

# Verarbeitung von Events

Udo Stachowiak / Frank Hildebrandt  
SECTOR NORD AG

Stand II-2012



# Kundenworkshop 2012

- Monitoring von Events
- SV3 Eventlog
- Livedemo



# Datenquellen für Monitoring

## Aktive Abfragen:

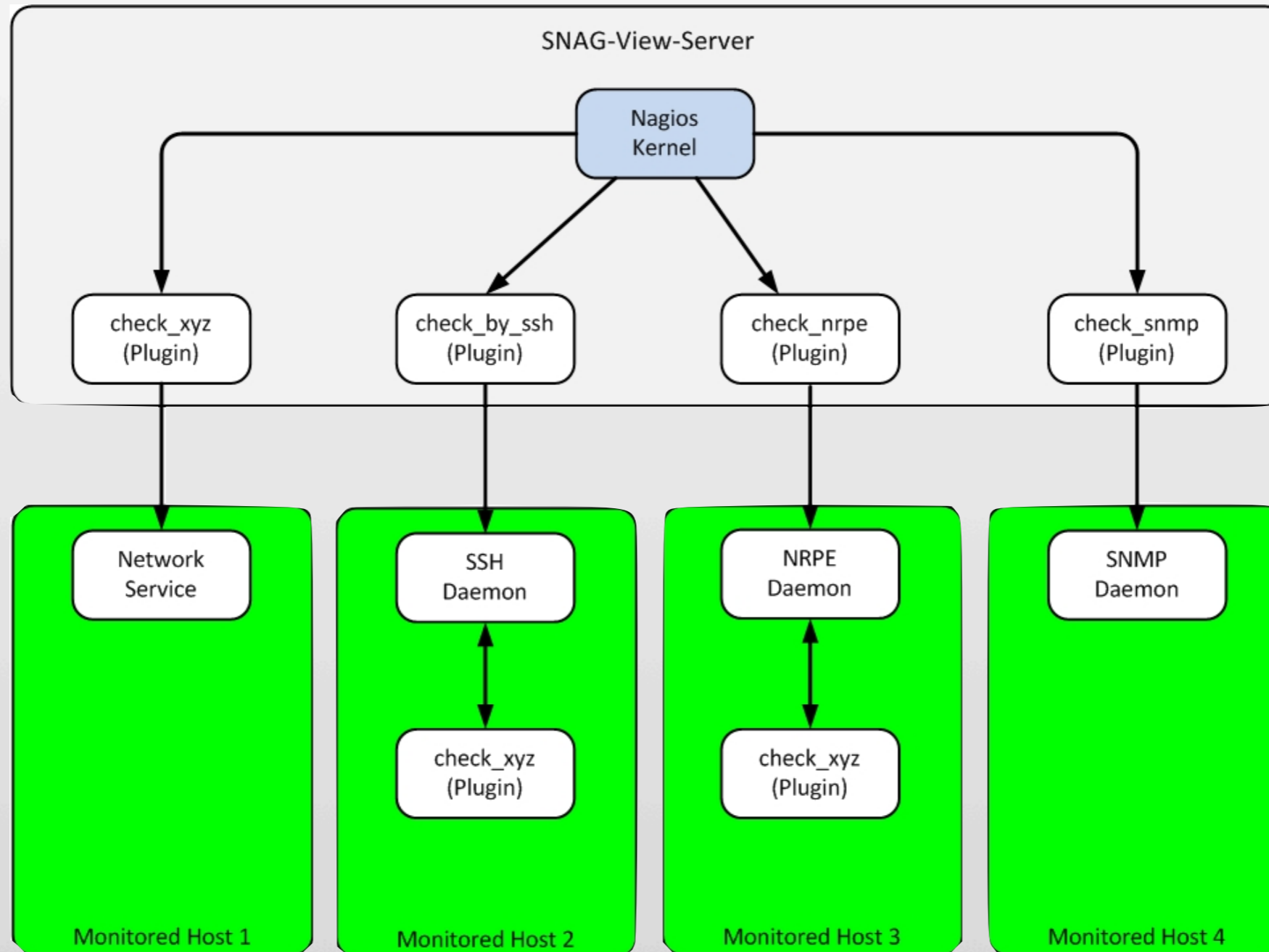
- Lokale Abfragen  
Disk, CPU, Memory
- Netzwerkdienste  
HTTP, DNS, SMTP,  
POP3, IMAP
- Remote-Abfragen  
SNMP, SSH, NRPE

