ZABBIX MONITORING

DIE VOLLE KONTROLLE

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Thorsten Kramm
SLAC 2011

Was ist Zabbix?

Opensource Monitoringlösung
Basierend auf:
Serverdaemon
SQL Datenbank
Webgui
Agent

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Was macht Zabbix?

- Daten sammeln (Items)
  Zabbix Agent (Unix, Windows)
  SNMP, IMPI, SSH, Telnet, ODBC
- Daten auswerten (Trigger)
- Daten präsentieren (Graph)
- Aktionen auslösen (Action)
  Mail, SMS, Telefonanruf,
  Kommando lokal und remote

Monitoring

Wissen, was passiert.

Wissen, was zu tun ist.

Zabbix installieren

Systemvoraussetzungen Server

- Unix mit gcc
- SQL Datenbank
  MySQL, Postgre SQL, Oracle, DB2
- Webserver mit PHP

Die Installation aus den Quellen gelingt auf allen gängigen Distributionen.

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Zabbix konfigurieren

- Konfiguration ausschließlich über Webgui
- Alle Daten werden in DB gespeichert
- Agenten sind „dumm“, alle Steuerung geht vom Server aus
- Minimale Konfig-Datei für Server mit DB Zugangsdaten

Monitoring

Wissen, was passiert.

Wissen, was zu tun ist.

Zabbix
Konfigurieren

Terminologie

Host:

Wer wird beobachtet?
IP Adresse, DNS-Name

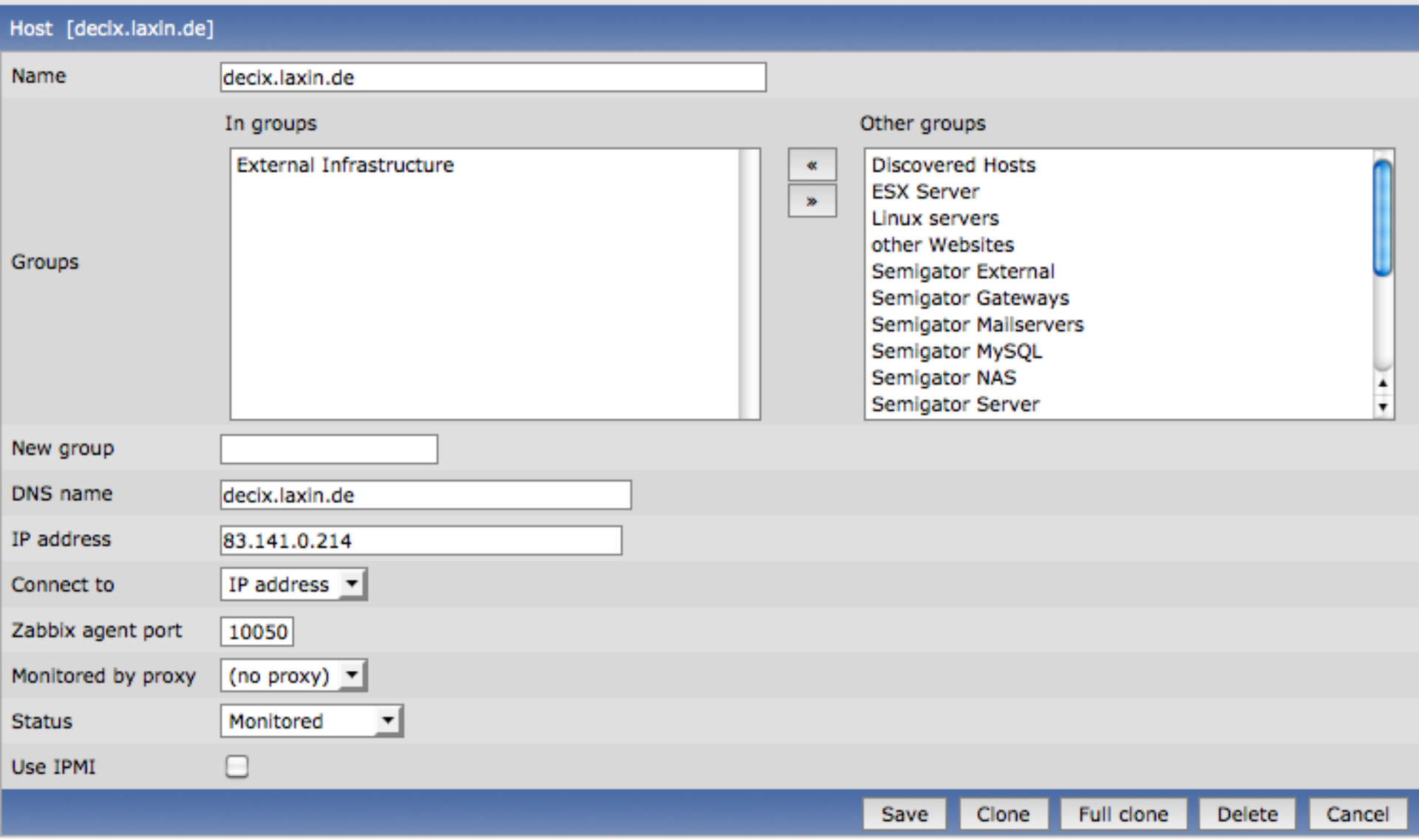
Host werden in Gruppen zusammengefasst.

Template = vorkonfigurierter Host ohne Adresse, die eine Konfiguration vererben.

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Host anlegen*:



Zabbix
Konfigurieren

Terminologie

Item:

Was wird beobachtet?

CPU-Auslastung,
Speicherverbrauch,
Erreichbarkeit, Festplattenauslatung, etc.

