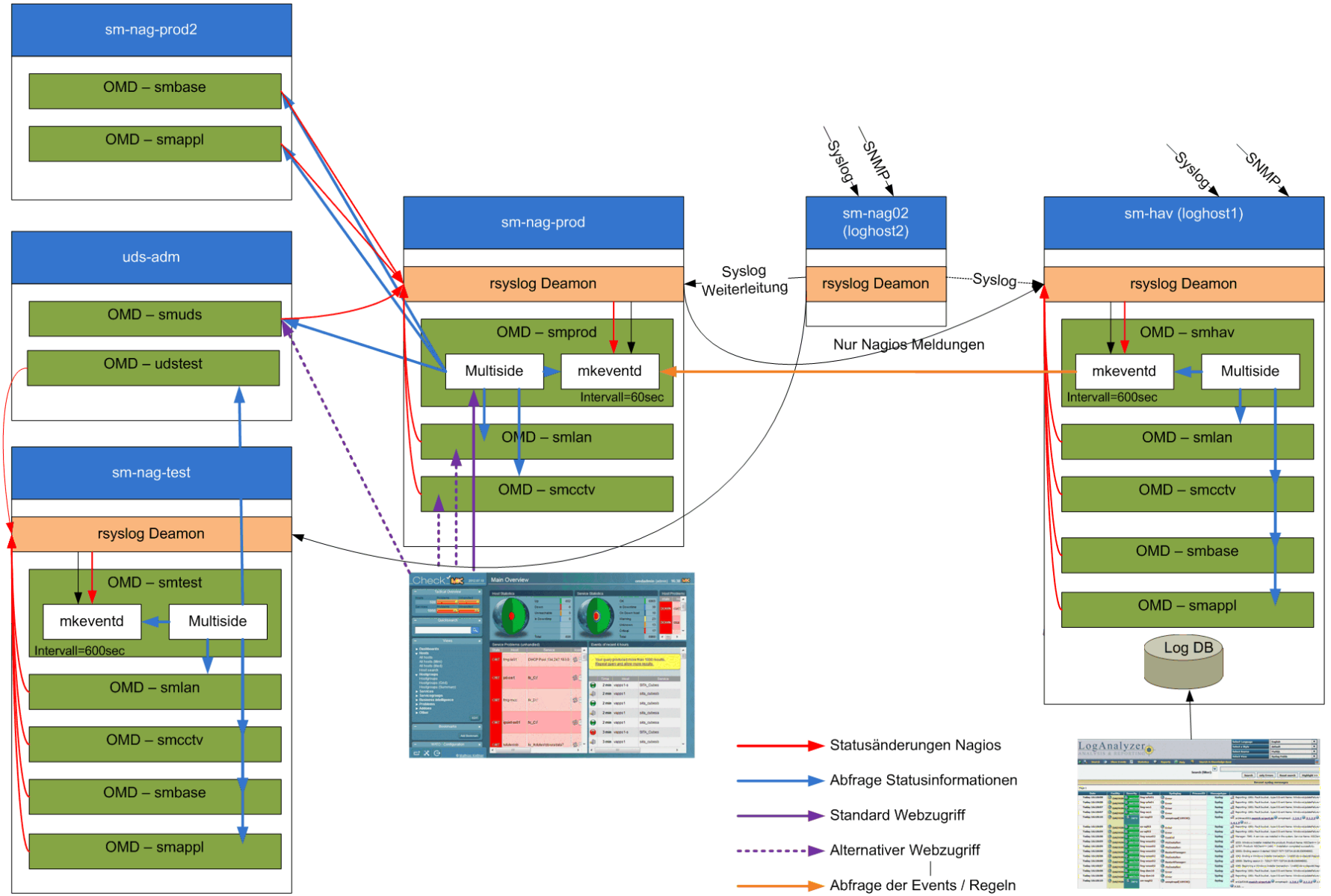
ID	Icons	Last	Cnt.	Rule	State	Host	Level	Host	Applicatio
412029		5 min	4	r1308	WARN	ipoint-sv01	SL_Bronce	ipoint-sv01	Schannel
317935		19 min	942	Syslog-Crit	WARN		SL_Bronce	bv120	smartd
410839		19 min	359	Syslog-Crit	WARN		SL_Bronce	bv120	smartd
500663		26 min	8	nagios	CRIT	fmgbip-sap	SL_Bronce	fmgbip-sap	SAP Freie Batch WorkProzesse

Bestimmte Aktionen können auch über die GUI angestoßen werden (für einen oder mehrere Events)

