

Inhaltsverzeichnis

1	Wie ist dieses Buch aufgebaut?	1
1.1	Über dieses Buch	1
1.2	Der große Zabbix-Baukasten.	1
1.3	Die Reihenfolge der Kapitel.	2
1.4	Schnelleinstieg	2
1.5	Formalien	3
1.5.1	Typografie	3
1.5.2	Englische Begriffe und Anglizismen	3
2	Der Einstieg: Was ist Monitoring?	5
2.1	Warum Monitoring?	5
2.2	Monitoring ist mehr als ein Alarm im Fehlerfall	5
2.3	Zabbix, die Datenkrake.	8
2.4	Was leistet Zabbix?	9
2.5	Die Grenzen und Schwächen von Zabbix	10
2.6	Bestandteile und Funktionen von Zabbix	10
2.7	Die Basisterminologie	11
2.7.1	Host und Item: Daten sammeln	11
2.7.2	Trigger: Daten verarbeiten	12
2.7.3	Graphen und Screens: Daten anzeigen	13
2.7.4	Medien und Aktionen	14
2.8	Die Arbeitsschritte für Eilige	15
3	Zabbix 3: Was ist neu	17
3.1	Warten auf Zabbix 3.	17
3.2	Die größten Neuerungen in Zabbix 3	17
3.2.1	Webfrontend	17
3.2.2	Verschlüsselung	18
3.2.3	SMTP-Authentifizierung	19

3.2.4	Kontextbezogene Makros	20
3.2.5	Uhrzeitgesteuertes Abrufen von Messwerten	20
3.3	Kleine Neuerungen	21
3.3.1	VMware-Monitoring.	21
3.3.2	Housekeeper	21
3.3.3	Loglevel.	21
4	Den Zabbix-Server installieren	23
4.1	Die Zabbix-Installation planen	23
4.2	Benötigte Komponenten	24
4.3	Hardware dimensionieren	25
4.4	Hinweis zu fertigen Paketen der Distributionen	26
4.5	Zabbix mit fertigen Paketen von Zabbix LLC installieren (empfohlen)	27
4.5.1	MySQL installieren	28
4.5.2	DEB-Pakete für Debian und Ubuntu nutzen	29
4.5.3	RPM-Pakete für Red Hat und CentOS verwenden	30
4.5.4	Problemfall CentOS 7.1 und Zabbix 2.4.5	31
4.6	Zabbix aus den Quellen installieren (kompilieren)	32
4.6.1	Das Betriebssystem für das Übersetzen der Quellen vorbereiten	32
4.6.2	Zabbix-Server kompilieren und installieren.	36
4.6.3	Zabbix-Datenbank installieren	38
4.6.4	Zabbix-Server konfigurieren und starten.	39
4.6.5	Start-Stop-Skripte für den Zabbix-Server	40
4.7	Firewall-Regeln erweitern	43
4.7.1	SUSE Firewall2	43
4.7.2	Red Hat und CentOS	43
4.8	Das Zabbix-Webfrontend.	43
4.9	Webfrontend aus dem Zabbix-Paket-Repository installieren	44
4.9.1	Debian und Ubuntu.	44
4.9.2	CentOS und Red Hat	44
4.10	Webserver, PHP und Webfrontend manuell installieren	45
4.11	Webfrontend konfigurieren	46
4.12	Hinweise zur Sicherheit des Webfrontends	48
5	Den Zabbix-Agenten installieren	49
5.1	Hinweise zum Zabbix-Agenten.	49
5.2	Die Komponenten des Zabbix-Agenten	50

