Thorsten Kramm

Monitoring mit Zabbix

Das Praxishandbuch

Grundlagen, Skalierung,
Tuning und Erweiterungen

dpunkt.verlag

Thorsten Kramm beschäftigt sich seit 1999 mit IT-Systemen im Unternehmenseinsatz. In verschiedenen Firmen leitete er die IT-Abteilungen. Frustriert über die mangelnde Benutzerfreundlichkeit vieler Monitoring-Lösungen kam er 2006 zu Zabbix. Als Berater hat er in vielen Firmen Zabbix eingeführt und große Setups aufgebaut.

Thorsten Kramm beschäftigt sich nicht nur mit den technischen Details von IT-Systemen. Sein Augenmerk gilt auch den Soft Skills und der menschlichen Komponente. Ein System funktioniert nur so gut, wie die Menschen, die es betreiben. Thorsten Kramm gibt Trainings zu den Themen Monitoring, IT-Automatisierung und Kanban in der IT. Er lebt und arbeitet in Berlin. Mehr Informationen finden Sie auf seiner Webseite http://system42.io.

Thorsten Kramm

Monitoring mit Zabbix

Das Praxishandbuch

dpunkt.verlag

Thorsten Kramm

Lektorat: Christa Preisendanz
Copy-Editing: Annette Schwarz
Satz: III-satz, www.drei-satz.de
Herstellung: Nadine Thiele
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN:
Buch 978-3-86490-335-9
PDF 978-3-86491-897-1
epub 978-3-86491-898-8
mobi 978-3-86491-899-5

1 Auflage 2016

Wieblinger Weg 17
69123 Heidelberg

5 4 3 2 1 0

Inhaltsverzeichnis

1 Wie ist dieses Buch aufgebaut?

1.1 Über dieses Buch

Die Anzahl der IT-Systeme wächst stetig. Täglich kommen neue Server und Geräte in unsere Netzwerke. Doch die Anzahl der Personen, die diese Netzwerke betreuen, wächst nicht im gleichen Maße, wie neue Geräte hinzukommen. Effektives und effizientes Monitoring wird zu einem entscheidenden Faktor, damit Systeme und Netzwerke stabil bleiben. Zabbix bietet seit mehr als 10 Jahren eine Monitoring-Lösung für den Unternehmenseinsatz.

In diesem Buch erfahren Sie alles über Monitoring mit Zabbix. Es ist ein Buch für die Praxis. Neben den Grundlagen werden auch die Spezialthemen wie Skalierung, Tuning und Erweiterung von Zabbix erläutert. Der Autor gibt zahlreiche konkrete Beispiele aus seinem beruflichen Einsatz von Zabbix. Das Buch richtet sich gleichermaßen an Anfänger und Profis. Wenn Sie noch nicht mit Zabbix überwachen, lernen Sie Schritt für Schritt die Einrichtung eines professionellen IT-Monitorings. Wenn Sie bereits Zabbix nutzen, gibt Ihnen das Buch viele Tipps aus der Praxis und sofort nutzbare Beispiele, wie Sie konkrete Anforderungen mit Zabbix umsetzen.

1.2 Der große Zabbix-Baukasten

Zabbix ist ein großer Baukasten, mit dem Sie ein hoch professionelles Monitoring sowohl für einfache als auch für sehr komplexe EDV-Systeme aufbauen können. Für sehr viele Bedürfnisse und Anwendungsfälle verfügt Zabbix über fertige Lösungen in Form von Modulen, Checks, Programmen oder Konfigurationsbeispielen.

Für einige andere Anwendungsfälle gibt es keine Lösung »von der Stange«. Doch dafür bietet Ihnen Zabbix zahlreiche Schnittstellen, Erweiterungsmöglichkeiten und eine mächtige API. Es gibt fast nichts, was Sie nicht mit Zabbix überwachen können.

Sie müssen nur wissen, wie Sie den Inhalt des Baukastens richtig einsetzen.

Nutzen Sie dieses Buch ebenfalls wie einen Baukasten. Vielleicht ist nicht die 100% passende Lösung für Ihr Bedürfnis beschrieben. Doch die zahlreichen Beispiele werden Ihnen sicher helfen, Ihre passende Lösung zu erstellen.