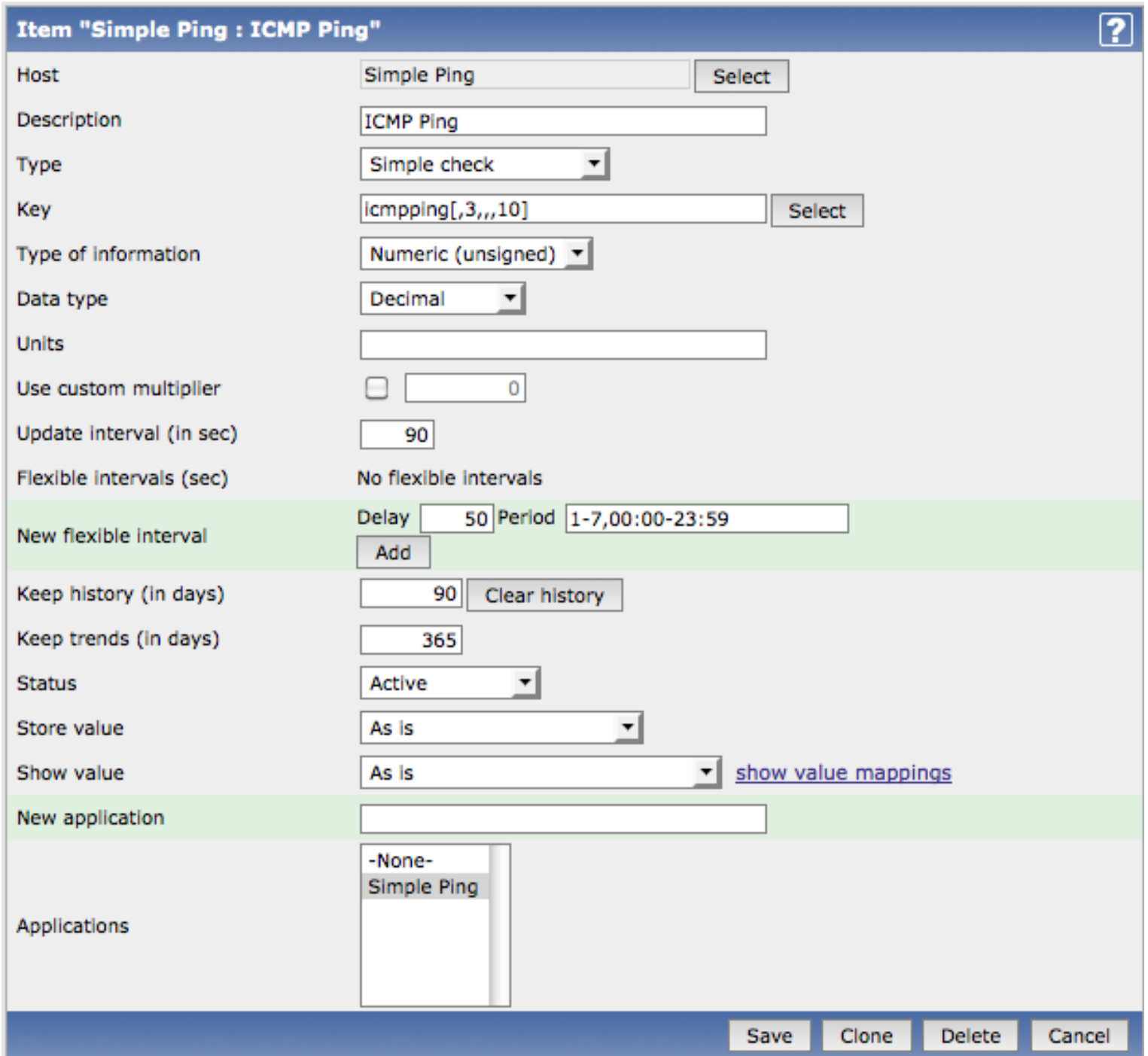
Aus welcher Quelle stammen die Daten?

Zabbix Agent, SNMP, IPMI, SSH, ODBC, externe Skripte auf Agent oder Server

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Item anlegen *



Werte der Items: *

ITEMS Group all Host all

Filter

Show items with description like

Filter Reset

Host	Description	Last check	Last value	Change
dev.semigator.int	**Linux Base Information** (8 Items)			
	CPU IDLE AVG5	08 Jun 2010 20:40:34	99.855922	-0.01
	CPU IOwait AVG5	08 Jun 2010 20:40:35	0.000000	-
	CPU load AVG5	08 Jun 2010 20:40:33	0.030000	+0.01
	CPU User AVG5	08 Jun 2010 20:40:37	0.050255	-0
	Free disk on / (percent)	08 Jun 2010 20:40:39	78.356553	-0
	Free disk on /var (percent)	08 Jun 2010 20:40:40	82.712075	-0.01
	Net Usage eth0 IN	08 Jun 2010 09:31:45	56.76 b	-23.50
	Net Usage eth0 OUT	08 Jun 2010 09:32:21	50.87 b	-33.92
dev.semigator.int	**System Base Information** (4 Items)			
	Agent Ping	08 Jun 2010 20:40:07	1	-
	Local Time	08 Jun 2010 09:30:09	1275982209.000000	+360
	Packet Loss	08 Jun 2010 20:40:09	0.000000	-
	Ping Check	08 Jun 2010 20:40:31	1	-
exchange.semigator.int	**Exchange** (1 Items)			
	Exchange Process Running	08 Jun 2010 20:40:14	1	-
exchange.semigator.int	**System Base Information** (4 Items)			
	Agent Ping	08 Jun 2010 20:39:52	1	-
	Local Time	08 Jun 2010 09:28:54	1275982134.000000	+360
	Packet Loss	08 Jun 2010 20:39:54	0.000000	-
	Ping Check	08 Jun 2010 20:40:09	1	-
exchange.semigator.int	**Windows Base Information** (2 Items)			
	CPU Load	08 Jun 2010 20:40:16	0.383333	-2.55
	Free Disk C: Percent	08 Jun 2010 09:29:18	14.386481	-0.01
gate1.semigator.de	**Base Checks** (1 Items)			
gate1.semigator.de	**Postfix** (1 Items)			
gate1.semigator.int	**Linux Base Information** (8 Items)			
	CPU IDLE AVG5	08 Jun 2010 20:40:13	99.842197	+0.10
	CPU IOwait AVG5	08 Jun 2010 20:40:18	0.000000	-
	CPU load AVG5	08 Jun 2010 20:39:53	0.000000	-
	CPU User AVG5	08 Jun 2010 20:40:23	0.067155	-0.03

Zabbix
Konfigurieren

Terminologie

Trigger:

Daten der Items auswerten

Daten der Items berechnen

Durchschnitt, Summe etc.