5.3	Zabbix-Agent mit den DEB- oder RPM-Paketen von Zabbix LLC installieren	50
5.4	Den Zabbix-Agenten aus den Quellen installieren.....	52
5.4.1	Zabbix-Agent kompilieren	52
5.4.2	Zabbix-Agent als Daemon einrichten.....	53
5.4.3	Start-Stop-Skripte für den Zabbix-Agenten	53
5.5	Den Zabbix-Agenten testen.....	55
5.6	Zabbix-Agent für Windows installieren.....	56
5.7	Zabbix-Agent konfigurieren	58
6	Schnellstart: In 5 Minuten zum ersten Alarm	61
6.1	Einleitung	61
6.2	Den ersten Host anlegen	61
6.3	Das erste Item anlegen.....	63
6.4	Die ersten Messwerte ablesen (Latest Data).....	64
6.5	Den ersten Trigger einrichten	66
6.6	Den ersten Alarm auslösen (Action und Mediatype)	68
6.7	Wie geht's weiter?	71
7	Daten sammeln: Hosts und Items konfigurieren	73
7.1	Hosts anlegen	73
7.1.1	Name	73
7.1.2	Groups, New Group	74
7.1.3	Interfaces	74
7.1.4	Monitored by proxy.....	75
7.1.5	Status.....	75
7.1.6	Templates.....	76
7.1.7	Clone, Full Clone.....	76
7.1.8	Verschlüsselung	77
7.2	Gruppen anlegen und Hosts zusammenfassen	77
7.3	So sammelt und speichert Zabbix die Daten	78
7.4	Der generelle Aufbau von Items.....	79
7.4.1	Itemname und die Datenquelle.....	79
7.4.2	Der Item-Key	81
7.5	Datentypen und Einheiten.....	82
7.5.1	Update interval.....	83
7.5.2	Historische Daten speichern.....	84
7.5.3	Differenzbildung und Werte-Mapping	85
7.5.4	Items kategorisieren, klonen und deaktivieren	86

8	Simple Checks: Daten ohne Agent sammeln	87
8.1	Was sind einfache Checks?	87
8.2	Beispiel: Webserver überprüfen.	88
8.3	ICMP echo request einrichten.	89
8.4	TCP-Portscans durchführen	90
9	Daten mit dem Zabbix-Agenten sammeln	93
9.1	Was ist der Zabbix-Agent?	93
9.1.1	Aufbau der Item-Keys	93
9.2	Beispiel 1: Neues Item anlegen	94
9.3	Beispiel 2: Items klonen	95
9.4	Welche Daten kann der Agent liefern?	97
9.4.1	Zabbix-Agent, Systeminformationen.	97
9.4.2	Netzwerk	99
9.4.3	Prozesse.	101
9.4.4	CPU-Auslastung	102
9.4.5	Speicher und Swap	103
9.4.6	Dateisysteme und Festplatten	104
9.4.7	Dateien	105
9.4.8	Sonstiges	106
9.5	Der Unterschied zwischen Zabbix-Agent und Zabbix-Agent (active)	107
10	Verschlüsselte Verbindungen	109
10.1	Zabbix 3 erforderlich	109
10.2	Pre-Shared Keys verwenden	109
10.2.1	Zertifikate verwenden	112
11	Daten visualisieren	113
11.1	Daten visualisieren mit Graphen.	113
11.1.1	Graphen bringen den Durchblick	113
11.1.2	Einfache Graphen	113
11.1.3	Definierte Graphen anlegen.	115
11.1.4	Die verschiedenen Graphentypen	120
11.2	Informationen zusammenstellen mit Screens.	122
11.2.1	Informationen bündeln mit Screens.	122
11.2.2	Inhalte in Screens einfügen	123
11.2.3	Dynamische Screens und Templates	125
11.2.4	Screens in Slideshows zeigen	126