## Events:

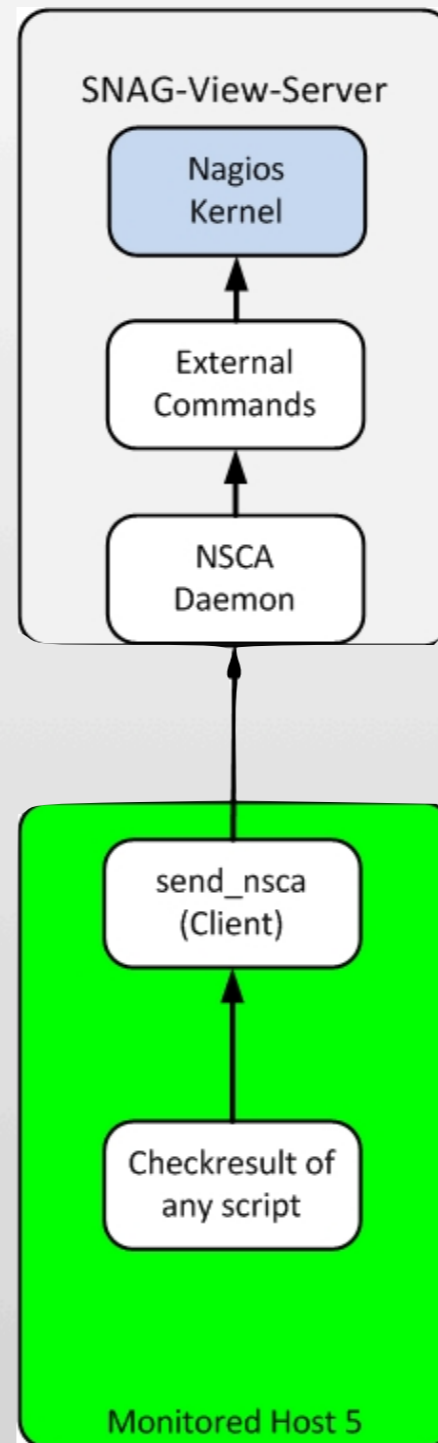
- Syslog-Meldungen
- Windows Eventlog
- SNMP-Traps
- Emails
- Sonstiges