Sollwerte definieren und mit Istwerten vergleichen

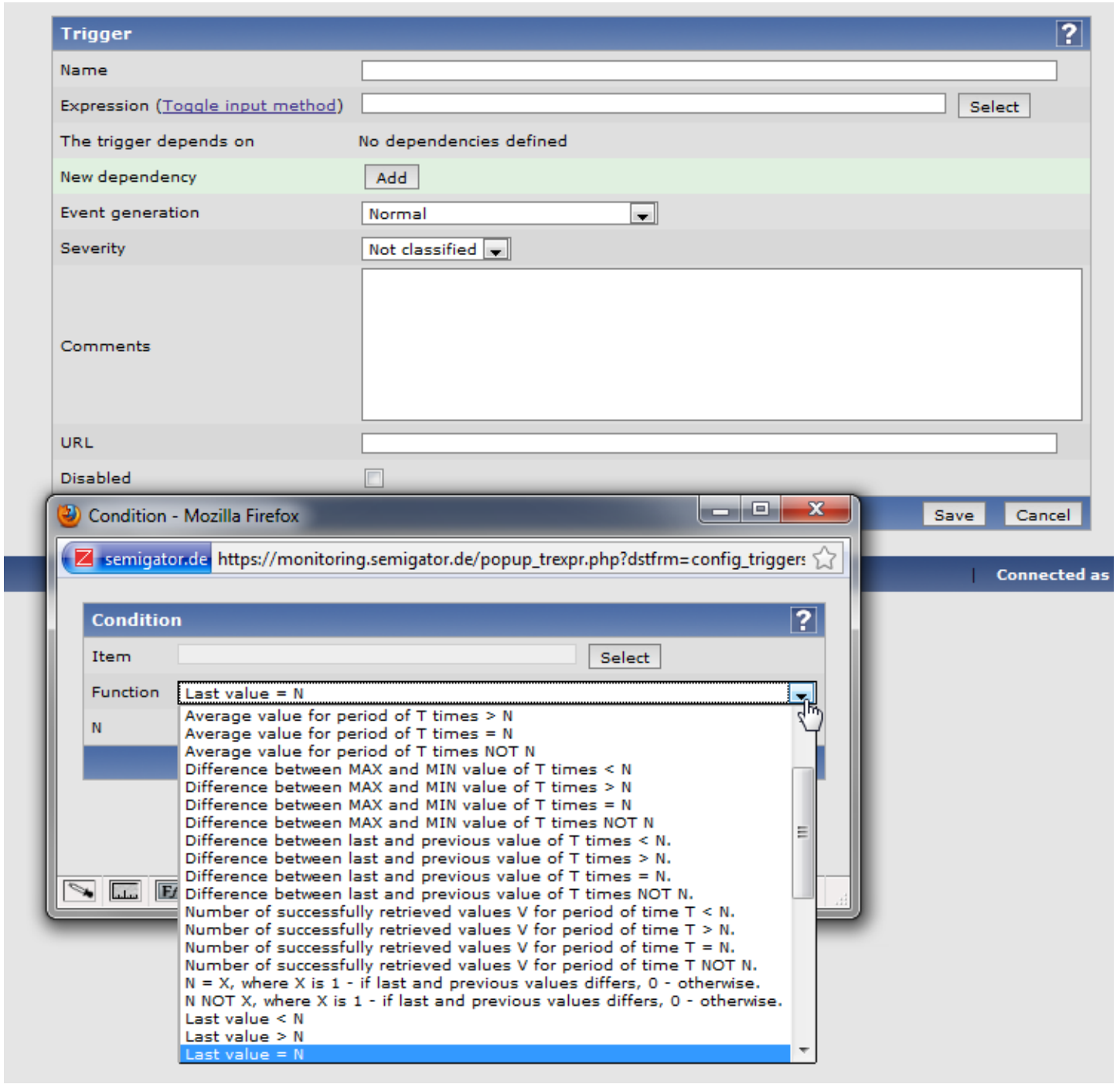
Trigger kennt nur den Status TRUE oder FALSE.

Monitoring

Wissen, was passiert.

Wissen, was zu tun ist.

Trigger anlegen:



Zabbix
Konfigurieren

Terminologie

Template:

Templates = fertige Konfiguration bestehend aus Items und Triggern.
Hosts können zu beliebig vielen Templates hinzugefügt werden.
Der Großteil der Konfiguration wird über Templates realisiert.

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Template Übersicht

Templates	Applications	Items	Triggers	Graphs	Linked templates	Linked to
Semigator agentless	Applications (1)	Items (1)	Triggers (1)	Graphs (0)	-	gate1.semigator.de, gate2.semigator.de, postamt.semigator.de, wi.semigator.de
Semigator Base	Applications (1)	Items (4)	Triggers (2)	Graphs (0)	-	dev.semigator.int, exchange.semigator.int, gate1.semigator.int, gate2.semigator.int, sql03.semigator.int, syslog.semigator.int, web01.semigator.int
Semigator Exchange	Applications (1)	Items (1)	Triggers (0)	Graphs (0)	-	exchange.semigator.int
Semigator Linux Base	Applications (1)	Items (9)	Triggers (0)	Graphs (0)	-	dev.semigator.int, gate1.semigator.int, gate2.semigator.int, monitoring.semigator.de, office.semigator.int, sql03.semigator.int, syslog.semigator.int, web01.semigator.int
Semigator MySQL	Applications (1)	Items (3)	Triggers (0)	Graphs (0)	-	sql03.semigator.int
Semigator Postfix	Applications (1)	Items (4)	Triggers (0)	Graphs (0)	-	gate1.semigator.int, gate2.semigator.int, office.semigator.int, web01.semigator.int
Semigator Windows Base	Applications (1)	Items (3)	Triggers (0)	Graphs (0)	-	exchange.semigator.int
SMTP Server	Applications (1)	Items (0)	Triggers (0)	Graphs (0)	-	exchange.semigator.int, gate1.semigator.de, gate2.semigator.de
Website	Applications (1)	Items (1)	Triggers (1)	Graphs (0)	-	pv2.semigator.de, vtiger.semigator.com, www.semigator.de