11.3	Interaktive Karten	127
11.3.1	Interaktive Karten	127
11.3.2	Beispiel	127
12	Daten bewerten: Trigger einrichten	129
12.1	Das Trigger-Prinzip	129
12.2	Beispiel Prozessorauslastung überwachen	129
12.3	Einrichten eines Triggers	131
12.4	Beispiel: Kurvenausreißer erkennen	135
12.5	Triggerfunktionen im Detail	137
12.5.1	Differenzen	138
12.5.2	Durchschnitt	139
12.5.3	Erfolgreich abgerufene Daten	139
12.5.4	Gleich-ungleich-Prüfung	140
12.5.5	String-Vergleiche: Worte finden	140
12.5.6	Summen	141
12.5.7	Zeitstempel	141
13	Alarm auslösen: Medien und Aktionen einrichten	143
13.1	Kommunikation mit der Außenwelt: Medien einrichten	143
13.1.1	Zabbix kommuniziert mit der Außenwelt	143
13.1.2	E-Mail einrichten	143
13.1.3	SMS-Benachrichtigung einrichten	146
13.1.4	Eigene Medien hinzufügen	150
13.2	Alarm! Alarm! Aktionen einrichten	152
13.2.1	Alarmierung gleich Aktion	152
13.2.2	Eine neue Aktion anlegen	153
13.2.3	Eskalation	157
13.2.4	Makros für Aktionen	158
13.3	SMS über das Internet verschicken	161
13.3.1	Scriptpath setzen	161
13.3.2	Skripte als Medium einbinden	161
13.3.3	SMS per Sipgate HTTP-API senden	161
13.4	Telefonanrufe auslösen und SMS verschicken	164
13.4.1	SMS und Telefonanrufe per HTTP-API auslösen	164
13.4.2	Medien in Zabbix einrichten	165
13.5	SMS mit eigener Hardware verschicken	166
13.5.1	Gammu und Gammu-SMSD	166
13.5.2	Gammu installieren und Modem testen	166
13.5.3	SMS-Server einrichten	167

13.5.4	Gammu als Zabbix-Medium einrichten.....	168
13.5.5	SMS-Server monitoren	169
13.6	Benachrichtigungen auf dem Desktop erhalten.....	170
13.6.1	Warum Desktop-Nachrichten?	170
13.6.2	Das Benachrichtigungssystem Growl.....	170
13.6.3	Growl-Client konfigurieren.....	171
13.6.4	Growl als Medium im Zabbix-Server einrichten	171
13.7	Skripte: Kleine Helfer für den Notfall.....	174
13.7.1	Was sind Skripte?	174
13.7.2	Skripte anlegen	175
14	Benutzer und Berechtigungen verwalten	179
14.1	Wer darf was und bekommt wie und wann eine Nachricht?.....	179
14.2	Benutzer hinzufügen.....	179
14.3	Media, die Kommunikation mit dem Benutzer	181
14.4	Einstellungen vom Benutzer in seinem Profil.....	182
14.5	Gruppen anlegen und verwalten.....	183
15	Effizientes Arbeiten mit Templates	187
15.1	Effiziente Konfigurationen mit Templates.....	187
15.1.1	Die mitgelieferten Standardtemplates	187
15.2	Templates anlegen	188
15.2.1	Beispiel: Ping-Check-Template	189
15.3	Templates individualisieren mit Makros.....	191
15.3.1	Beispiel 1: Makros in Items	191
15.3.2	Beispiel 2: Makros in Triggern	192
15.3.3	Beispiel 3: Makros in Aktionen	192
15.4	Templates strukturieren	193
15.5	Hostspezifische Items automatisch erzeugen (Low Level Discovery)	194
15.5.1	Beispiel 1: Dateisysteme erkennen	197
15.5.2	Beispiel 2: Netzwerkgeräte automatisch hinzufügen	198
15.5.3	Eigene Discovery-Regeln erstellen	200
16	SNMP	201
16.1	Zabbix und SNMP.....	201
16.1.1	Simple Network Management Protocol (SNMP).....	201
16.1.2	OIDs identifizieren	208
16.1.3	Geräte per SNMP mit Zabbix überwachen	211