Kommunikation und Konfiguration

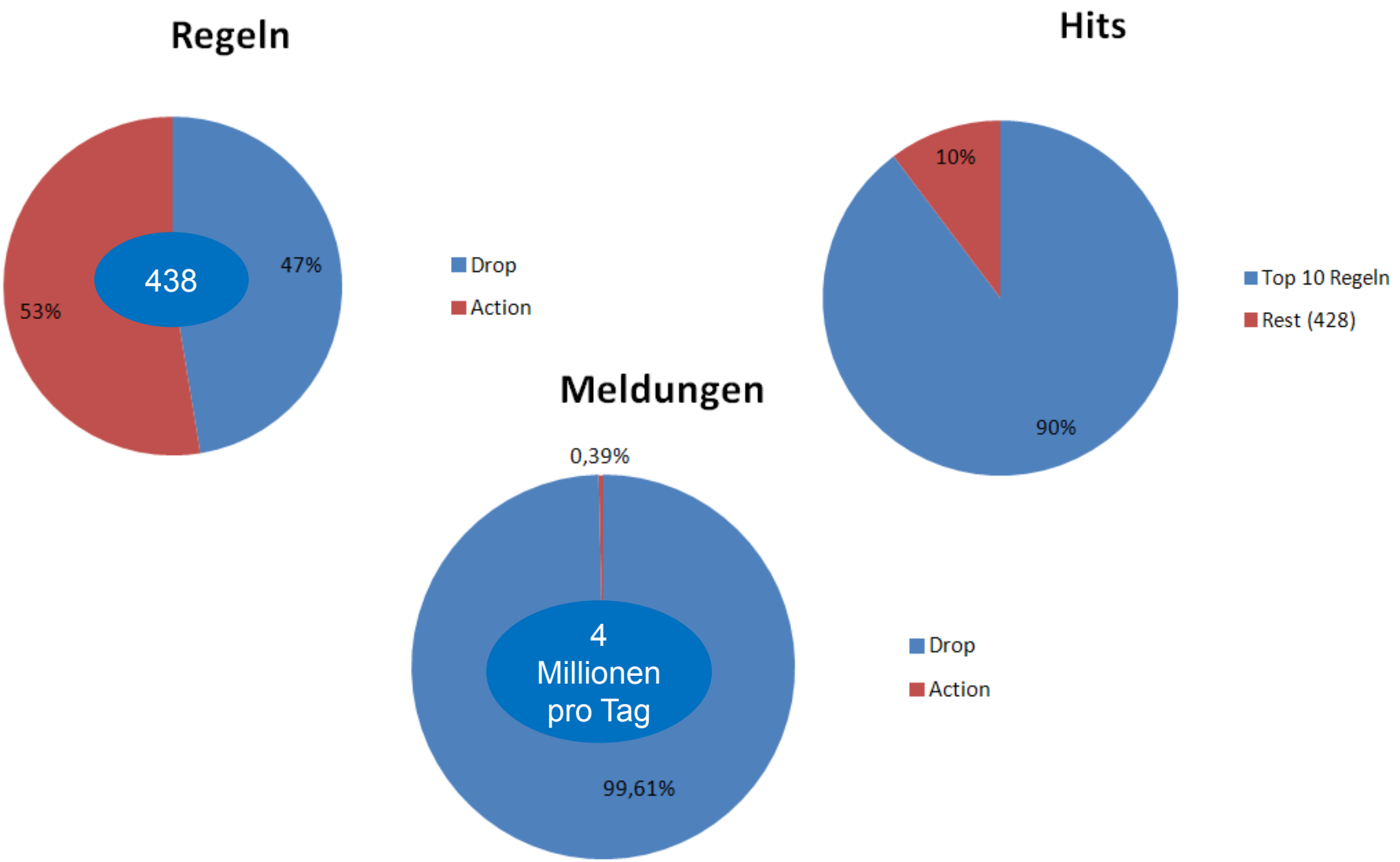


Monitoring Umgebung Flughafen München

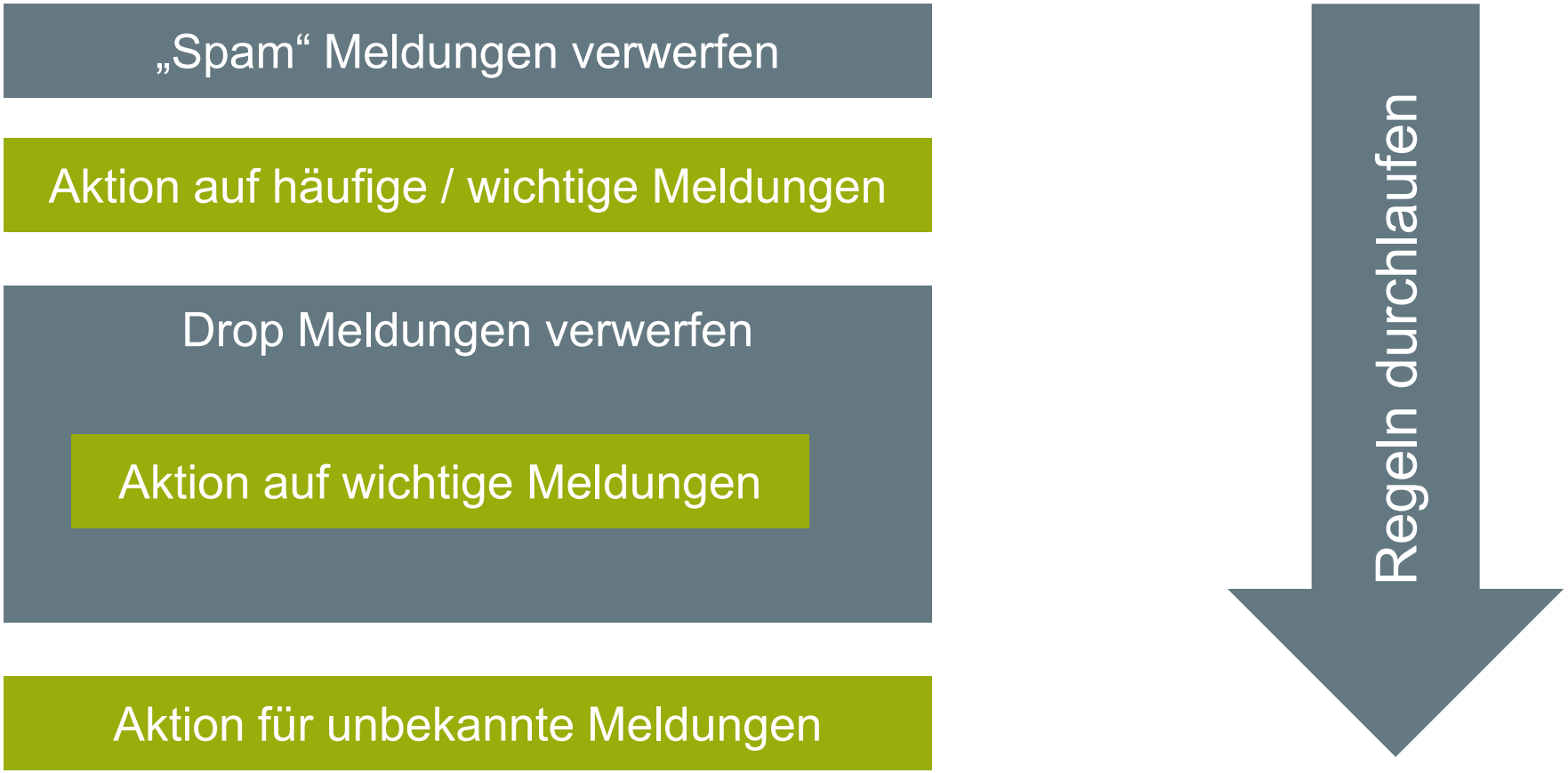


Der Weg zum Event

Regelwerk - Verteilung



Grundschema Regelwerk



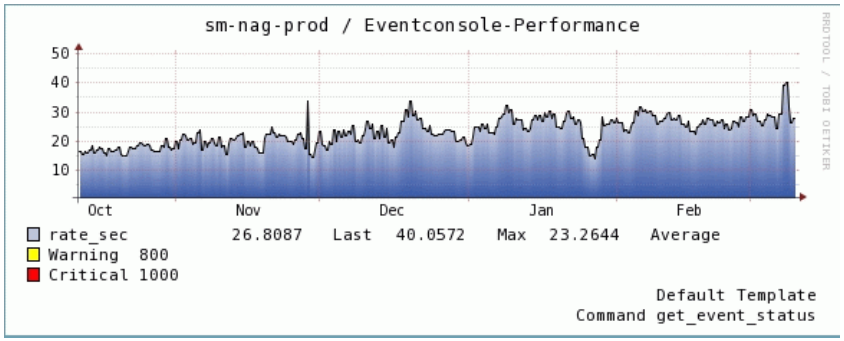
Grundschema Regelwerk

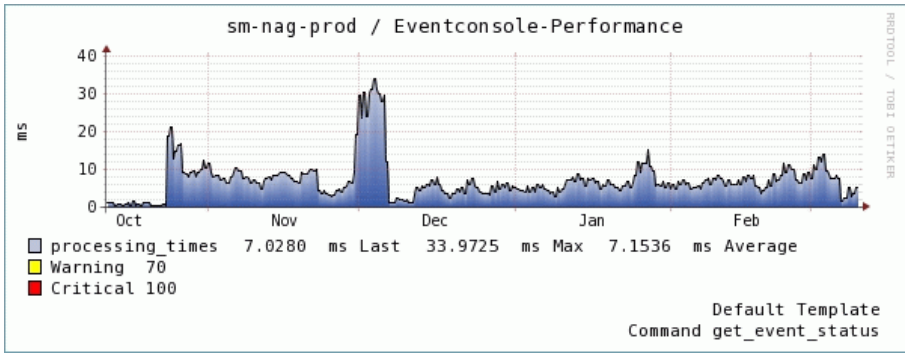
ID	Priority	Priority	Facility	Service Level	Hits	Description	Tex
sec-audit	DROP	notice	daemon	SL_No_Service	47784621	Security-Auditing	
wlan-ctrl3	DROP	alert	local1	SL_None	41463100	wlan-ctrl 3	.*1.3.6.1.4.1.9.9.599.1.3.*
wlan-ctrl1	DROP	alert	local1	SL_None	38600982	wlan-ctrl 1	.*1.3.6.1.4.1.14179.2.6.2.43.*
r212	DROP	notice	daemon	SL_None	21409250	Win OS	^600: Provider.*?is Started\. Detai
