Verarbeitung von Events

Udo Stachowiak / Frank Hildebrandt
SECTOR NORD AG

Stand 11-2012

SECTOR NORD AG
OpenSource based enterprise solutions

Kundenworkshop 2012

- Monitoring von Events
- SV3 Eventlog
- Livedemo

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Datenquellen für Monitoring

Aktive Abfragen:

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

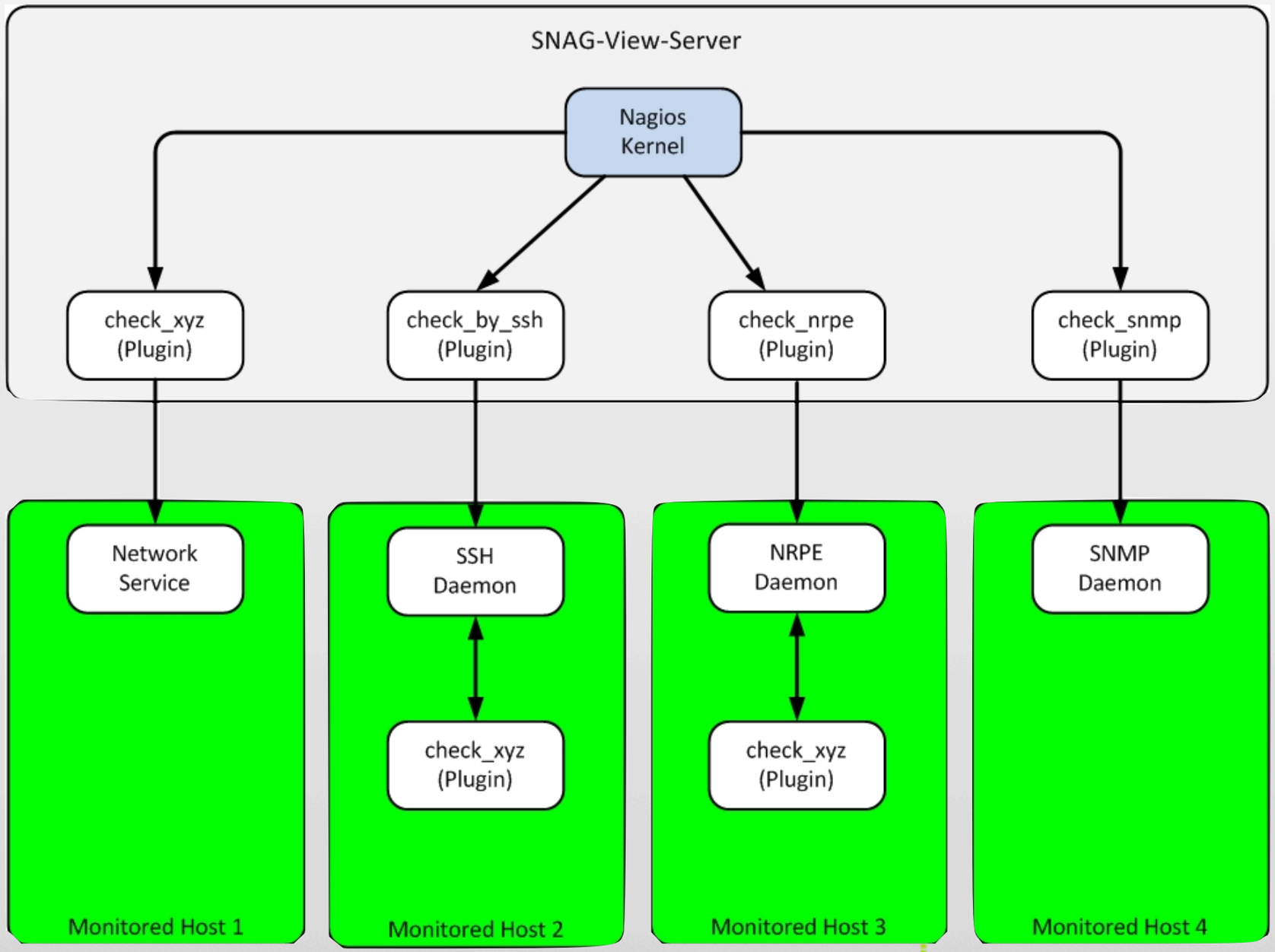
Events:

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

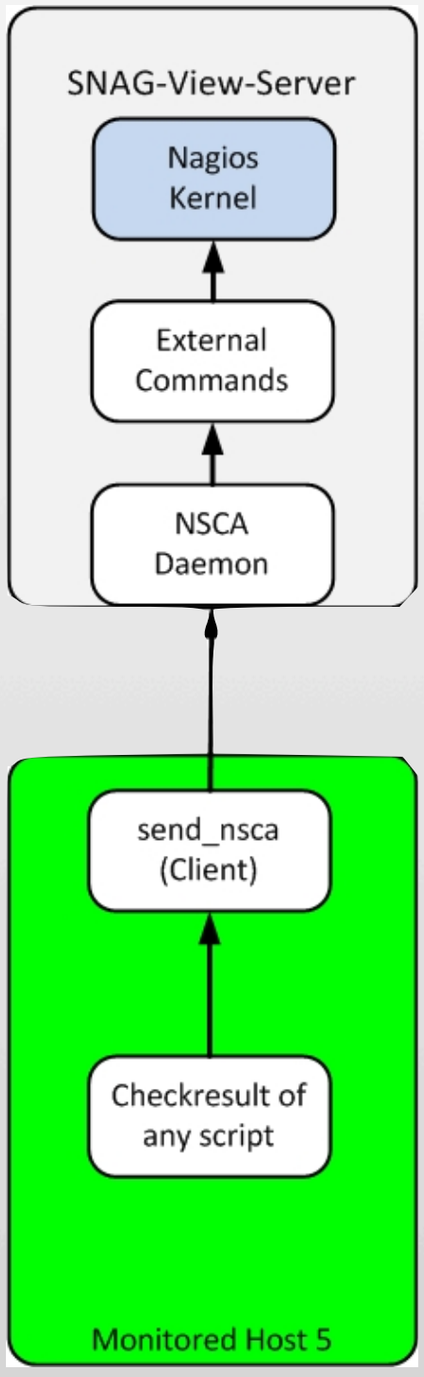
Remote Checks



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

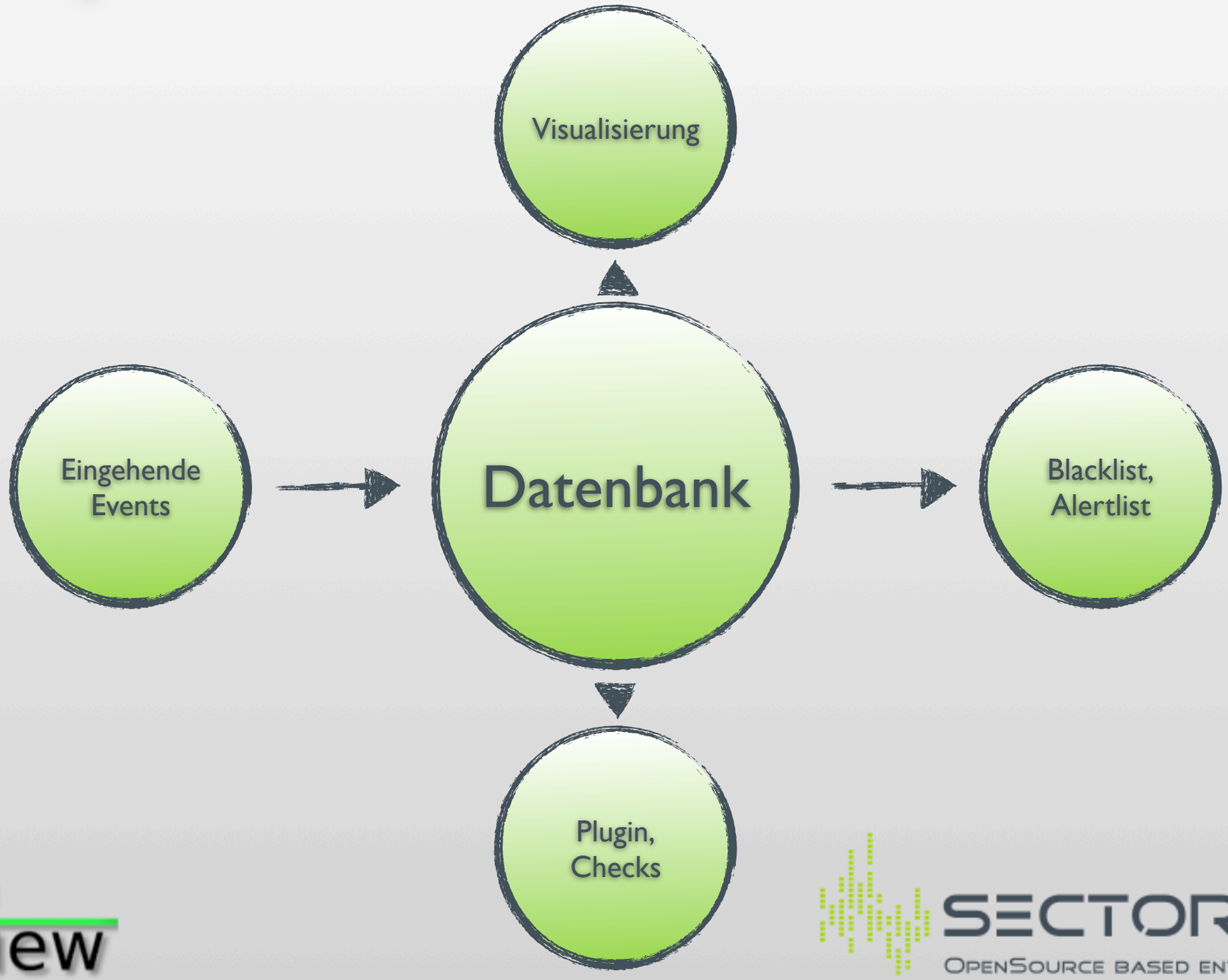
Remote Checks



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Speichern von Events



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Fragen ???