16.1.4	Dynamische Schlüssel-Wert-Paare	214
16.1.5	Low-Level-Discovery per SNMP	218
16.2	SNMP-Traps empfangen	223
16.2.1	snmptrapd und snmptt installieren	223
16.2.2	Zabbix-Server und Proxy konfigurieren	224
16.2.3	Items und Trigger einrichten	225
16.3	Beispiel: Dell iDrac per SNMP überwachen	227
16.3.1	Dell iDrac spricht SNMP	227
16.3.2	SNMP in iDrac aktivieren	227
16.3.3	Ein Template erstellen	230
16.4	SNMP-Agenten einrichten	234
16.4.1	Es geht auch ohne Zabbix-Agenten	234
16.4.2	SNMP-Agent einrichten	234
17	Hardware per IPMI überwachen	239
17.1	Hardware überwachen mit IPMI	239
17.2	IPMI auf der Hardware aktivieren	239
17.2.1	Beispiel 1: IPMI mit Dell-iDrac	239
17.2.2	Beispiel 2: Supermicro KVM	241
17.2.3	Beispiel 3: Intel RMM3	242
17.3	IPMI-Poller starten	243
17.4	IPMI-Item einrichten	243
17.4.1	Den Zugriff per IPMI testen	243
17.4.2	IPMI-Überwachung für einen Host hinzufügen	245
17.4.3	Ein IPMI-Item einrichten	246
17.5	Problemfall »Discrete Sensors«	247
17.5.1	Beispiel: Discrete Sensors in Dell-iDrac	248
17.5.2	Diskrete Sensoren per ipmitool auslesen	249
18	Geräte per SSH und Telnet überwachen	251
18.1	Warum SSH und Telnet?	251
18.2	Authentifizierung	252
18.2.1	Passwort	252
18.2.2	SSH-Keys	252
18.3	Item anlegen	253
18.3.1	Optionen für Telnet- und SSH-Items	254
18.4	Beispiel: Embedded-Linux-Systeme überwachen	255
18.5	Nützliche Kommandos	256

19	Webseiten auf Verfügbarkeit und Inhalte prüfen	259
19.1	Webszenario	259
19.2	Webszenarios einrichten	260
19.2.1	Einen Host auswählen	260
19.2.2	Test anlegen	261
19.2.3	Schritte (URLs) hinzufügen	263
19.2.4	POST-Daten verwenden	265
19.2.5	Ergebnisse der Webtests auswerten	267
19.2.6	Trigger für Webszenarios einrichten	268
19.3	Alternativen zu Webszenarios	269
19.3.1	Webtest mit Bash und Curl	269
20	Eigene Datenquellen: Zabbix erweitern	271
20.1	Den Zabbix-Agenten mit eigenen Datenquellen verbinden	271
20.2	User-Parameter einrichten	271
20.3	Regeln und Hinweise für User-Parameter	272
20.4	Berechtigungen	273
20.5	Wenn es klemmt	274
20.5.1	Checkliste	274
20.5.2	Items über den Agent testen	274
20.5.3	Item per zabbix_get testen	275
20.6	Beispiel: Fehlgeschlagene Login-Versuche überwachen	275
20.7	Den Zabbix-Server mit eigenen Datenquellen erweitern	277
20.8	Externe Skripte aktivieren	277
20.9	Ein Skript als Item verwenden	277
20.9.1	Der erste Test	277
20.9.2	Item anlegen	278
20.10	Hinweise und Rahmenbedingungen für externe Skripte	278
20.11	Beispiel: Ablauf von SSL-Zertifikaten prüfen	279
21	Daten aus beliebigen Quellen mit dem Zabbix-Sender schicken	281
21.1	So funktioniert der Zabbix-Sender	281
21.1.1	Was macht Zabbix-Sender?	281
21.1.2	Den Zabbix-Trapper konfigurieren	281
21.1.3	Item anlegen	282
21.1.4	Daten schicken	283
21.2	Beispiel: Linux-Sicherheitsupdates monitoren	284
21.2.1	Anzahl der verfügbaren Security-Updates für Linux monitoren	284