1.3 Die Reihenfolge der Kapitel

Die Reihenfolge der Kapitel ist so angeordnet, dass Sie sich zuerst mit den wichtigsten Aspekten und der Installation von Zabbix auseinandersetzen. Sobald Sie ein erstes Verständnis haben, können oder sollten Sie zwischen den Kapiteln hin und her wechseln, je nachdem welche Aspekte von Monitoring Sie interessieren. Wie fast jedes Buch über eine Software, so ist auch dieses nicht dafür gedacht, dass Sie es von vorne nach hinten komplett durchlesen. Wenn Sie eine Monitoring-Software wie Zabbix installieren und einrichten, müssen Sie sich zwangsläufig mit verschiedenen Aspekten gleichzeitig beschäftigen.

1.4 Schnelleinstieg

Wenn Sie schnell in Zabbix einsteigen wollen, sollten Sie sich zuerst mit der Terminologie von Zabbix und der Funktionsweise von Zabbix-Server und -Agenten vertraut machen. Besonders das Zusammenspiel von Daten sammeln (Item) und Daten bewerten (Trigger) muss klar sein.

Alle Kapitel enthalten viele Beispiele. Wenn Sie schnell und praxisorientiert in Zabbix einsteigen möchten, stürzen Sie sich auf die Beispiele. Diese sind mit einer Glühbirne markiert, so dass Sie schnell von einem Beispiel zum nächsten springen können.

So steigen Sie noch schneller in Zabbix ein

Wenn Sie sich dieses Buch zugelegt haben, um zu klären, ob Zabbix die geeignete Monitoring-Lösung für Sie ist, dann testen Sie die Software mit der virtuellen Appliance. Die Kapitel, die sich mit der Installation von Server und Agent befassen, sollten Sie erst einmal überspringen. Beschäftigen Sie sich erst einmal mit den Funktionen von Zabbix.

Wenn Sie Zabbix sofort in Aktion sehen möchten, konzentrieren Sie sich nach einer kurzen Lektüre der Terminologie auf die Beispiele. Sie werden Schritt für Schritt durch den Aufbau eines professionellen Monitorings geführt. Detailfragen, die sich ggf. beim Durcharbeiten der Übungen ergeben, klären Sie dann durch gezieltes Nachlesen in den entsprechenden Kapiteln.

1.5 Formalien

1.5.1 Typografie

In diesem Buch werden die folgenden typografischen Stile verwendet:

- `Monospace-Schrift` wird für Dateinamen, Variablen und Konfigurationsoptionen verwendet, zum Beispiel `Server = localhost`.
- Links, Schaltflächen und Menüeinträge, die sich auf die Weboberfläche beziehen, werden *kursiv* gedruckt. Einträge in verschachtelte Menüs werden mit einem Pipe-Zeichen abgetrennt, zum Beispiel *Configuration|Hosts*.
- Programmcode, Terminalausgaben oder größere Blöcke einer Konfigurationsdatei werden in einem grau hinterlegten Block in Monospace-Schrift gedruckt, zum Beispiel

```
chown zabbix /var/run/zabbix
chown zabbix /var/log/zabbix
```

- Lange Terminaleingaben werden oft über mehrere Zeilen dargestellt, obwohl es sich um nur eine Eingabe handelt. Wie auch in der Bash-Eingabe werden Zeilenumbrüche mit einem Backslash vorgenommen. Am Ende der Zeile erfolgt mit der Enter-Taste also nicht das Auslösen der Eingabe, sondern das Kommando wird in einer weiteren Zeile fortgeführt. Beispiel:

```
echo "Ein sehr\
 langes Kommando"
```

- Es handelt sich um nur ein Kommando, welches Sie auch wie folgt eingeben können:

```
 echo "Ein sehr langes Kommando"
```

1.5.2 Englische Begriffe und Anglizismen

Obwohl eine deutschsprachige Variante der Zabbix-Weboberfläche existiert, beziehen sich alle Anleitungen und Screenshots immer auf die englischsprachige Version von Zabbix. An dieser Stelle sei Ihnen auch empfohlen, Zabbix auf Englisch zu verwenden. Dies erleichtert Ihnen später die Suche nach weiteren Informationen im Internet oder dem Zabbix-Support-Forum. Dort werden so gut wie alle Fragen nur auf Englisch geklärt. In Konfigurationsdateien oder in Software von Drittanbietern werden die Begriffe der deutschsprachigen Zabbix-Version ebenfalls nicht verwendet. Um Missverständnisse zu vermeiden und eine einheitliche Terminologie zu verwenden, werden englischsprachige Fachbegriffe nicht ins Deutsche übersetzt. Englisch ist nun einmal die Sprache der Computer- und Internetwelt.

2 Der Einstieg: Was ist Monitoring?

2.1 Warum Monitoring?

Die perfekten IT-Systeme, die zuverlässig und ohne Fehler ihre Dienste tun, gibt es nicht. Ein funktionierendes IT-System ist kein Zustand, sondern ein Prozess, der von Menschen (Administratoren) permanent begleitet werden muss.