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

~~Syslog++~~

Eventlog Agent

Regelbasierte Überwachung von auftretenden Events

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Frank Hildebrandt

31 Jahre alt
Entwickler & Projektmanager

Twitter: @frank_ol

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

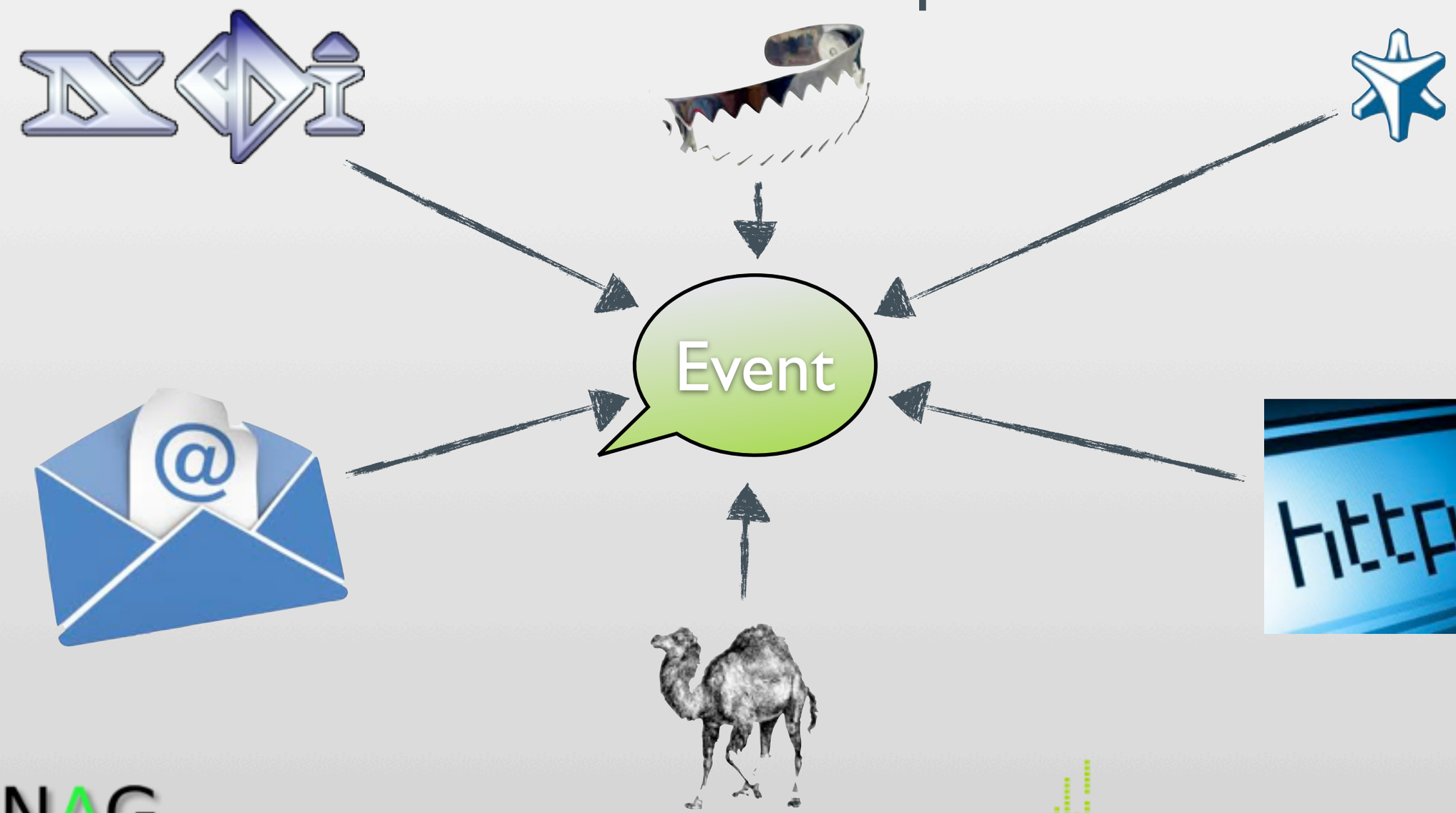
Warum Eventlog

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

eingehende Events



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Event

Eventlog Daemon

Filter

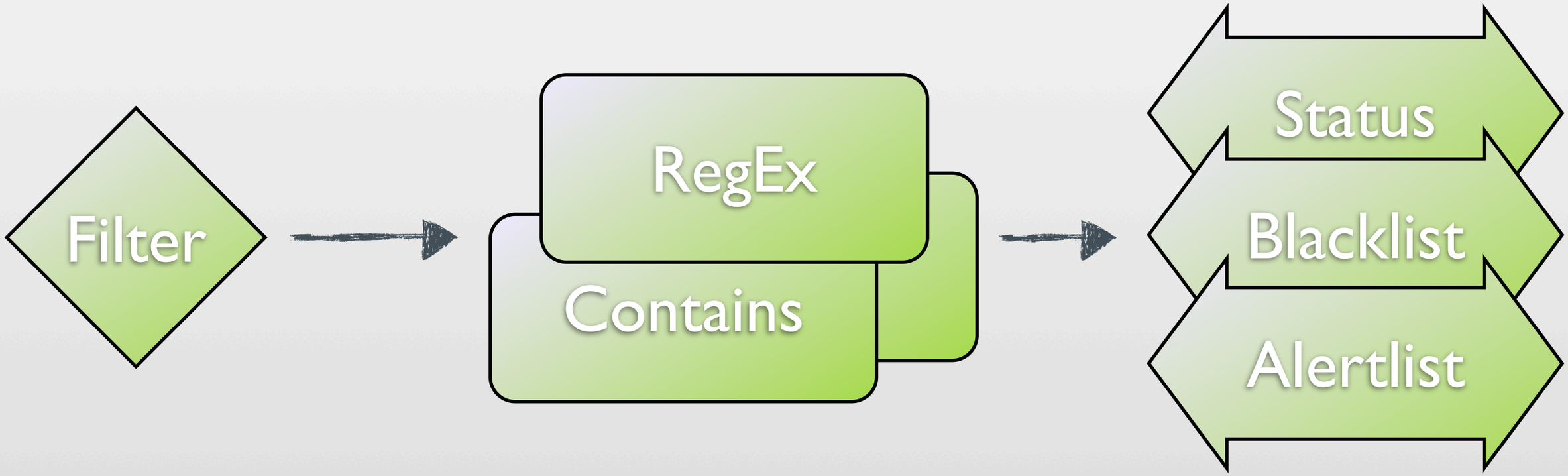
SNAG View

SECTOR NORD AG

OpenSource based enterprise solutions

Filterfunktionen

Aktionen



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Die „Eventlog“ Listen

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Alertlist

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

SNAG-View 3

172.16.100.131

Host: 1 0 0 0