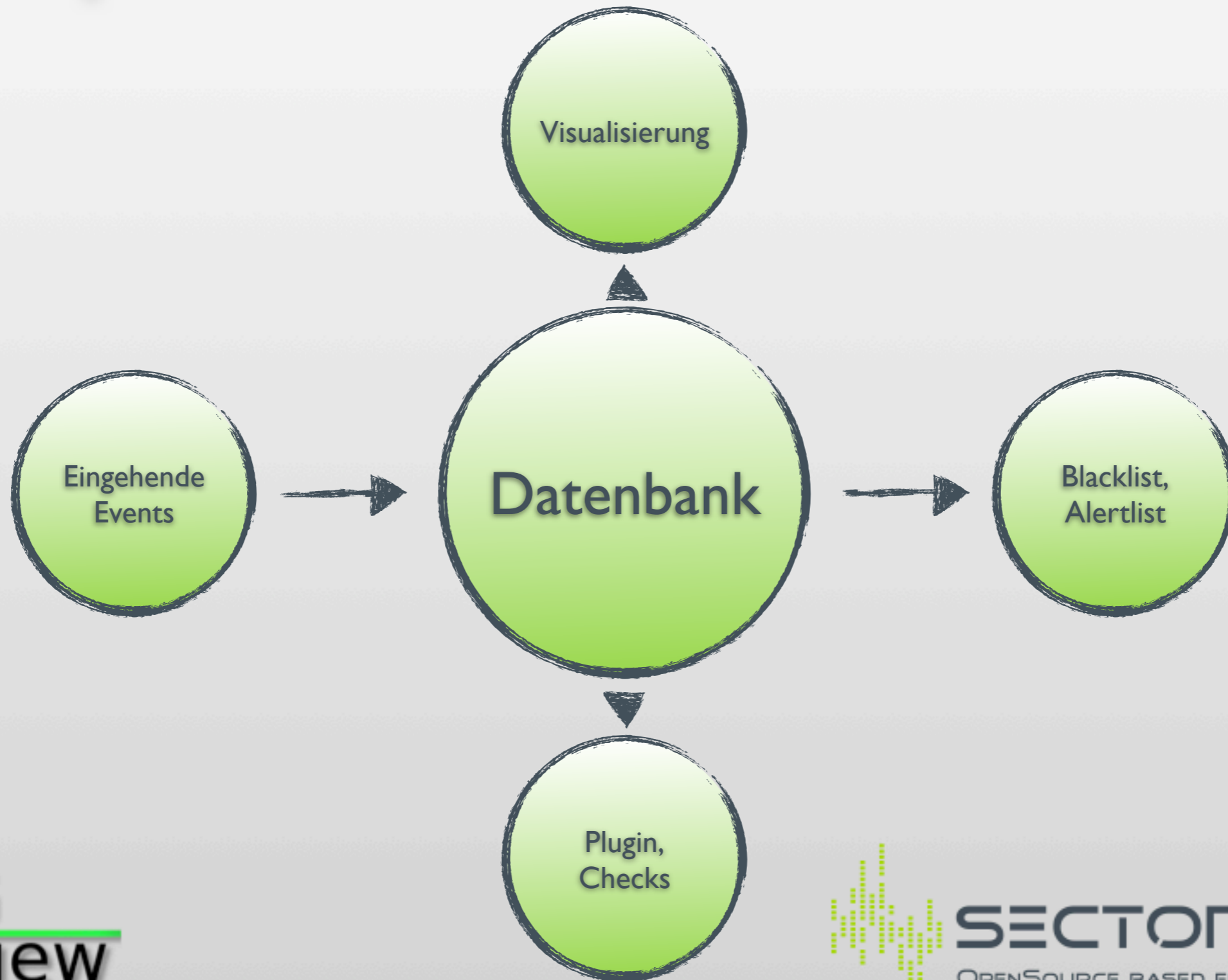
# Remote Checks



# Remote Checks



# Speichern von Events



# Aktive Checks

## Vorteile:

- werden regelmäßig ausgeführt
- Sammeln historischer Daten
- nicht funktionierender Check übermittelt einen Status

## Nachteile:

- belastet den Monitoring Server durch Einplanen von Checks
- belastet überwachte Systeme



# Events

## Vorteile:

- reduzierte Last auf dem Monitoring Server