gauge32	DROP	alert	local1	SL_None	8320991	Gauge 32 Wrong Type	.*Wrong Type \(should be INTEGE
DNSupdate	DROP	err	daemon	SL_None	12204699	DNS Update	^client .*?update.* denied$
SQLAgent	DROP	notice	daemon	SL_None	10134573	SQLAgent	.*53: \[sqagtres\].*
r210a	DROP	notice	daemon	SL_None	5081088	Win OS	.*Engine state is changed from.*
nagios_ruf_uds	CRIT	wa..cr	uucp	SL_Platin_RB	7	Regeln über mkventd - UDS-BSV Schnittstellenüberwachung	
nagios_gol_rb	(syslog)	cr..em	uucp	SL_Gold_RB	5	Regeln über mkventd - Statusänderungen	
nagios_pla_rb	(syslog)	cr..em	uucp	SL_Platin_RB	1	Regeln über mkventd - Statusänderungen	
nagios	(syslog)	wa..em	uucp	SL_Bronce	49467	Regeln über mkventd - Statusänderungen	
NT-AUTH-673	DROP	err	daemon	SL_None		Ticket Reques Failed	673: NT AUTHORITY.SYSTEM: Service Ticket Request: User N User Domain:.* Service Name:.* Service ID:.* Ticket Options: (Encryption Type: .*
sshd_reset	DROP	crit	authpriv	SL_None	8916	Inkompatibilitaet Client - Server, funktioniert normalerweise trotzdem	fatal: Read from socket failed: Connection reset by peer
DSM-TFTP	DROP	notice	daemon	SL_Platin	28077	TFTP Datei nicht gefunden. - DSM Server	1000: TFTP: Datei
Kerberos4	WARN	err	daemon	SL_No_Service	6539	Kerberos Meldungen fmg-infra02	4: The Kerberos client received a KRB_AP_ERR_MODIFIED.*
Syslog-Crit	WARN	crit		SL_Bronce	2629	Syslog Critical Meldung	(.*)