21.2.2	Red Hat und CentOS	284
21.2.3	Ubuntu und Debian	285
21.3	Beispiel: Windows-Updates monitoren	287
21.3.1	Verfügbare Updates per Skript abfragen.	287
21.3.2	Items und Trigger einrichten	288
21.3.3	Geplanten Task anlegen	289
22	Daten berechnen und zusammenfassen: Calculated Items	291
22.1	Daten berechnen und zusammenfassen	291
22.2	Calculated Items	292
22.2.1	Beispiel 1: IO-Operationen summieren.	292
22.2.2	Beispiel 2: Prozentwerte berechnen.	293
22.3	Aggregated-Items.	294
22.3.1	Beispiel: Aggregated Item einrichten.	295
23	Microsoft Windows überwachen	297
23.1	Besonderheiten unter Microsoft Windows.	297
23.2	Den Status von Windows-Diensten überwachen	297
23.3	Performance-Counter	298
23.3.1	Numerische Referenzen verwenden	299
23.4	Wichtige Leistungsindikatoren (Performance-Counter)	301
23.4.1	Datenträger	301
23.4.2	Prozessor	302
23.4.3	Netzwerk	302
23.4.4	Arbeitsspeicher.	303
23.4.5	Exchange	303
23.5	Netzwerkkarten identifizieren	304
23.6	Monitoring per Windows Management Instrumentation (WMI).	304
23.6.1	WMI-Objekte finden	305
23.6.2	WMI-Items anlegen	307
23.7	PowerShell als User-Parameter	308
24	VMware ESX überwachen	309
24.1	Der Zabbix VMware Collector	309
24.1.1	Technisches Konzept	309
24.1.2	VMwareCollector aktivieren	309
24.1.3	Items einrichten	310
24.1.4	Discovery-Regeln	314

24.2	Die Hardware von ESX-Servern überwachen	317
24.2.1	ESX CIM-API	317
24.2.2	CIM-API mit Zabbix abfragen	318
24.2.3	ESX-Hardwareüberwachung in Zabbix einrichten	322
25	Informationen aus Datenbanken auslesen	327
25.1	Datenbanken als Informationsquelle.	327
25.2	UnixODBC per Paketmanager installieren	328
25.3	UnixODBC und Zabbix-Server aus dem Quellcode installieren	328
25.3.1	UnixODBC installieren	328
25.3.2	Zabbix mit UnixODBC kompilieren	328
25.3.3	Datenbanktreiber installieren	329
25.4	ODBC-Verbindungen und DSN einrichten	330
25.4.1	UnixODBC testen	330
25.5	Items vom Typ Database-Monitor einrichten	331
25.5.1	Vorgaben für die SQL-Abfragen	332
26	Logfiles und Systemevents überwachen	333
26.1	Logfiles mit aktiven Checks überwachen	333
26.2	Den Agent vorbereiten	333
26.2.1	Hostname im Agenten konfigurieren	333
26.2.2	Zabbix-Serveradresse im Agenten konfigurieren	334
26.2.3	Netzwerk, Routing und NAT prüfen.	334
26.3	Leserechte für Logfiles einräumen.	335
26.4	Items zur Logfile-Überwachung einrichten	336
26.4.1	Rotierende Logfiles	338
26.4.2	Zeitstempel erhalten	340
26.5	Überwachen des Windows-Eventlogs	341
26.6	Trigger einrichten für die Logfile-Überwachung	343
27	Java JMX-Monitoring mit Zabbix	345
27.1	Was ist Java- und JMX-Monitoring?	345
27.2	Zabbix-Java-Gateway	345
27.2.1	Java-Gateway aktivieren	346
27.2.2	Java-Gateway als Datenlieferant für den Zabbix-Server . . .	346
27.3	JMX in einer Applikation aktivieren.	347
27.3.1	Beispiel Jedit	347
27.3.2	Beispiel Ubuntu und Tomcat 7	348
27.3.3	Passwortschutz	348