- reduzierte Last auf dem überwachten System
- Letzter Hilferuf

## Nachteile:

- keine Informationen über den Status, wenn Events ausbleiben
- keine Performancedaten
- Events werden durch den Hersteller definiert
- Inhalt kann sehr unterschiedlich sein



# Fragen ???



~~Syslog++~~

# Eventlog Agent

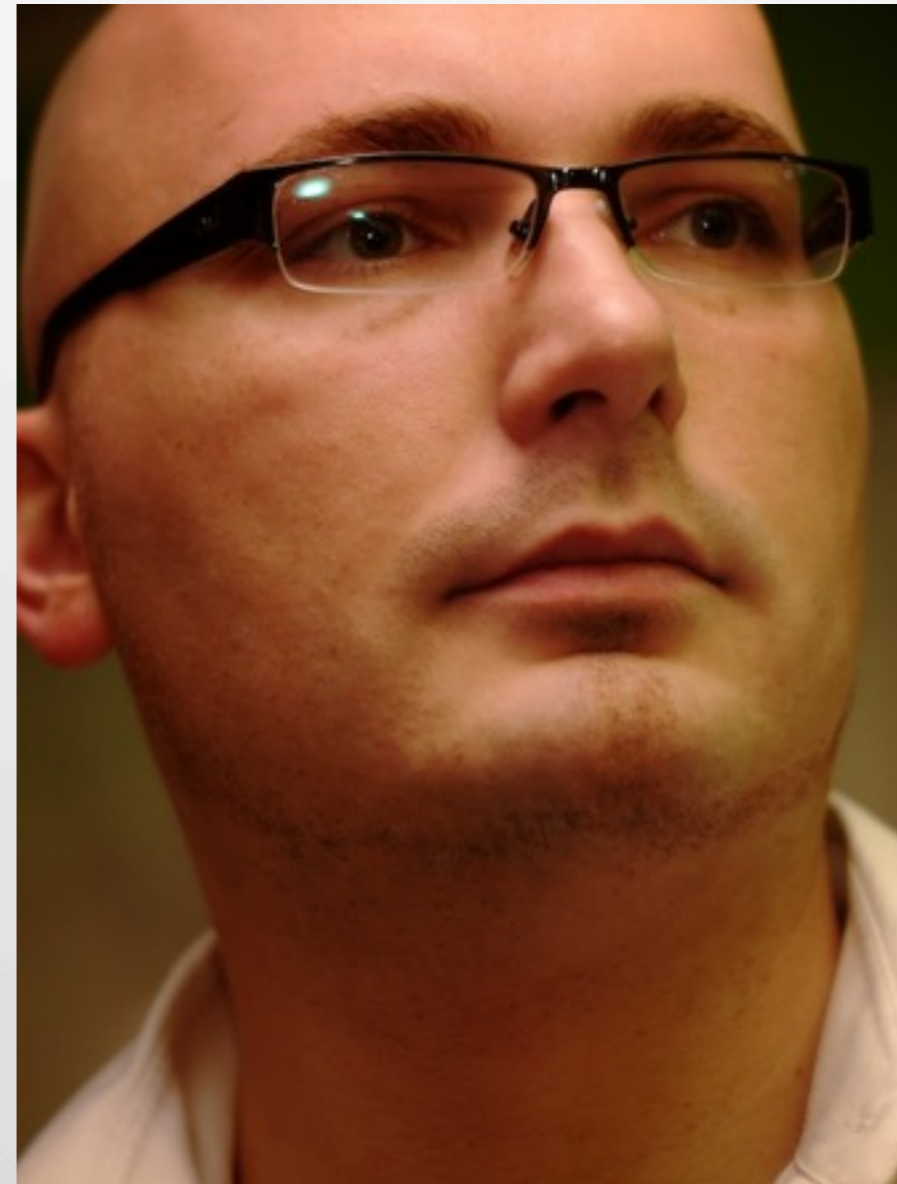
Regelbasierte Überwachung von auftretenden Events