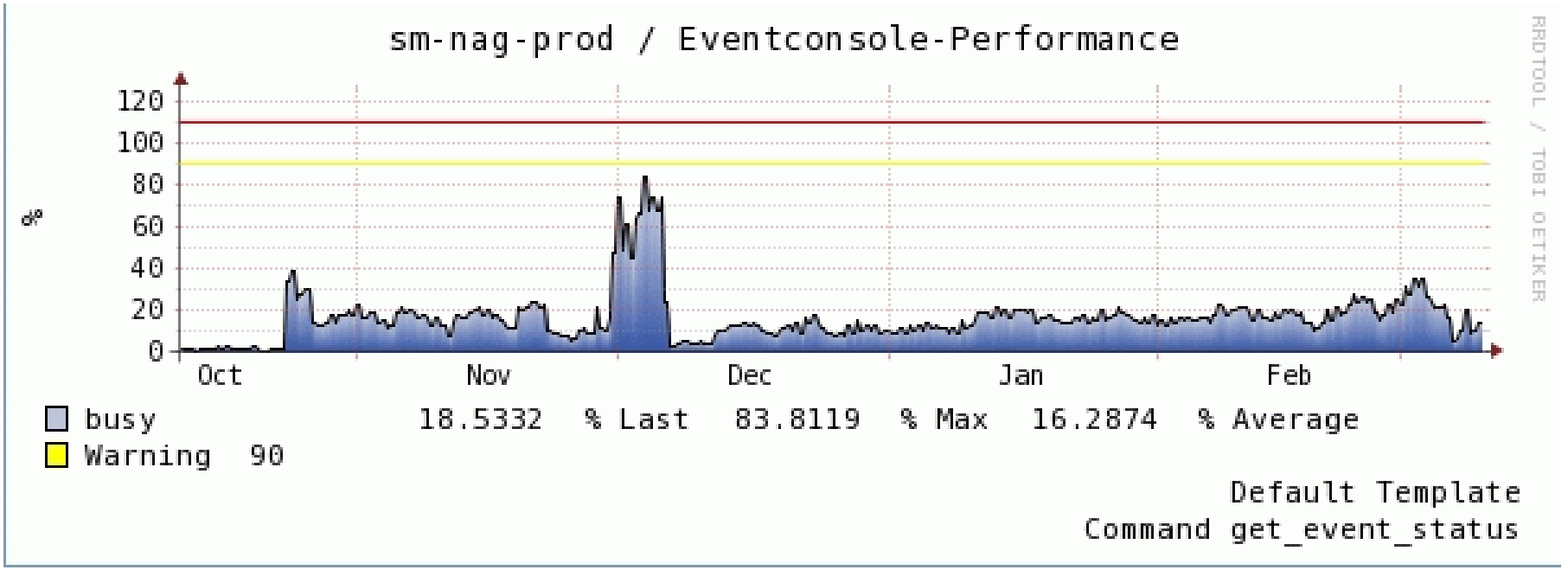
Bewertung einer Meldung

- Meldungstext
- Ursprung
- Severity/Facility (Nur Syslog)
- Servicelevel (Nur Statusmeldungen)
- Zeitpunkt
- Anzahl Meldungen in einem Intervall