Template und Items Übersicht

Log	Description ▲	Triggers	Key	Interval	History	Trends	Type	Status
	Semigator Base:Agent Ping	Triggers (1)	agent.ping	60	30	60	Zabbix agent	Active
	Semigator Linux Base:CPU IDLE AVG5	Triggers (0)	system.cpu.util[,idle,avg5]	90	90	365	Zabbix agent	Active
	Semigator Linux Base:CPU IOwait AVG5	Triggers (0)	system.cpu.util[,iowait,avg5]	90	90	365	Zabbix agent	Active
	Semigator Linux Base:CPU KERNEL AVG5	Triggers (0)	system.cpu.util[,kernel,avg5]	90	90	365	Zabbix agent	Not support
	Semigator Linux Base:CPU load AVG5	Triggers (0)	system.cpu.load[,avg5]	90	90	365	Zabbix agent	Active
	Semigator Linux Base:CPU User AVG5	Triggers (0)	system.cpu.util[,user,avg5]	90	90	365	Zabbix agent	Active
	Semigator Linux Base:Free disk on / (percent)	Triggers (0)	vfs.fs.size[/,pfree]	90	90	365	Zabbix agent	Active
	Semigator Linux Base:Free disk on /var (percent)	Triggers (0)	vfs.fs.size[/var,pfree]	90	90	365	Zabbix agent	Active
	Semigator Base:Local Time	Triggers (0)	system.localtime	360	90	365	Zabbix agent	Active
	Mails bounced per 5min	Triggers (0)	mysql.exec[bounced_mails]	300	90	365	Zabbix agent	Active
	Mails deferred per 5min	Triggers (0)	mysql.exec[deferred_mails]	300	90	365	Zabbix agent	Active
	Mails sent per 5min	Triggers (0)	mysql.exec[sent_mails]	300	90	365	Zabbix agent	Active
	Semigator MySQL:mysqld up and running	Triggers (0)	proc.num[mysqld]	90	90	365	Zabbix agent	Active
	Semigator MySQL:mysql ping	Triggers (0)	mysql.ping	90	90	365	Zabbix agent	Active
	Semigator Linux Base:Net Usage eth0 IN	Triggers (0)	net.if.in[eth0]	90	90	365	Zabbix agent	Active
	Semigator Linux Base:Net Usage eth0 OUT	Triggers (0)	net.if.out[eth0]	90	90	365	Zabbix agent	Active
	Semigator Base:Packet Loss	Triggers (0)	icmppingloss	60	30	60	Simple check	Active
	Semigator Base:Ping Check	Triggers (1)	icmpping	60	30	60	Simple check	Active

Zabbix
Konfigurieren

Terminologie

Action:

Aktion in Abhängigkeit von einem Trigger auslösen.

Aktionen =

- Email senden
- Lokales Kommando ausführen
- Remote Kommando ausführen

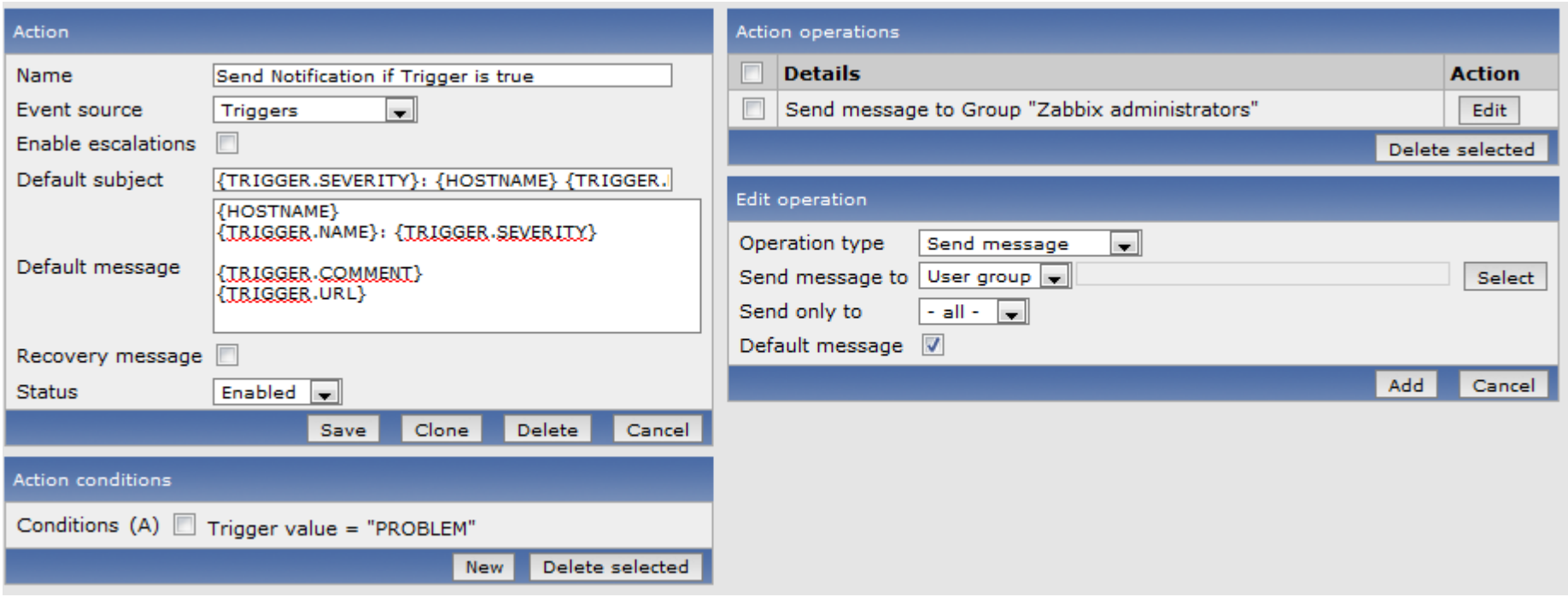
In vielen Fällen reicht eine Standardaktion: „Send Notification if Trigger is true”