# Frank Hildebrandt

31 Jahre alt  
Entwickler & Projektmanager

Twitter: @frank\_ol

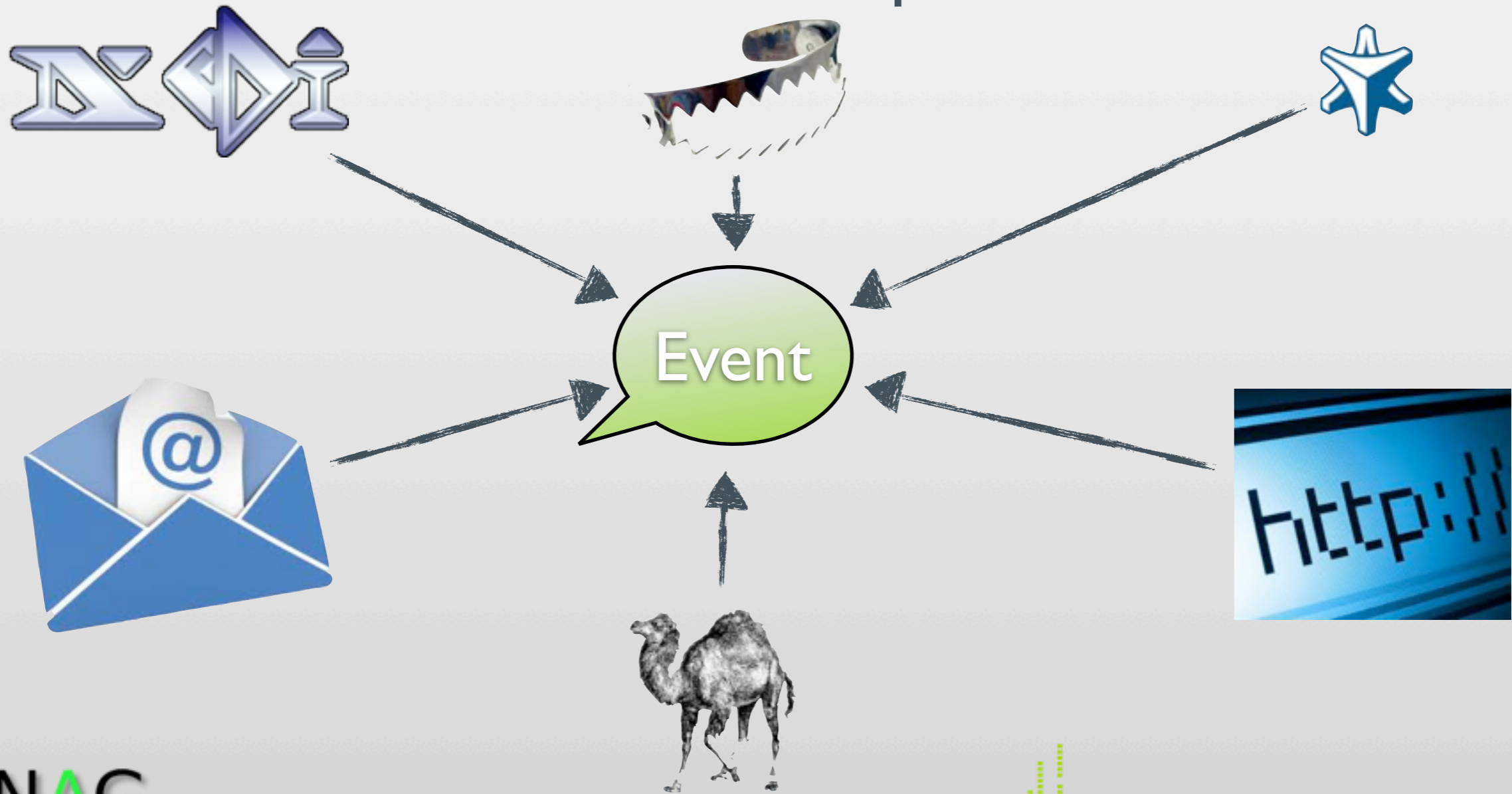


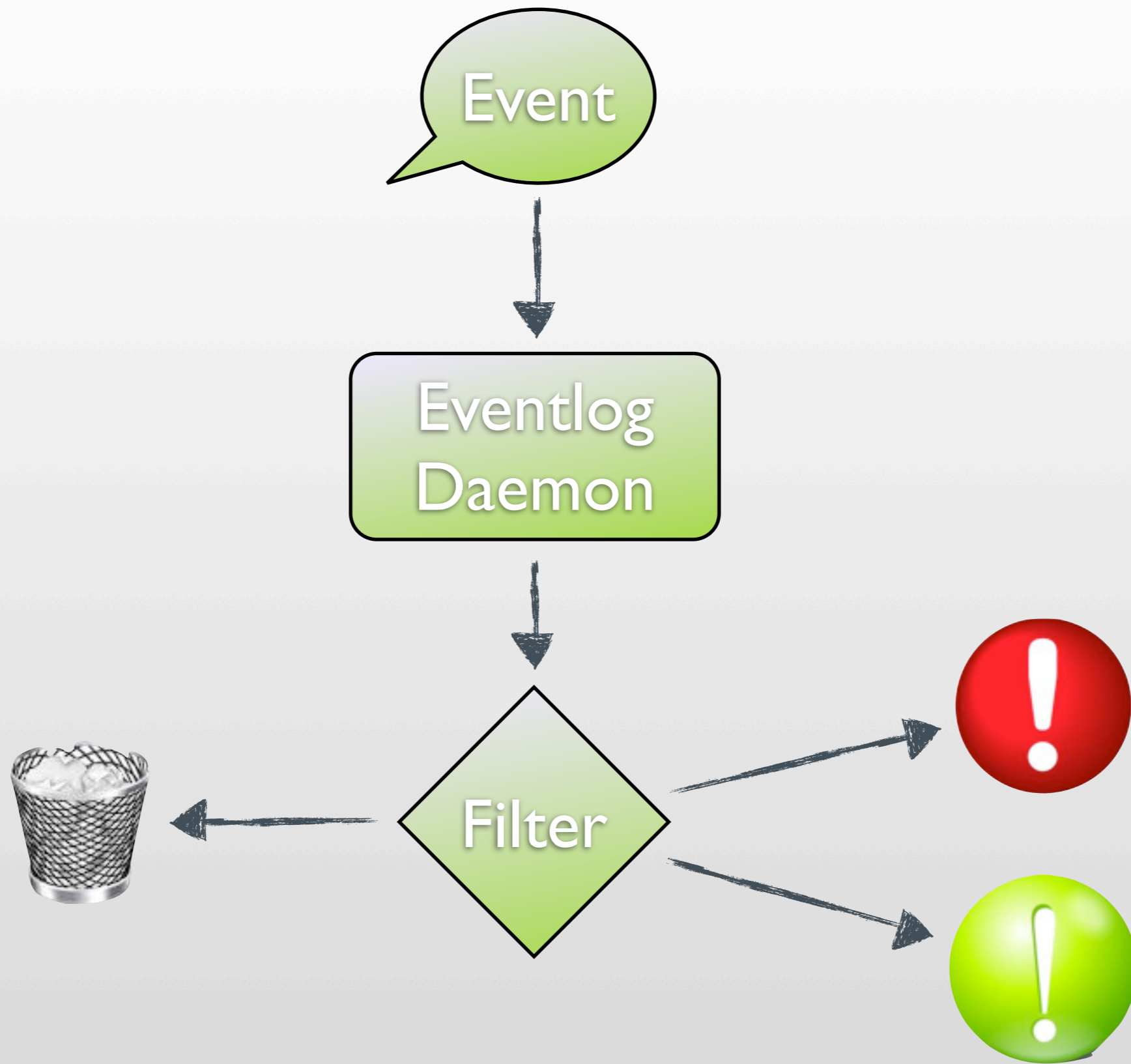
# Warum Eventlog

- mehr Funktionen
- mehr Quellen
- erweiterbar
- der Name Syslog++ passte einfach nicht mehr!