Performance Eventkonsole

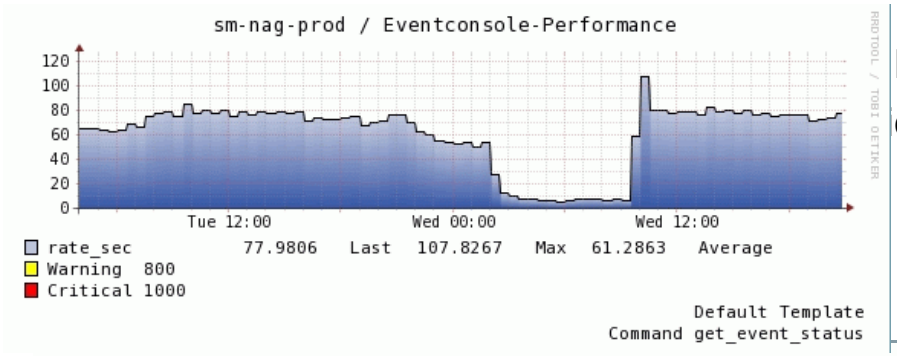


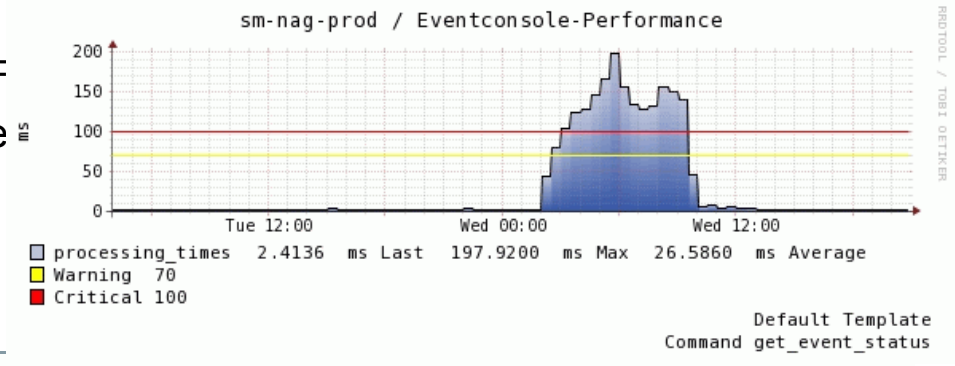


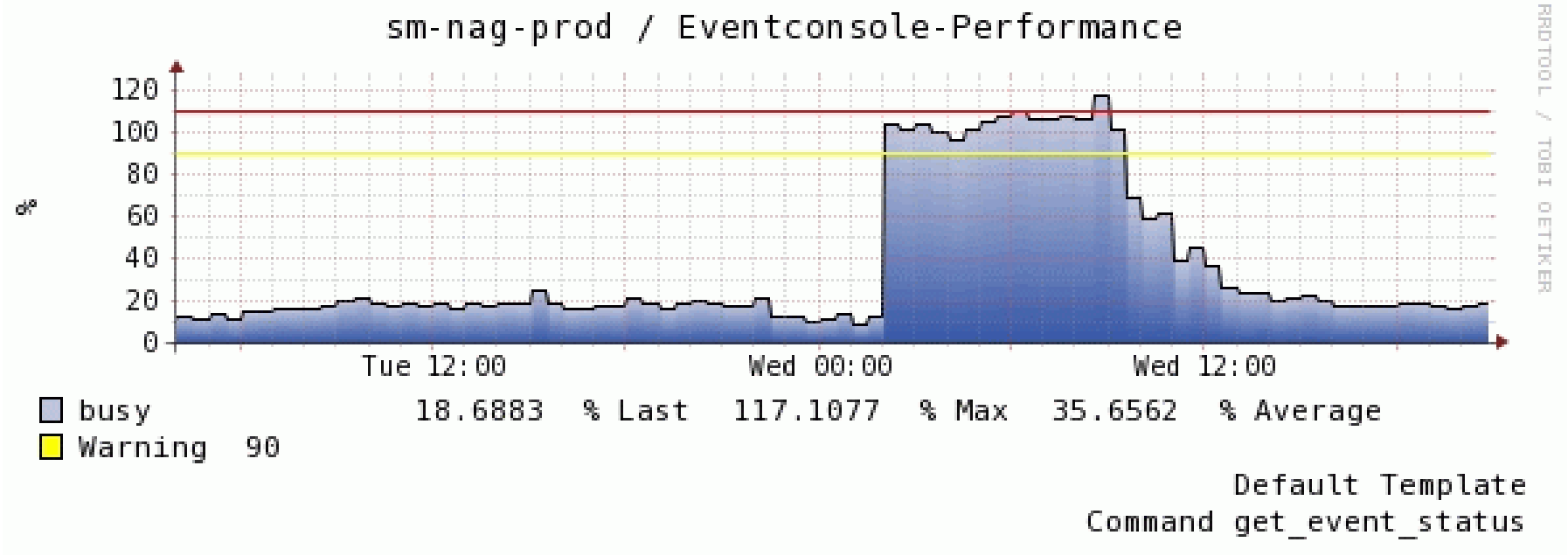


Bei passender Konfiguration sind 200 Meldungen pro Sekunde kein Problem

Performanceoptimierung

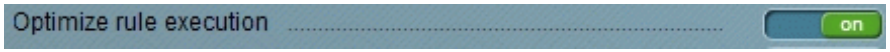


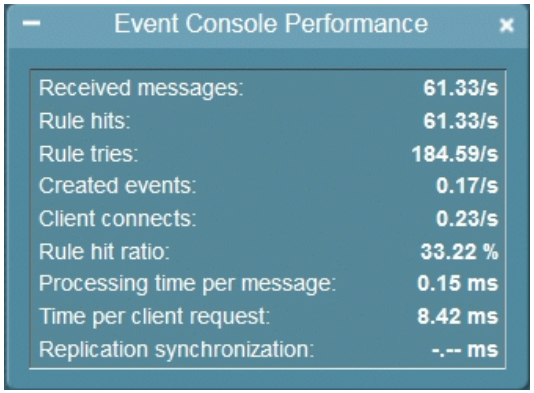




Performanceoptimierung - Hashes

```
Cleaning up event pipe
Top 20 of facility/priority:
 local1/alert - 1945796 (44.62%)
 daemon/notice - 1820703 (41.75%)
 daemon/err - 244550 (5.61%)
 kern/info - 66958 (1.54%)
 local7/crit - 62763 (1.44%)
 daemon/warning - 56616 (1.30%)
 mail/info - 37998 (0.87%)
...
```