27.4	JMX-Items einrichten	350
27.5	Beispiele von JMX-Monitoring-Objekten	351
27.5.1	Heap space in Java?	351
27.5.2	Wichtige Parameter eines Java-Prozesses	351
28	Die Zabbix-API	353
28.1	Was ist die Zabbix-API?	353
28.2	Ein Perl-Beispiel.	354
28.3	PHP-Klassenbibliothek	356
28.3.1	Beispiel 1: Trigger abrufen	357
28.3.2	Beispiel 2: Einen neuen Host anlegen	358
28.4	Ein Python-Beispiel	359
29	Hosts hinzufügen mit Hostdiscovery und Autoregistration	361
29.1	Automatisches Hinzufügen von Hosts	361
29.2	Autoregistration	361
29.2.1	Trapper aktivieren	361
29.2.2	Zabbix-Agent vorbereiten	362
29.2.3	Regeln festlegen	364
29.3	Discovery	365
29.3.1	Netz scannen	366
29.3.2	Scanergebnisse verarbeiten	368
30	Distributed Monitoring mit Zabbix-Proxys	371
30.1	Was ist der Zabbix-Proxy?	371
30.2	Zabbix-Proxy installieren	373
30.3	Zabbix-Proxy aus den Quellen kompilieren	374
30.3.1	Die Datenbank anlegen	375
30.3.2	Ein Start-Stop-Skript anlegen	375
30.4	Die Proxy-Modus: Aktiv vs. Passiv	376
30.5	Proxys einrichten	377
30.5.1	Proxys benennen: Der Name ist alles!	377
30.5.2	Aktiv-Modus	379
30.5.3	Passiv-Modus	380
30.5.4	Proxy starten und testen	381
30.6	Hosts über einen Proxy überwachen	382
30.7	Proxys überwachen	382
30.8	Beispiel: Georedundantes Monitoring mit Proxys	384
30.9	Einstellungen zur Proxy-Performance	386

31	Zabbix-Internas überwachen	387
31.1	Einleitung	387
31.2	Auslastung der Zabbix-internen Prozesse monitoren	387
32	System und Datenbank tunen für große Setups	391
32.1	Hardware richtig dimensionieren	391
32.1.1	LogSlowQueries aktivieren	391
32.2	MySQL-Datenbank tunen	392
32.2.1	MySQL Bufferpool erhöhen	392
32.2.2	MySQL Innodb-Logfile vergrößern	392
32.2.3	Festplattenzugriffe reduzieren	393
32.2.4	MySQL Buffer-Pool-Instanzen erhöhen	393
32.2.5	Innodb-Plugin nutzen	393
32.2.6	Transaktionssicherheit reduzieren	394
32.2.7	Das Dateisystem tunen	394
32.2.8	IO-Schedulers wechseln	395
33	Backup des Zabbix-Servers	397
33.1	Backup des Zabbix-Servers erstellen	397
33.2	Die MySQL-Datenbank sichern	398
33.2.1	MySQL-Dump	398
33.2.2	Percona XtraBackup	399
33.3	Backup regelmäßig ausführen	401
33.4	Weiterführende Hinweise	401
34	Zabbix als virtuelle Appliance installieren	403
34.1	Einen passenden Virtualisierer auswählen	403
34.2	Zabbix-Appliance mit Virtual Box	404
34.3	Zabbix-Appliance mit VMware installieren	406
34.3.1	Appliance Headless starten	407
34.3.2	Appliance automatisch starten	408
34.4	Die Appliance benutzen und konfigurieren	409
34.4.1	An der Appliance anmelden	409
34.4.2	Hilfsprogramme	409
34.4.3	Eine feste IP-Adresse für die VM einrichten	410
	Index	413