# eingehende Events

SNMP-Trap

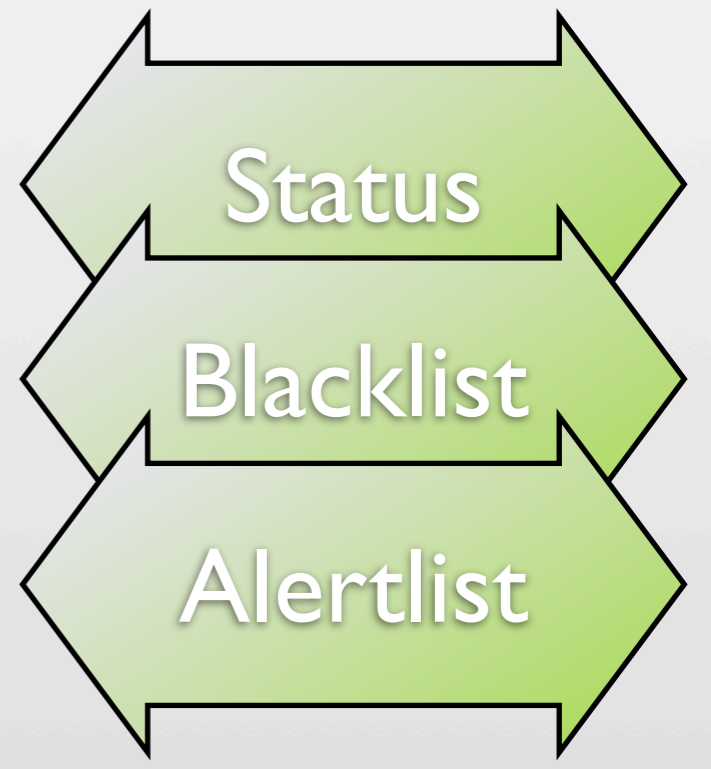
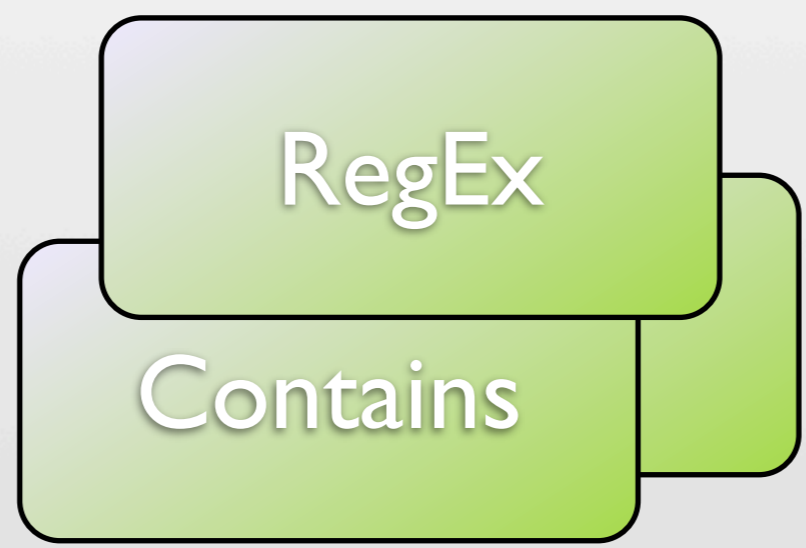






# Filterfunktionen

# Aktionen





# Die „Eventlog“ Listen



# Alertlist

- Organisationsmittel zum Hervorheben von wichtigen Events
- Servicechecks sehr einfach möglich
- Events können „acknowledged“ werden

SNAG-View 3

172.16.100.131

Host: 1 0 0 0

Service: 2 0 0 0

13.11.2012 23:37:54 svadmin

SNAG View

Dashboard Servicebrowser Eventlog

Alerts Blacklist Quellen Filter

Datum/Zeit	Host	Status	Typ	Nachricht	Kommentar
2012-11-13 23:07:02	snagview-ser...	Ok	✳	root: foobar	
2012-11-13 23:06:32	snagview-ser...	Warning	✳	root: warning	
2012-11-13 23:04:55	snagview-ser...	Critical	✳	root: Link is Down	

Seite 1 von 1 357

Zeige 1 - 3 von 3



# Blacklist

- Archiv von Events
- Servicechecks möglich



SNAG-View 3

172.16.100.131

Host: 1 0 0 0

Service: 2 0 0 0

13.11.2012 23:38:36 svadmin

SNAG view

Dashboard Servicebrowser Eventlog

Alerts Blacklist Quellen Filter

Datum/Zeit	Host	Status	Typ	Nachricht	Kommentar
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP 2. ImageProxy->__construct() /opt/snag-view/fronten...	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP 1. {main}() /opt/snag-view/frontend/php/image.php:0	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP Stack trace:	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP Notice: Undefined index: HTTPS in /opt/snag-view/util/...	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP 2. ImageProxy->__construct() /opt/snag-view/fronten...	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP 1. {main}() /opt/snag-view/frontend/php/image.php:0	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP Stack trace:	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP Notice: Undefined index: HTTPS in /opt/snag-view/util/...	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP 2. ImageProxy->__construct() /opt/snag-view/fronten...	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP 1. {main}() /opt/snag-view/frontend/php/image.php:0	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP Stack trace:	
2012-11-13 23:38:34	snagview-ser...	Ok	✳	httpd: PHP Notice: Undefined index: HTTPS in /opt/snag-view/util/...	

Seite 1 von 47

Zeige 1 - 50 von 2325



# Quellen

- Auflistung aller unbearbeiteten Events
- nach Quellen
  - Syslog
  - E-Mail
  - SNMP-Traps
  - NeDi