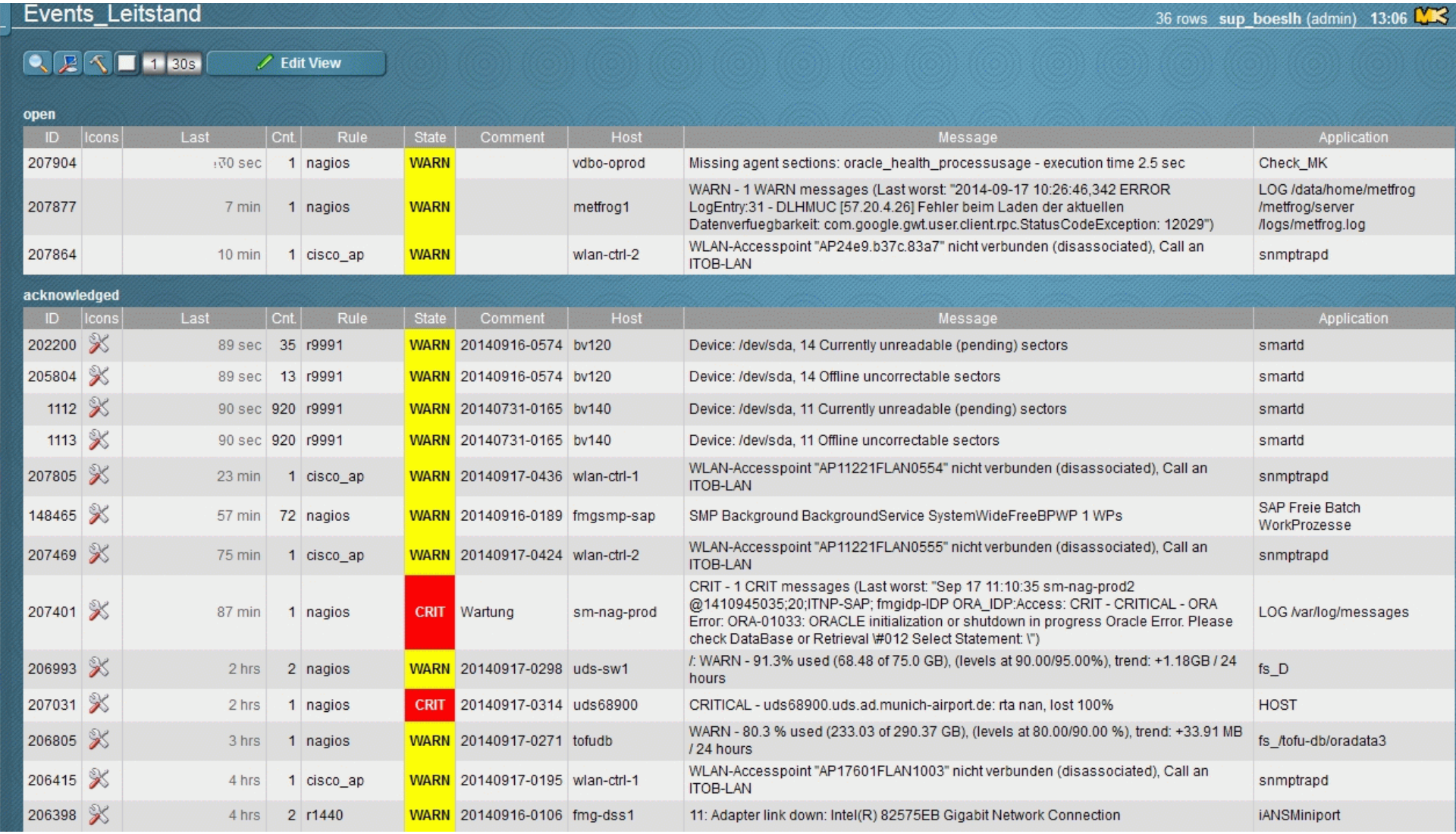





```
Compiled 438 active rules (ignoring 4 disabled rules)
Rule hash: 438 rules - 423 hashed, 15 unspecific
 kern         : emerg(18) alert(21) crit(24) err(105) warning(119) notice(21) info(20) debug(18)
 user         : emerg(19) alert(22) crit(27) err(113) warning(126) notice(24) info(20) debug(18)
 mail         : emerg(18) alert(21) crit(24) err(105) warning(119) notice(22) info(21) debug(18)
 daemon       : emerg(20) alert(23) crit(33) err(146) warning(141) notice(33) info(21) debug(19)
 auth         : emerg(18) alert(21) crit(25) err(105) warning(120) notice(21) info(20) debug(18)
 syslog       : emerg(18) alert(21) crit(24) err(106) warning(119) notice(21) info(21) debug(18)
 lpr          : emerg(18) alert(21) crit(24) err(105) warning(119) notice(21) info(20) debug(18)
 news         : emerg(18) alert(21) crit(24) err(105) warning(119) notice(21) info(20) debug(18)
 uucp         : emerg(22) alert(25) crit(30) err(109) warning(123) notice(22) info(21) debug(19)
 cron         : emerg(18) alert(21) crit(24) err(105) warning(119) notice(21) info(21) debug(18)
 authpriv     : emerg(18) alert(22) crit(25) err(109) warning(120) n
 ftp          : emerg(18) alert(21) crit(24) err(105) warning(119) n
 local0       : emerg(18) alert(21) crit(24) err(105) warning(119) n
 local1       : emerg(47) alert(116) crit(53) err(134) warning(148)
```

Nur bei einer Aufteilung über facility / priority sinnvoll

Eventkonsole am Leitstand



Events_Leitstand

36 rows sup_boeslh (admin) 13:06

1 30s Edit View

open

ID	Icons	Last	Cnt.	Rule	State	Comment	Host	Message	Application
207904		30 sec	1	nagios	WARN		vdbo-oprod	Missing agent sections: oracle_health_processusage - execution time 2.5 sec	Check_MK
207877		7 min	1	nagios	WARN		metfrog1	WARN - 1 WARN messages (Last worst: "2014-09-17 10:26:46,342 ERROR LogEntry:31 - DLHMUC [57.20.4.26] Fehler beim Laden der aktuellen Datenverfuegbarkeit: com.google.gwt.user.client.rpc.StatusCodeException: 12029")	LOG /data/home/metfrog /metfrog/server /logs/metfrog.log
207864		10 min	1	cisco_ap	WARN		wlan-ctrl-2	WLAN-Accesspoint "AP24e9.b37c.83a7" nicht verbunden (disassociated), Call an ITOB-LAN	snmptrapd