Service: 2 0 0 0 0

13.11.2012 23:37:54

svadmin

SNAG View

Favoriten

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

SNAG View

SECTOR NORD AG

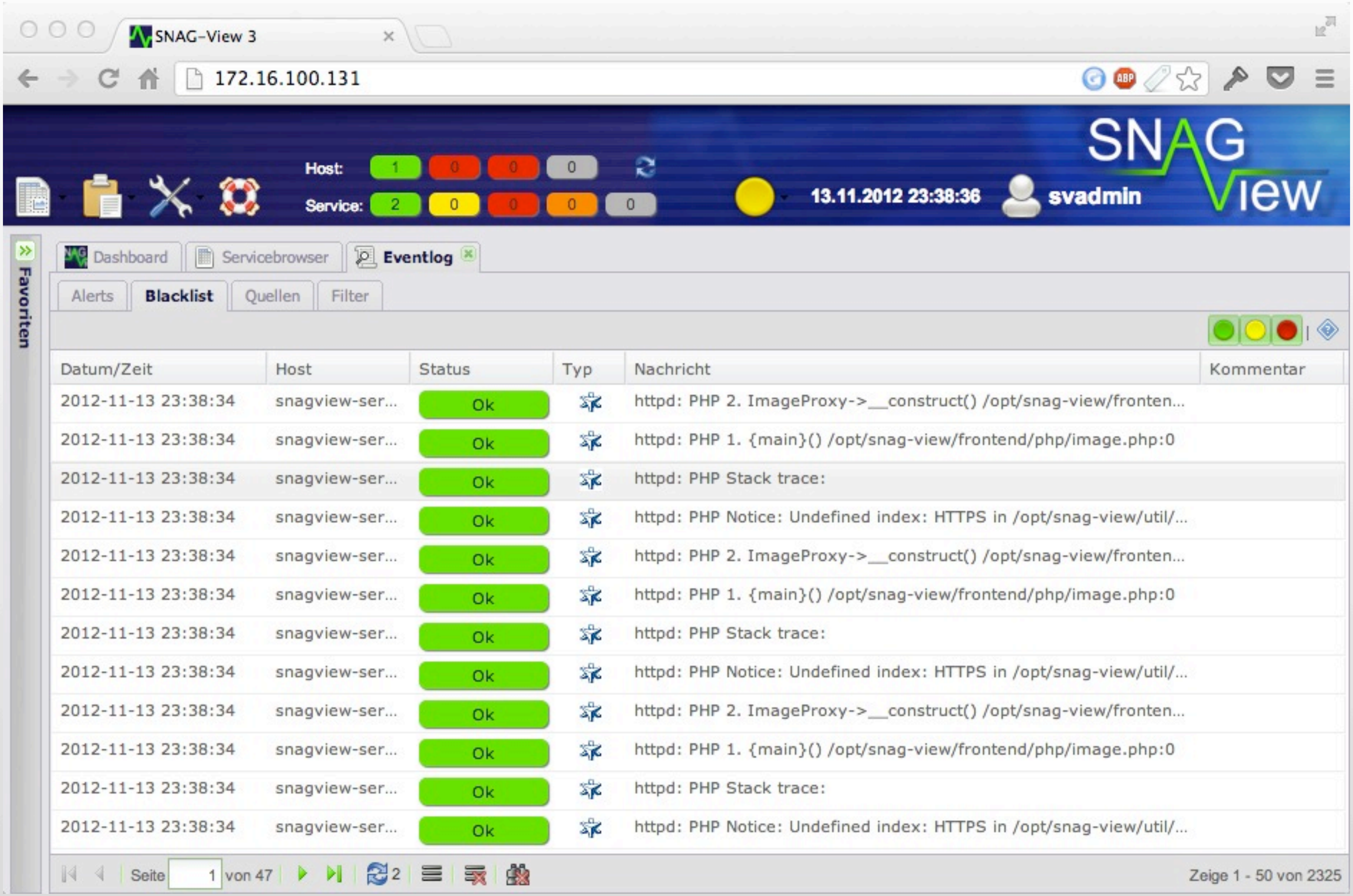
OpenSource based enterprise solutions

Blacklist

- Archiv von Events
- Servicechecks möglich

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions


SNAG-View 3
172.16.100.131
Host: 1 0 0 0
Service: 2 0 0 0 0
13.11.2012 23:38:36
svadmin
SNAG View
Favoriten
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
2
Zeige 1 - 50 von 2325

Quellen

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

SNAG-View 3

172.16.100.131

Host: 1 0 0 0

Service: 2 0 0 0 0

13.11.2012 23:41:31

svadmin

SNAG View

Favoriten

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 Vl1 as - with IP 0.0.0.0	
2012-11-13 23:30:02	switch437aff		Node 0026379f278c appeared on gi48 Vl1 as - with IP 0.0.0.0	
2012-11-13 23:04:19	sec-sw-04		Node 000c29cc3e97 appeared on DEFAULT_VLAN Vl0 as with IP 192.168.16.126	
2012-11-13 20:30:05	switch437aff		Node 685d43e93b21 appeared on gi48 Vl1 as - with IP 0.0.0.0	
2012-11-13 20:30:05	switch4390f1		Node 000c29d71473 appeared on gi43 Vl1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1		Node 000413703443 appeared on gi49 Vl1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1		Node 001c9b0108e0 appeared on gi49 Vl1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1		Node 000c298745b9 appeared on gi32 Vl1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1		Node 00041370341c appeared on gi49 Vl1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1		Node 000413703390 appeared on gi49 Vl1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1		Node 000413703439 appeared on gi49 Vl1 as - with IP 0.0.0.0	
2012-11-13 19:30:03	switch4390f1		Node 080027e234e0 appeared on gi49 Vl1 as - with IP 0.0.0.0	