Monitoring

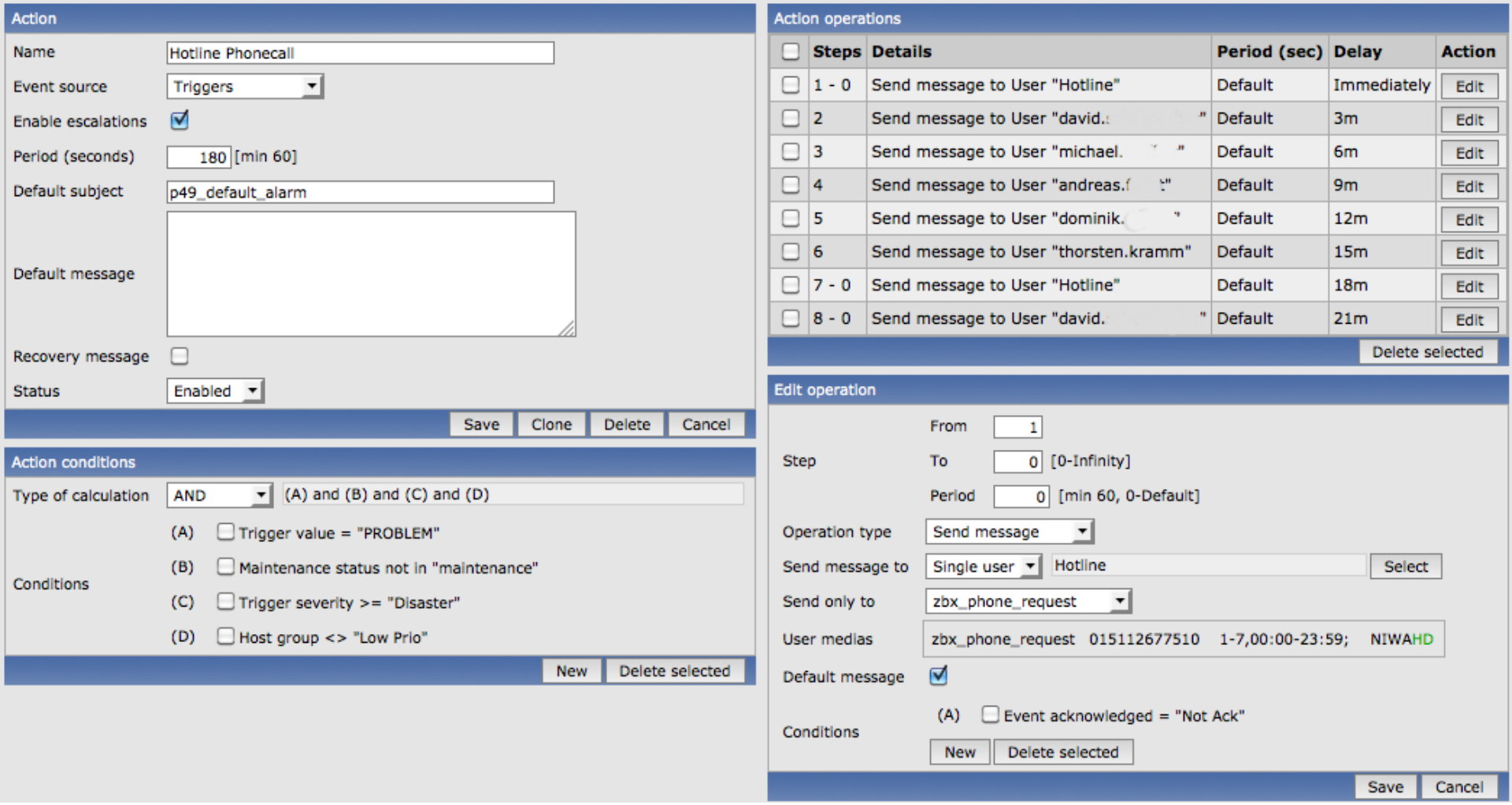
Wissen, was passiert.

Wissen, was zu tun ist.