Host: 1 0 0 0 | Service: 2 0 0 0 | 13.11.2012 23:41:31 | svadmin | **SNAG View**

Dashboard | Servicebrowser | **Eventlog**

Alerts | Blacklist | **Quellen** | Filter  
 Syslog | E-Mail | Traps | **NeDi**

Datum/Zeit	Host	Typ	Nachricht	Kommentar
2012-11-13 23:30:02	switch4390f1	⌘	Node 0001e6246f9b appeared on gi49 VI1 as - with IP 0.0.0.0	
2012-11-13 23:30:02	switch437aff	⌘	Node 0026379f278c appeared on gi48 VI1 as - with IP 0.0.0.0	
2012-11-13 23:04:19	sec-sw-04	⌘	Node 000c29cc3e97 appeared on DEFAULT_VLAN VI0 as with IP 192.168.16.126	
2012-11-13 20:30:05	switch437aff	⌘	Node 685d43e93b21 appeared on gi48 VI1 as - with IP 0.0.0.0	
2012-11-13 20:30:05	switch4390f1	⌘	Node 000c29d71473 appeared on gi43 VI1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1	⌘	Node 000413703443 appeared on gi49 VI1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1	⌘	Node 001c9b0108e0 appeared on gi49 VI1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1	⌘	Node 000c298745b9 appeared on gi32 VI1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1	⌘	Node 00041370341c appeared on gi49 VI1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1	⌘	Node 000413703390 appeared on gi49 VI1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1	⌘	Node 000413703439 appeared on gi49 VI1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1	⌘	Node 080027e234e0 appeared on gi49 VI1 as - with IP 0.0.0.0	

Seite 1 von 6 | 147 | Zeige 1 - 50 von 296





# Filtermöglichkeiten



# Felder

- jeder Event verfügt über allgemeine Felder
  - z.B.:  
Nachricht, Quelle, Status, etc...
- einige Events haben zusätzliche Felder
  - z.B.:  
eMail, Nedi

# Filterfunktionen

- Feld beinhaltet
- Feld matched auf regulären Ausdruck
- numerischer Vergleich mit Feld

# Aktionen

- Auf Alertliste setzen
- Auf Blackliste setzen
- Event verwerfen
- Status setzen

# Livebeispiel

The screenshot shows the SNAG View web interface in a browser window. The address bar displays the URL 172.16.100.131. The top navigation bar includes the SNAG View logo, a status bar with host and service counts (Host: 1, Service: 2), the current date and time (13.11.2012 23:50:49), and the user name (svadmin). The main content area is divided into several sections: a sidebar with 'Favoriten' and a list of filters (Severity, FooBar a, PHP Fehl, Link is D, Warning), a central area with tabs for 'Dashboard', 'Servicebrowser', and 'Eventlog', and a large configuration window titled 'Filter PHP Fehler ausblenden bearbeiten'. This window contains a form with a 'Pflichtfeld' (required field) for 'Aktion' and a list of actions including 'Erstellen', 'Löschen', 'Auf Alertliste setzen', 'Auf Blackliste setzen', 'Event verwerfen', 'Status setzen', 'Inhalte von Feld setzen/ändern', 'Korrelations ID setzen', and 'Korrelationsaktion ausführen'. A 'Speichern' button is located at the bottom right of the configuration window.



# Checkmöglichkeiten



# Einfache Checks

- Einträge auf Alertlist
- Anzahl „Warning“ & „Criticals“ auf Alertlist
- Höchster Status auf Alertlist
- gefiltert nach Host oder gesamt



# Komplexe Checks

- Events in einem Zeitraum
- Events eines Subtyps
- Events mit Feldinhalt
- u.v.m.

# Livedemo

The screenshot shows the SNAG View 3 web interface. At the top, there's a navigation bar with the SNAG View logo and a user profile for 'svadmin'. Below this, a dashboard provides a summary of host and service statuses. The 'Servicebrowser' section displays a table of services for the host 'snagview-server', all with an 'OK' status. The 'Alertticker' section shows a list of recent alerts, including a warning for 'Timespan' and a hard alert for 'Timespan'.

**Host Summary:** Host: 1 (Up), 0 (Down), 0 (Warning), 0 (Critical). Service: 5 (Up), 0 (Down), 0 (Warning), 0 (Critical).

Hoststatus	Hostname	Bezeichnung	Status	Letzter Check
Up	snagview-server	Alertlisten Einträge	OK	14.11.2012 01:30:11
		Max Warning and Critical	OK	14.11.2012 01:30:11
		Timespan	OK	14.11.2012 01:31:11