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

SNAG View

SECTOR NORD AG

OpenSource based enterprise solutions

Filtermöglichkeiten

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Felder

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Filterfunktionen

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

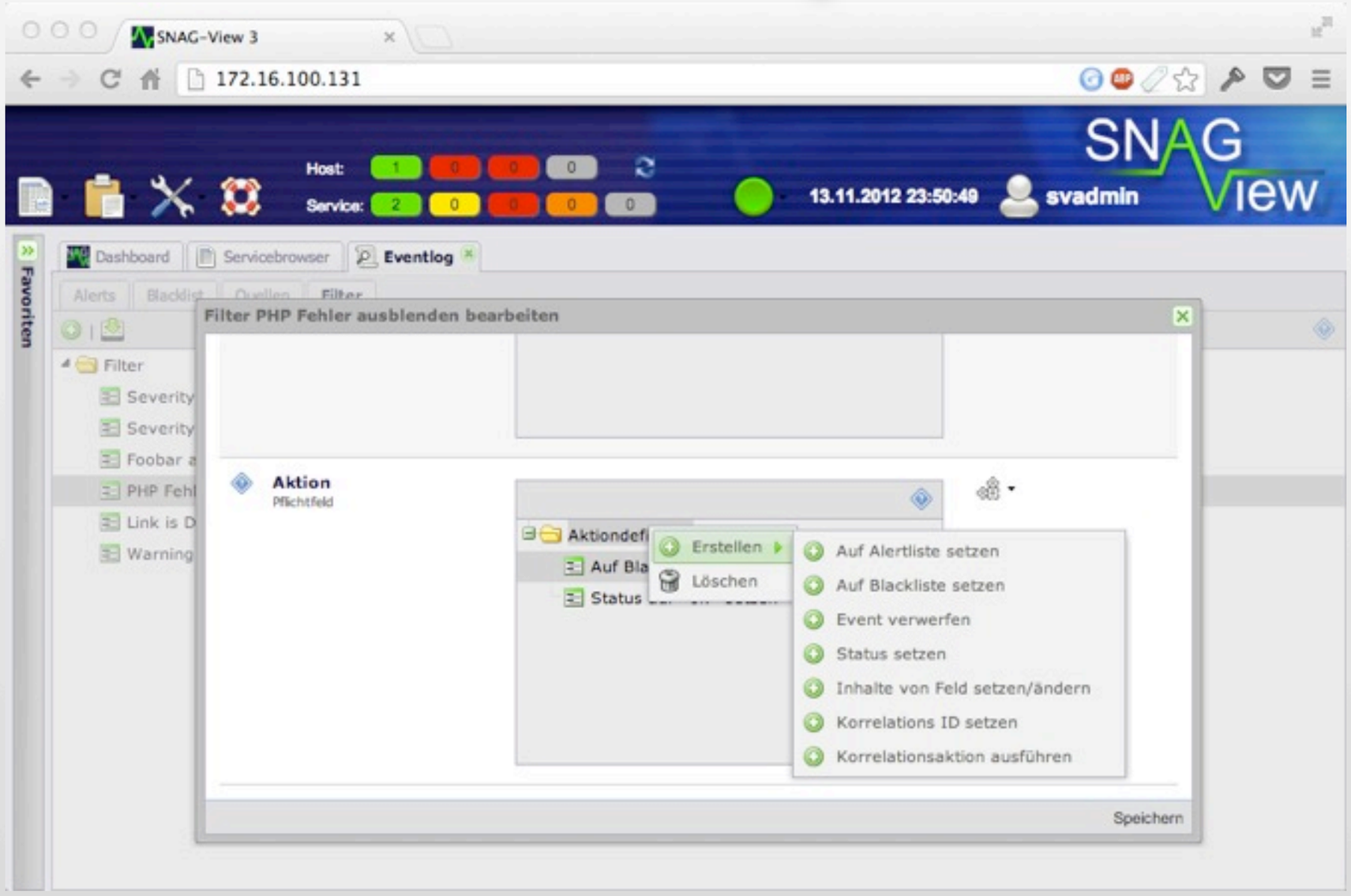
Aktionen

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Livebeispiel