Aktion Mail senden



Aktion Telefonkette



Zabbix
Konfigurieren

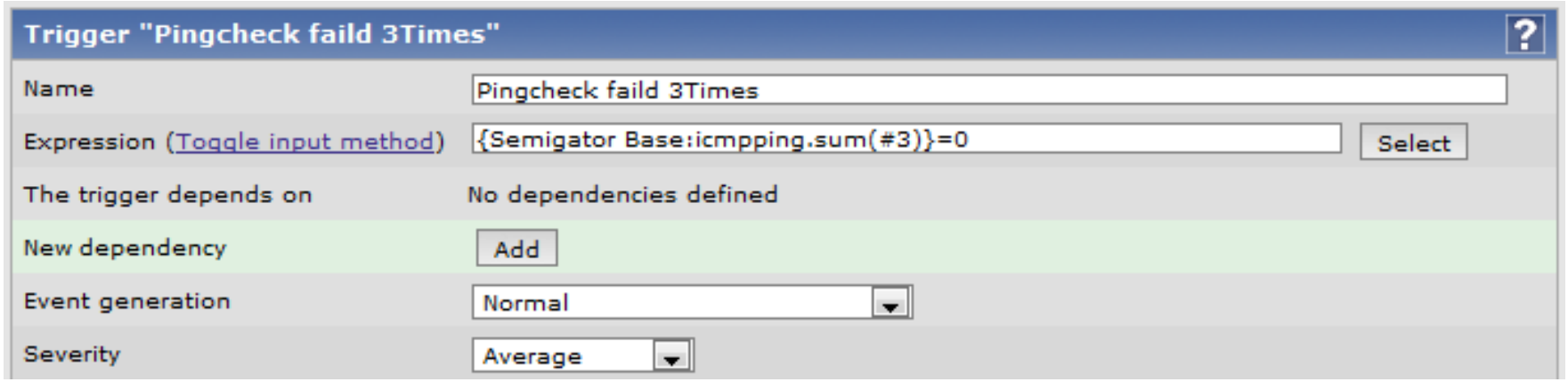
Alarmieren

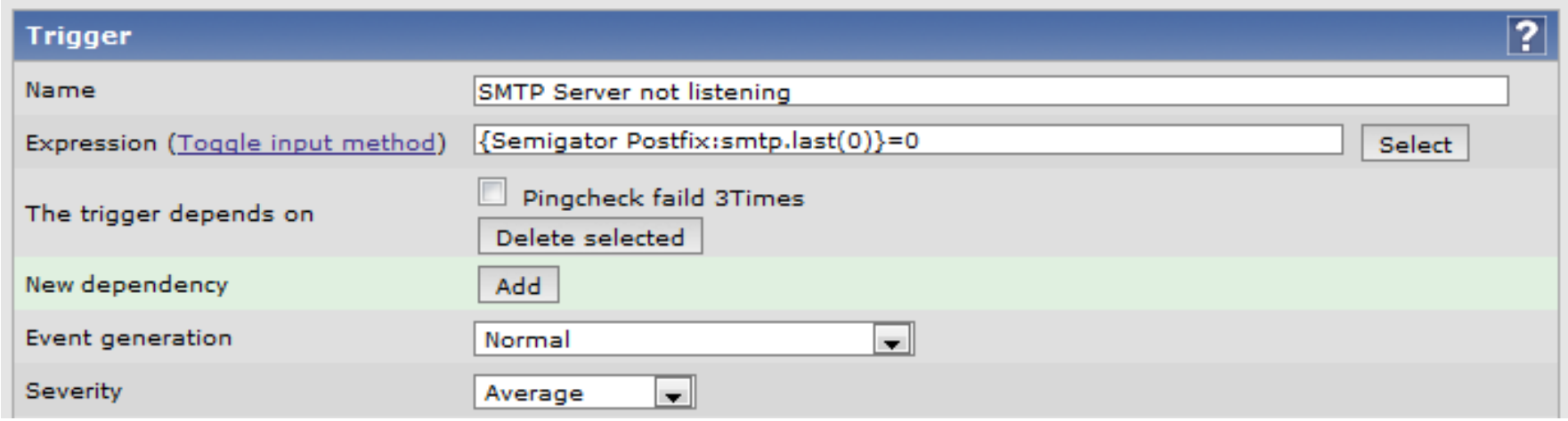
- Schwellwerte so einstellen, dass Fehlalarme vermieden werden.
- Trigger in Abhängigkeit setzen

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Abhängige Trigger





Zabbix
Konfigurieren

Alarmieren

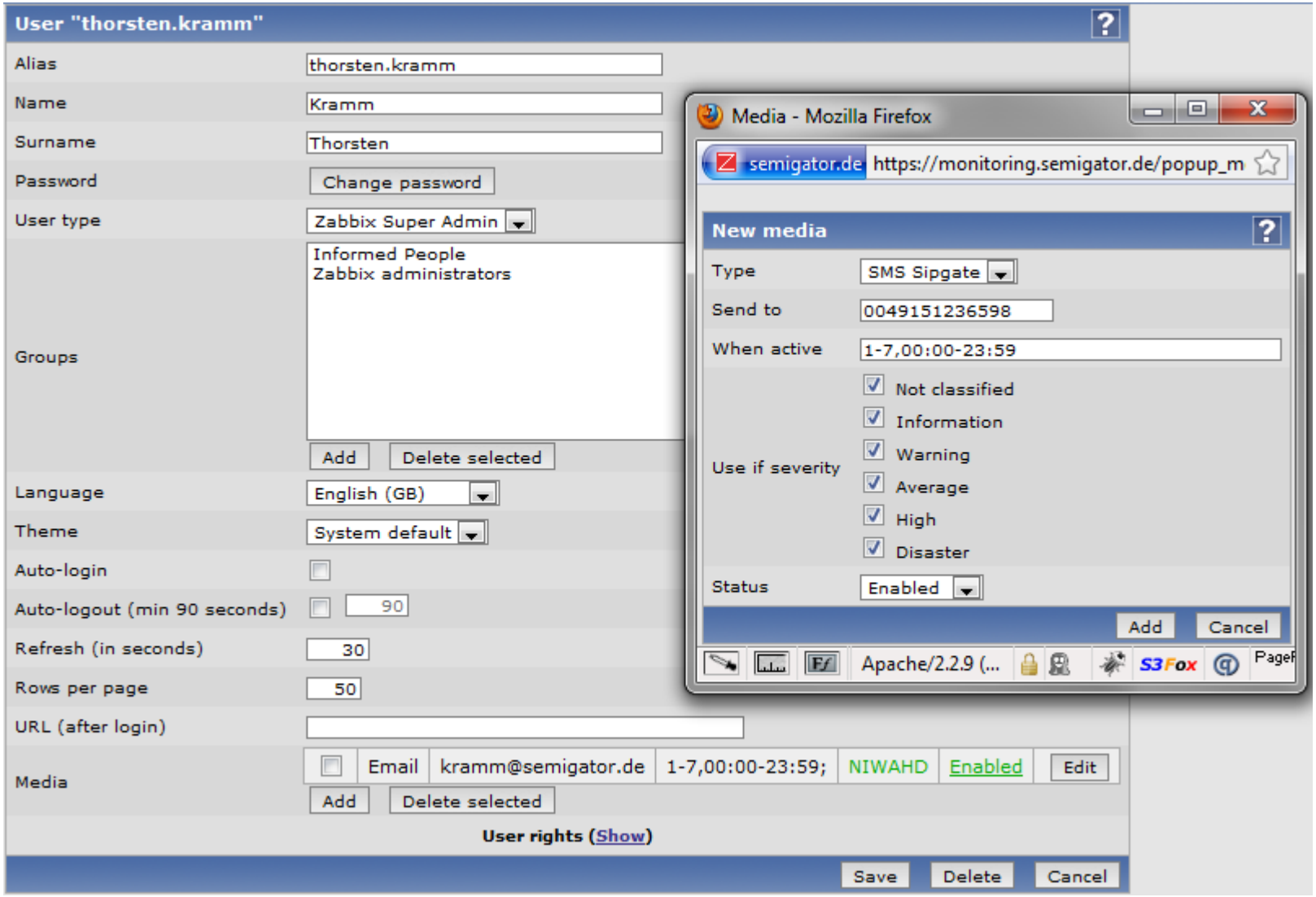
SMS Versenden:
Einfach z.B. über Sipgate-API
Sicherer über USB UMTS-Stick