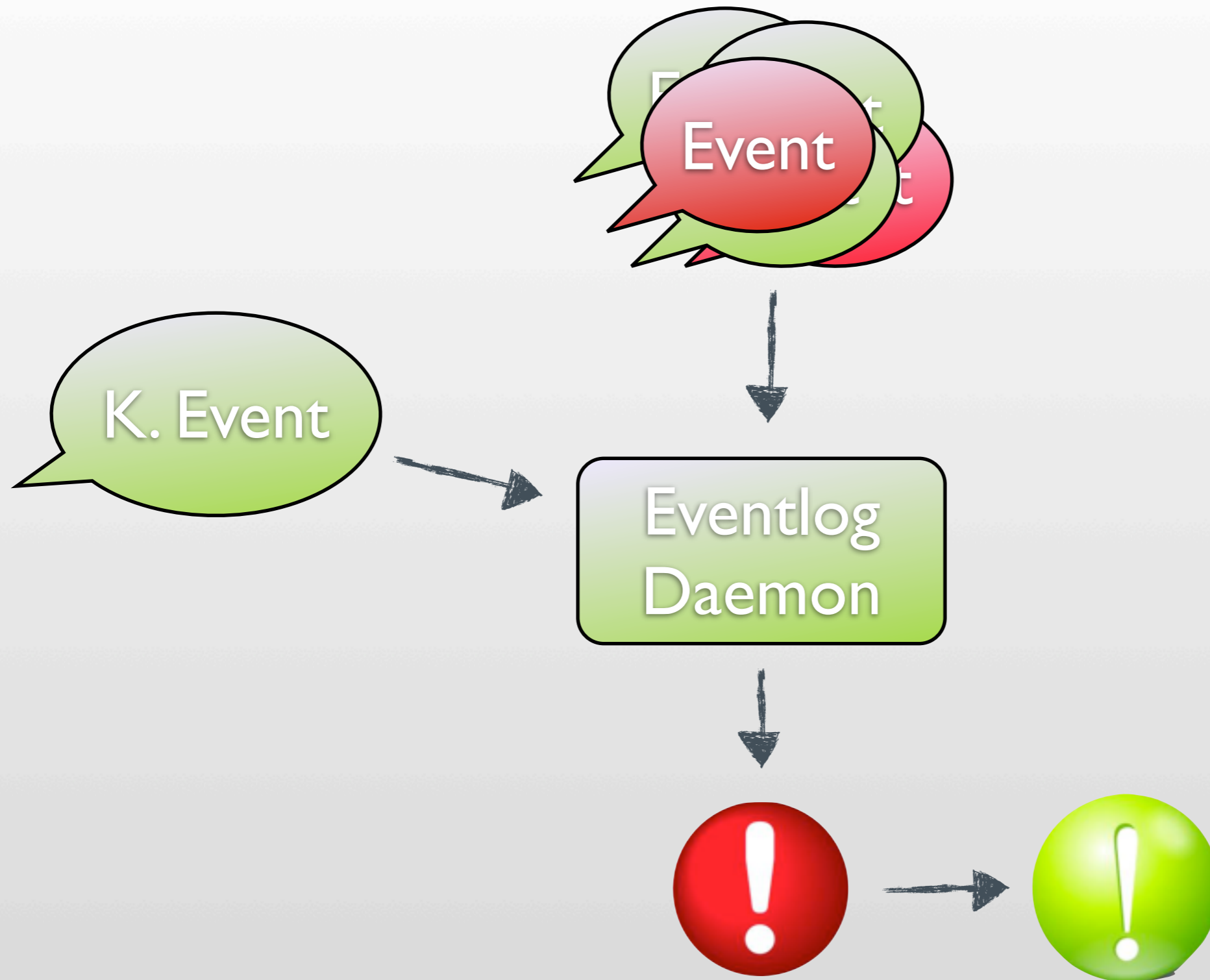
Zeitpunkt	T...	Label	Statusyp	Neuer Status	Alter Status	Ausgabe
14.11.2012 01:26:13		snagview-server - Timespan	SOFT	OK	Warning	EVENTLOG O...
14.11.2012 01:25:13		snagview-server - Timespan	SOFT	Warning	OK	EVENTLOG W...
14.11.2012 01:24:53		snagview-server - Timespan	HARD	OK	Critical	EVENTLOG O...



# Korrelation von Events









# Korrelation von Events

- Viele Events, die in einer Beziehung zueinander stehen, können in einem kurzen Zeitraum eintreffen
- Dabei können einige ignoriert werden,
- einige lösen einen Fehlerstatus aus
- und andere heben einen Fehlerstatus wieder auf

# Livedemo

The screenshot shows a web browser window with the address bar displaying '172.16.100.131'. The page title is 'SNAG-View 3'. The interface features a top navigation bar with the 'SNAG View' logo and a user profile 'svadmin'. Below the navigation bar, there are several status indicators: 'Host: 1 0 0 0' and 'Service: 2 0 1 0'. A search bar is also present. The main content area is divided into several sections: 'Dashboard', 'Servicebrowser', and 'Eventlog'. A modal dialog titled 'Filter Korrelationstest - OK bearbeiten' is open, showing a configuration interface for a correlation test. The dialog has a 'Filter' section with a list of items including 'Severity', 'Node Me', 'Foobar a', 'Link is D', 'Warning', 'Snagvier', 'Test Wa', 'PHP Fehl', and 'Korrelat'. Below the filter section, there is an 'Aktion' section with a 'Pflichtfeld' (required field) and an 'Aktiondefinition' section containing three items: 'Bei Korrelations ID »dienst«: »Event bestät', 'Auf Alertliste setzen', and 'Status auf »ok« setzen'. A 'Speichern' (Save) button is located at the bottom right of the dialog.





# Fragen ???



Vielen Dank für Ihre  
Aufmerksamkeit!