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Checkmöglichkeiten

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Einfache Checks

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

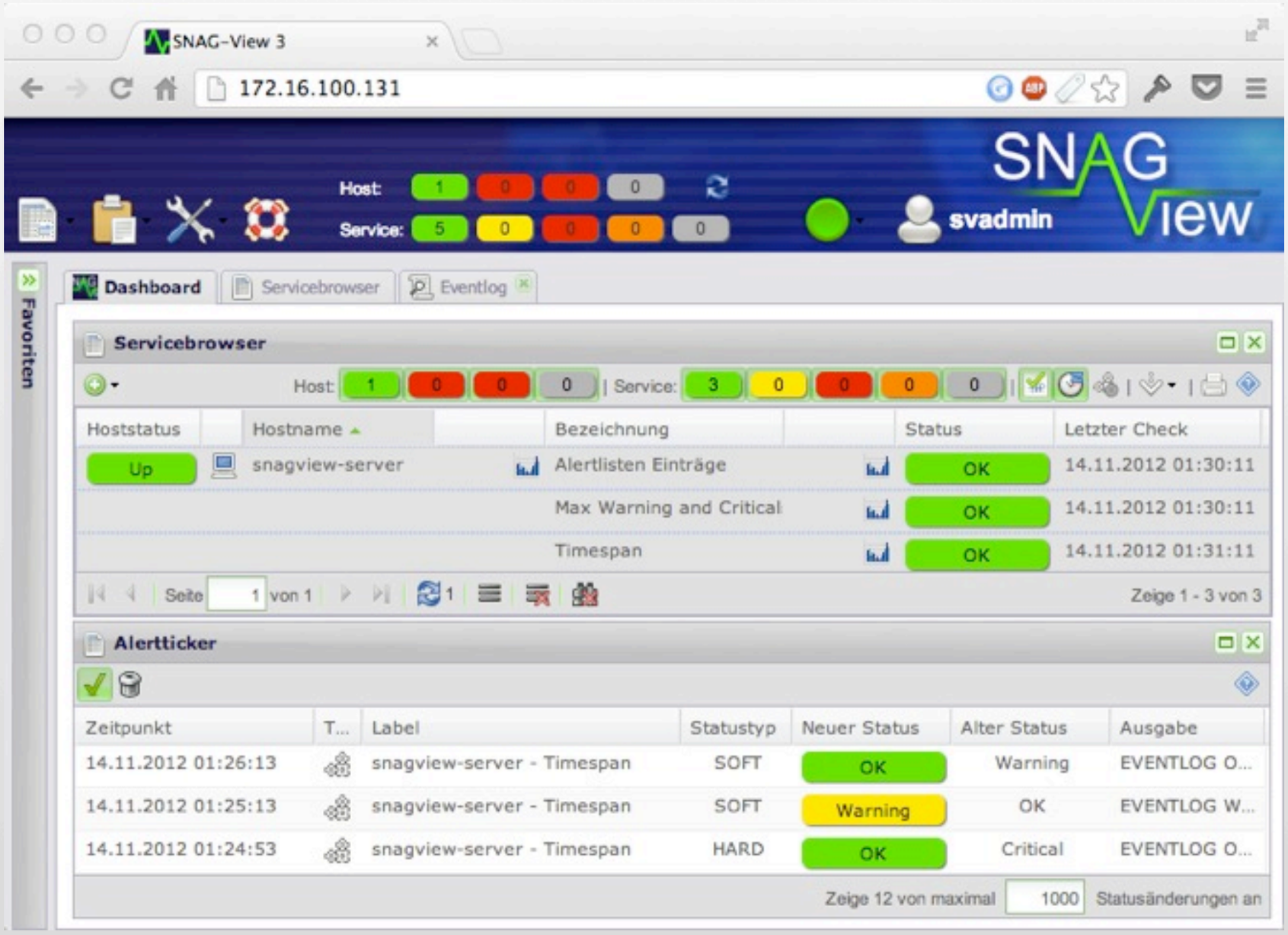
Komplexe Checks

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Livedemo



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

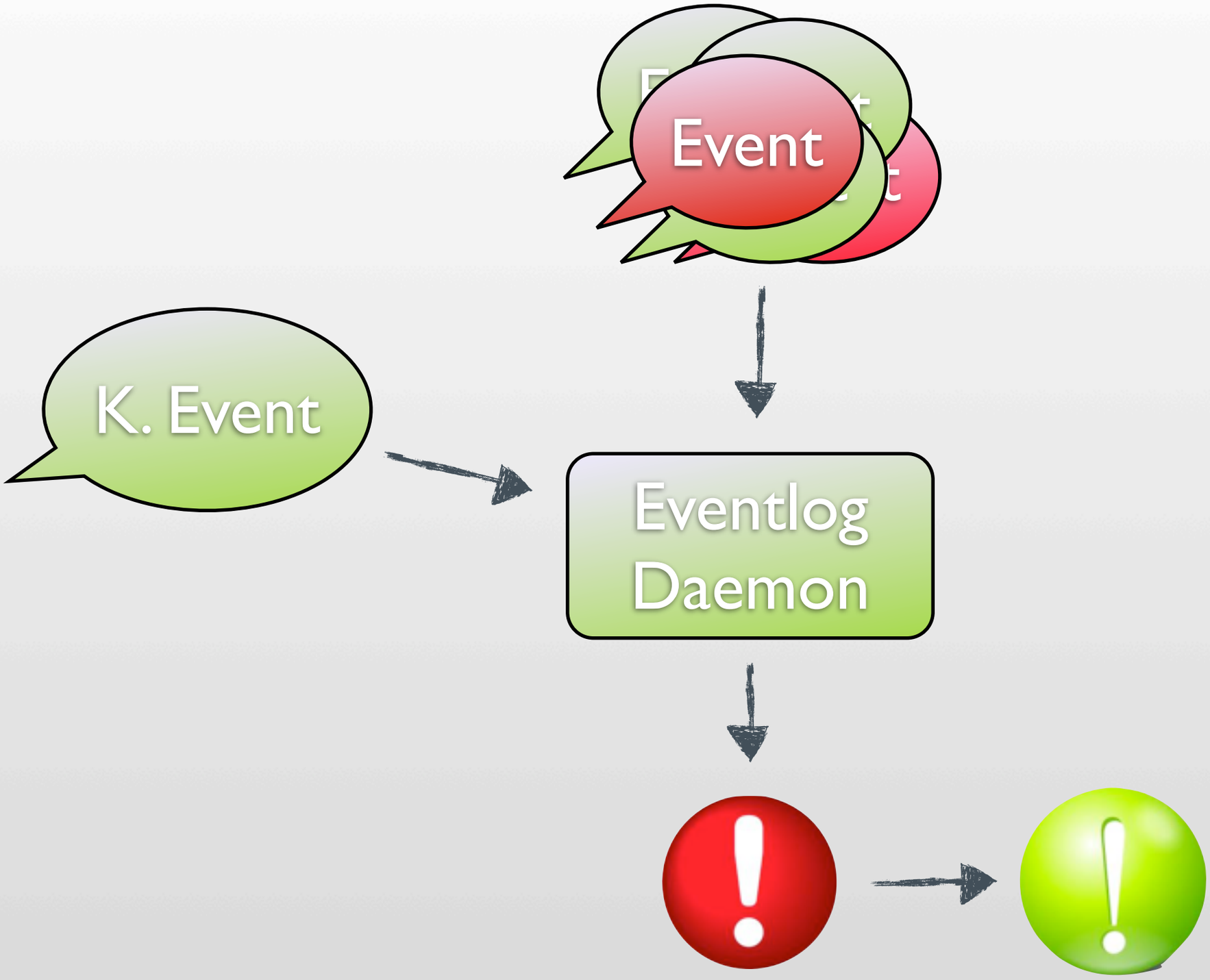
Korrelation von Events