Zabbix Benutzer steuern selbst, wann sie wie alarmiert werden.

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

SMS Alarm hinzufügen



Wahres Wissen ist Wissen,
das auf die Ursachen zurückgeht.

Francis Bacon

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Zabbix
Konfigurieren

Visualisieren

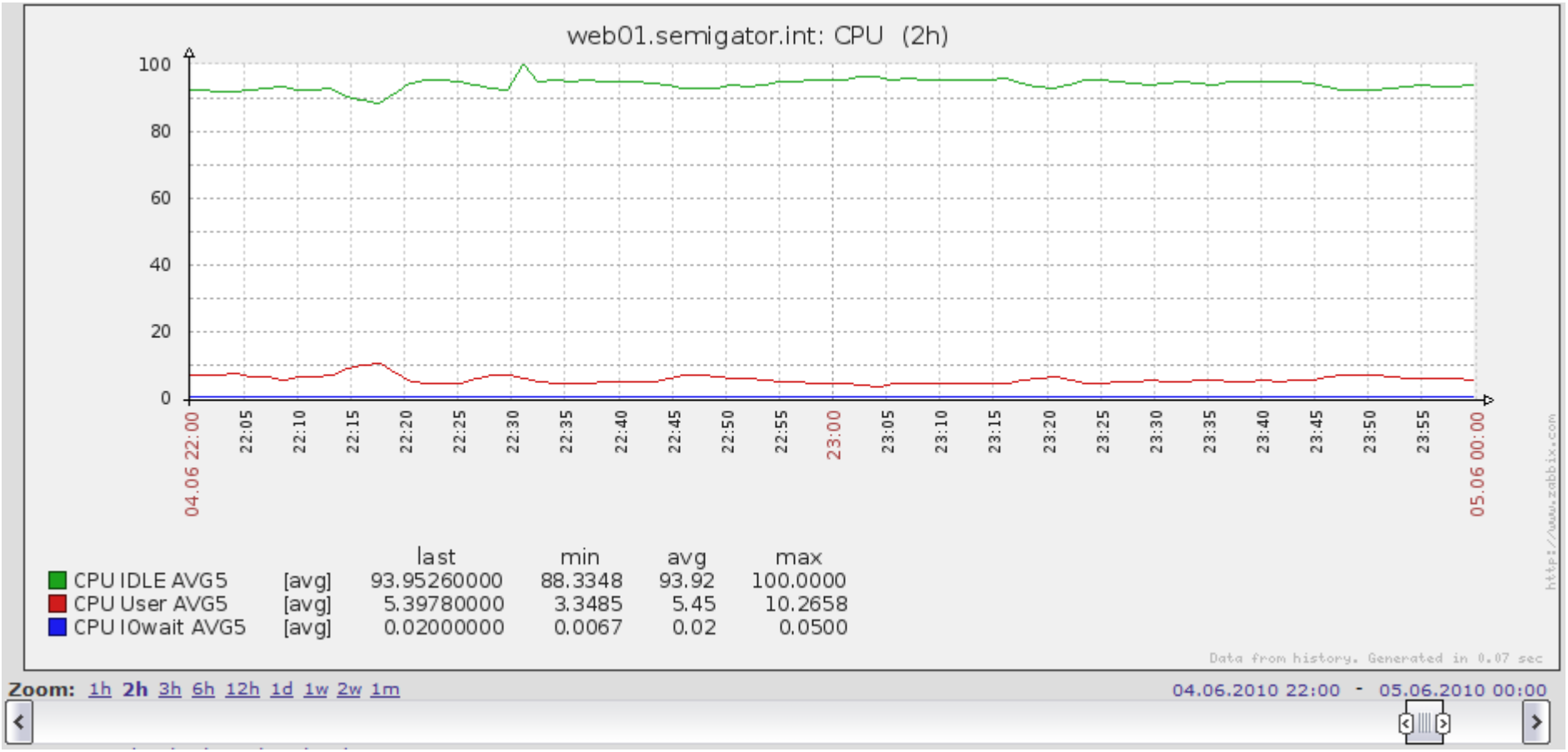
- Werte von Items in Graphen abbilden
- Mehrere Graphen zu Screen gruppieren
- Graphen können auch über Template konfiguriert werden.

Monitoring

Wissen, was passiert.

Wissen, was zu tun ist.