acknowledged

ID	Icons	Last	Cnt.	Rule	State	Comment	Host	Message	Application
202200		89 sec	35	r9991	WARN	20140916-0574	bv120	Device: /dev/sda, 14 Currently unreadable (pending) sectors	smartd
205804		89 sec	13	r9991	WARN	20140916-0574	bv120	Device: /dev/sda, 14 Offline uncorrectable sectors	smartd
1112		90 sec	920	r9991	WARN	20140731-0165	bv140	Device: /dev/sda, 11 Currently unreadable (pending) sectors	smartd
1113		90 sec	920	r9991	WARN	20140731-0165	bv140	Device: /dev/sda, 11 Offline uncorrectable sectors	smartd
207805		23 min	1	cisco_ap	WARN	20140917-0436	wlan-ctrl-1	WLAN-Accesspoint "AP11221FLAN0554" nicht verbunden (disassociated), Call an ITOB-LAN	snmptrapd
148465		57 min	72	nagios	WARN	20140916-0189	fmgsmp-sap	SMP Background BackgroundService SystemWideFreeBPWP 1 WPs	SAP Freie Batch WorkProzesse
207469		75 min	1	cisco_ap	WARN	20140917-0424	wlan-ctrl-2	WLAN-Accesspoint "AP11221FLAN0555" nicht verbunden (disassociated), Call an ITOB-LAN	snmptrapd
207401		87 min	1	nagios	CRIT	Wartung	sm-nag-prod	CRIT - 1 CRIT messages (Last worst: "Sep 17 11:10:35 sm-nag-prod2 @1410945035;20;ITNP-SAP; fmgidp-IDP ORA_IDP:Access: CRIT - CRITICAL - ORA Error: ORA-01033: ORACLE initialization or shutdown in progress Oracle Error. Please check DataBase or Retrieval \#012 Select Statement: \")	LOG /var/log/messages
206993		2 hrs	2	nagios	WARN	20140917-0298	uds-sw1	/: WARN - 91.3% used (68.48 of 75.0 GB), (levels at 90.00/95.00%), trend: +1.18GB / 24 hours	fs_D
207031		2 hrs	1	nagios	CRIT	20140917-0314	uds68900	CRITICAL - uds68900.uds.ad.munich-airport.de: rta nan, lost 100%	HOST
206805		3 hrs	1	nagios	WARN	20140917-0271	tofudb	WARN - 80.3 % used (233.03 of 290.37 GB), (levels at 80.00/90.00 %), trend: +33.91 MB / 24 hours	fs_/tofu-db/oradata3
206415		4 hrs	1	cisco_ap	WARN	20140917-0195	wlan-ctrl-1	WLAN-Accesspoint "AP17601FLAN1003" nicht verbunden (disassociated), Call an ITOB-LAN	snmptrapd
206398		4 hrs	2	r1440	WARN	20140916-0106	fmg-dss1	11: Adapter link down: Intel(R) 82575EB Gigabit Network Connection	iANSMiniport

Aktionen in der Eventkonsole

Beispiel Statusänderung und SLA

nagios_ruf_uds	CRIT	wa..cr	uucp	SL_Platin_RB	7	Regeln über mkventd - UDS-BSV Schnittstellenüberwachung
nagios_gol_rb	(syslog)	cr..em	uucp	SL_Gold_RB	5	Regeln über mkventd - Statusänderungen
nagios_pla_rb	(syslog)	cr..em	uucp	SL_Platin_RB	1	Regeln über mkventd - Statusänderungen
nagios	(syslog)	wa..em	uucp	SL_Bronce	49663	Regeln über mkventd - Statusänderungen

Anruf und Mail UDS Rufbereitschaft

Anruf und Mail IT Service Desk Rufbereitschaft

Darstellung des Events in der Eventkonsole (Filterung auf Servicelevel)

Generierung eines Tickets (Über GUI)

Anforderungen und Implementierung

- Alle wichtigen Systeme überwachen
- Ausfall möglichst schnell bemerken
- Wichtige Themen hervorheben
- Unwichtige Meldungen unterdrücken
- Zusatzinformationen
- Zeitliche Abläufe erkennen

Möglich über verschiedenste Wege.
Agent, Syslog (auch WIN), SNMP, Mail

Schnell über passive Wege
Sicher über aktive Wege

Einbindung von Servicelevel
Kumulieren von häufigen Meldungen

99,6% der Meldungen verwerfen
Filterung auf Servicelevel

Rewriting des Meldungstextes
Kontaktperson als Information hinzufügen

Zeitstempel, Intervalle, Counting
Archivierung

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?