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

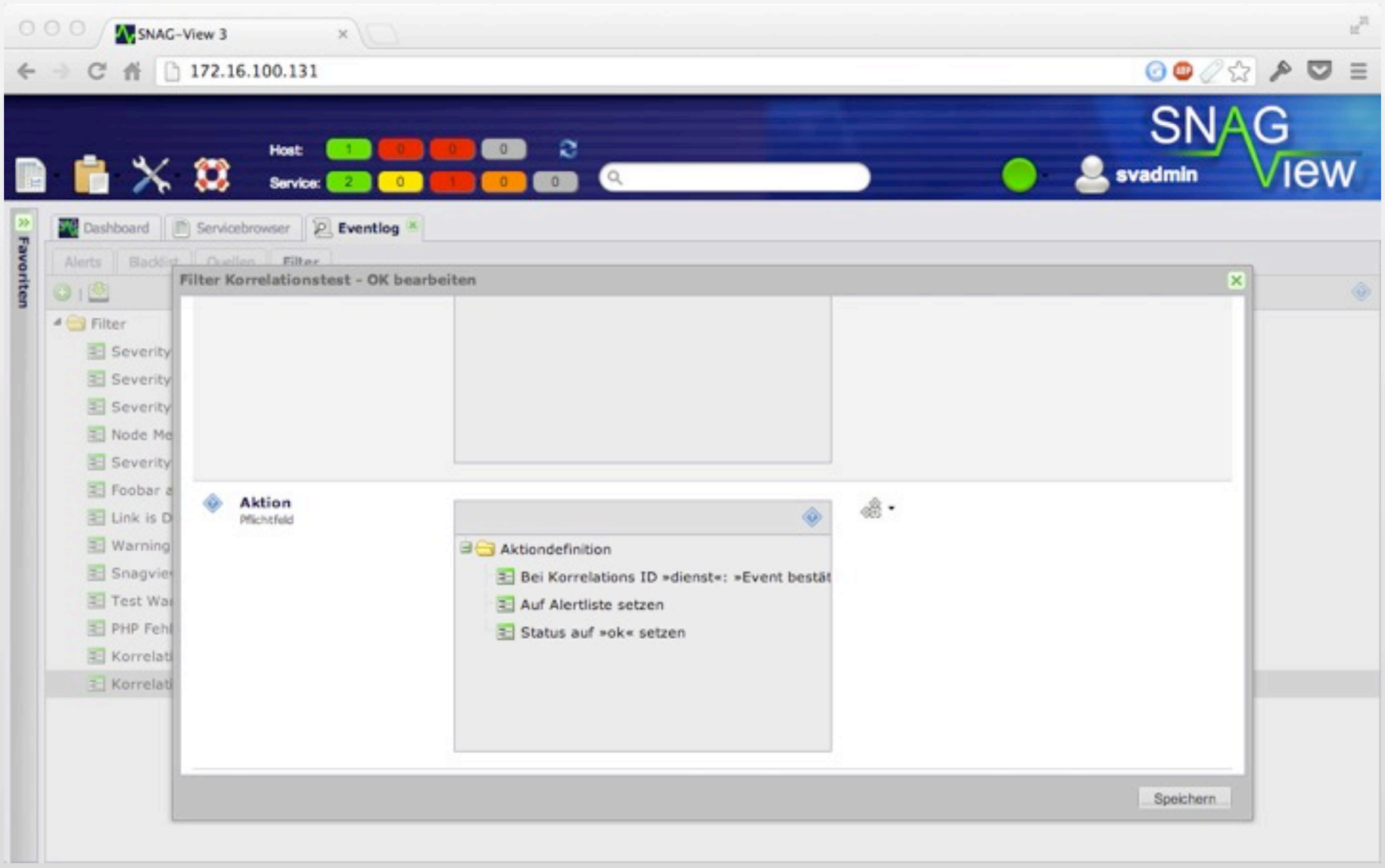
Korrelation von Events

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

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Livedemo



SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Fragen ???

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions

Vielen Dank für Ihre Aufmerksamkeit!

SNAG View

SECTOR NORD AG
OpenSource based enterprise solutions