Graph


web01.semigator.int: CPU (2h)
100
80
60
40
20
0
04.06 22:00
22:05
22:10
22:15
22:20
22:25
22:30
22:35
22:40
22:45
22:50
22:55
23:00
23:05
23:10
23:15
23:20
23:25
23:30
23:35
23:40
23:45
23:50
23:55
05.06 00:00
last min avg max
CPU IDLE AVG5 [avg] 93.95260000 88.3348 93.92 100.0000
CPU User AVG5 [avg] 5.39780000 3.3485 5.45 10.2658
CPU IOwait AVG5 [avg] 0.02000000 0.0067 0.02 0.0500
Data from history. Generated in 0.07 sec
Zoom: 1h 2h 3h 6h 12h 1d 1w 2w 1m
04.06.2010 22:00 - 05.06.2010 00:00

Zabbix
Konfigurieren

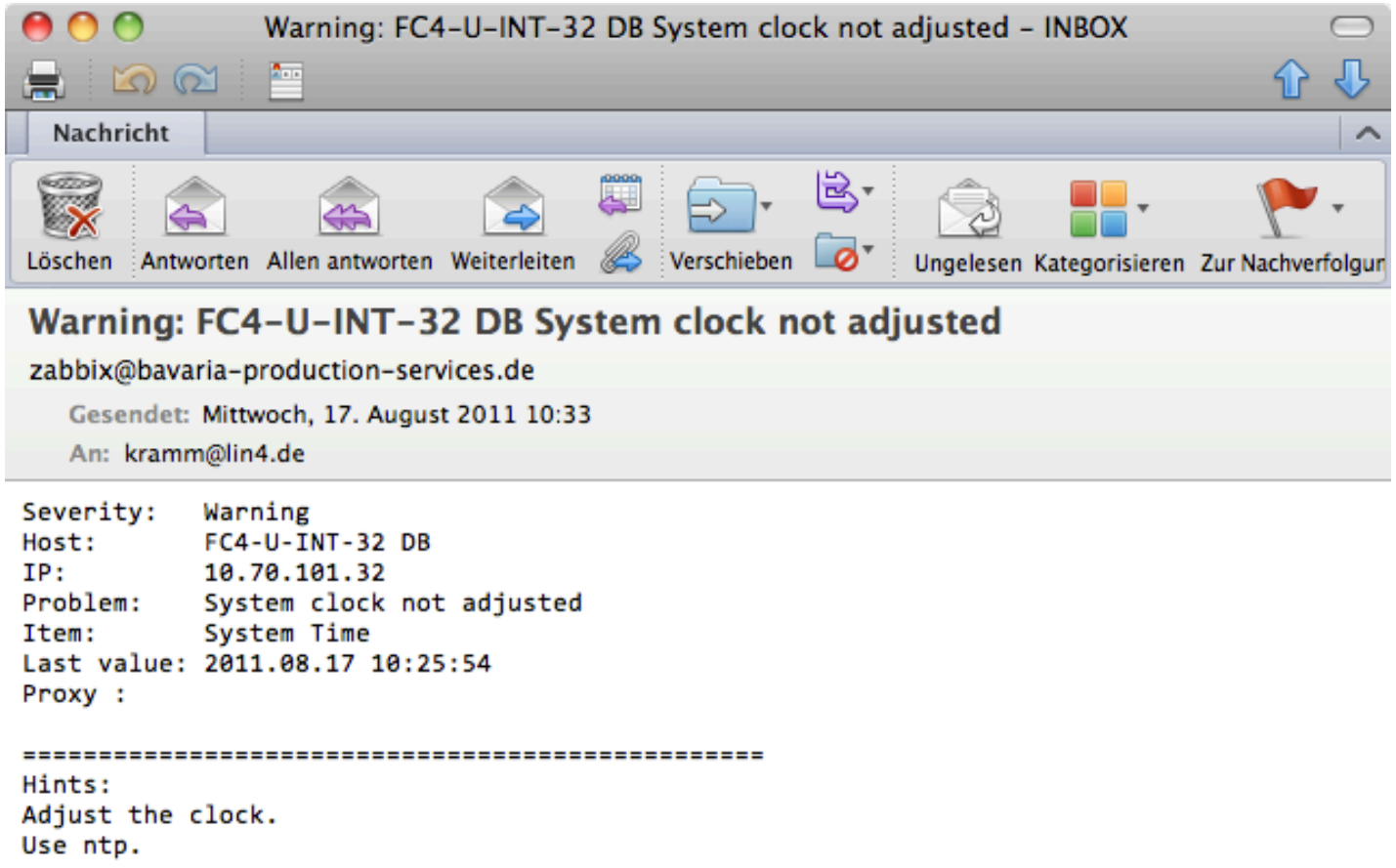
Informieren

- Zu jedem Trigger kann ein Link zu einem Wiki oder Notfallhandbuch hinterlegt werden
- Über Platzhalter in den Mailtexten können aber auch Suchen nach Triggern in Dokumentationen ausgelöst werden
  wiki.doku.de?search={TRIGGER_NAME}

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Alarm per Mail



Sonst noch was?

- Webseitenüberwachung inkl. Klickstrecken und POST-Requests
- Client Simulation für gängige Protokolle
- Ausgabe von Triggerstatus kann leicht aus der DB oder der API abgelesen werden

Monitoring

Wissen, was passiert.

Wissen, was zu tun ist.

Sonst noch was?

- Zabbix Proxy für Netzwerksegmente, DMZ, Intranet etc.
- Syslog mit Datenbank sinnvolle Ergänzung (Application und KPI Monitoring)

Monitoring

Wissen, was passiert.

Wissen, was zu tun ist.

Dokumentation

- Viele Tutorials für Einsteiger und Profis unter

http://lab4.org/wiki

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Support

DV Lösungen Schreiner GmbH

- Zabbix-Installationen aller Größen
- Einrichtung Monitoring für Linux und Windows
- Entwicklung von kundenspezifischen Checks
- Beratung
- Worry-Free Zabbix Appliance
- Outsourcing von Monitoring

www.dvloesungen.de

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.

Wissen nennen wir jenen
kleinen Teil
der Ungewissheit,
den wir geordnet und
klassifiziert haben.

Ambrose Bierce

Monitoring

Wissen, was passiert.
Wissen, was zu tun ist.