Zahlreiche Ereignisse sorgen immer wieder dafür, dass ein IT-System seinen Dienst versagt. Verschleißteile wie Festplatten, fehlerhafte Bedienung, bösartige Angriffe oder das Versäumen von regelmäßigen Pflegeaufgaben sind nur einige Gründe, warum Fehler und Ausfälle auftreten. Und spätestens dann, wenn Ihr Kunde schneller als Sie bemerkt, dass ein System nicht mehr funktioniert, brauchen Sie ein Monitoring.

Die folgenden Aufgaben sollte ein Monitoring-System für Sie erledigen:

- den Status aller Komponenten erfassen
- Daten aufbereiten, sortieren und bewerten
- übersichtliche Zusammenfassungen präsentieren
- Abweichungen vom Normalzustand erkennen
- Alarm auslösen
- Zustände und Veränderungen protokollieren
- die Einhaltung von Prozessen oder eine Abweichung überwachen und protokollieren

2.2 Monitoring ist mehr als ein Alarm im Fehlerfall

Je größer ein IT-System ist, desto schwieriger wird es, den Überblick über den Zustand des gesamten Systems und aller Einzelkomponenten zu behalten. Entsprechend muss das Monitoring-System komplexere Aufgaben als die zuvor beschriebenen erfüllen.

Einen Alarm zu senden, wenn ein Fehler auftritt, ist eine wichtige, aber bei weitem nicht die einzige Aufgabe eines Monitoring-Systems. Monitoring heißt, viele Daten zu sammeln und automatisiert die richtigen Schlüsse zu ziehen. Fällt eine Komponente aus, ist es nicht schwer, daraus zu schlussfolgern, dass ein Pro-

blem vorliegt! Es sollte sich jemand darum kümmern! Ab einer gewissen Anzahl von Systemen gehören Meldungen des Monitoring-Systems zum Alltag. Das Monitoring-System sollte harmlose von schweren Fehlern unterscheiden und je nach Schweregrad unterschiedliche Medien zur Benachrichtigung nutzen können.

Neben der Erkennung von Fehlern sollte ein Monitoring-System Schlüsse oder konkrete Aussagen zur Zuverlässigkeit von Systemen und Komponenten ermöglichen. Dazu ist das Speichern historischer Daten notwendig. Dabei sollte das System eine Schnittstelle und ein sogenanntes User-Interface zur Verfügung stellen, um die gespeicherten Daten schnell und bequem auswerten zu können.

IT-Verantwortliche und Systemadministratoren möchten mithilfe eines Monitoring-Systems auch vorbeugen, dass eine Komponente oder ein Dienst ausfällt. Dafür ist in der Regel die Auswertung vieler Daten notwendig. Die Performance von Komponenten und Diensten und die Auslastung der Infrastruktur muss ebenfalls permanent gemessen und grafisch dargestellt werden. Ein einfaches Beispiel ist der freie Speicher auf einer Festplatte. Wenn das Monitoring-System einen Anstieg des verbrauchten Speichers von X GB pro Tag berechnet, ist es nicht schwer, vorherzusagen, wann die Fesplatte voll sein wird.

Wenn nun ein Dienst auf fünf Server mit insgesamt 20 Festplatten zugreift, wollen Sie an einem Sonntagabend nicht in der Wochenendruhe gestört werden, nur weil eine Festplatte voll ist. Nun hat das Monitoring-System eine komplexe Aufgabe zu bewerkstelligen und muss die Daten von 20 Festplatten, fünf Servern, einem Dienst, den Wochentag und die Uhrzeit zu einer »Entscheidung« verarbeiten: Geht ein Alarm raus, oder nicht?

Performancedaten werden aber nicht zur Prognose des nächsten Ausfalls gebraucht. Ein Monitoring-System sammelt viele Daten auf Verdacht, ohne dass diese automatisiert ausgewertet werden. Diese Daten brauchen Sie, um nicht vorhersehbare Störfalle zu erklären. Ein einfaches Beispiel sind die Besucherzahlen auf einer Webseite. Wenn nun der Webserver »abstürzt«, können Sie sich die Besucherzahlen als Graphen anschauen. Wenn dem Ausfall des Webservers ein ungewohnt hoher Anstieg der Besucherzahlen vorausging, wäre dies eine plausible Erklärung für den Ausfall. Die hohen Besucherzahlen könnten eine so hohe Last verursacht haben, dass der Server abgestürzt ist.

Auch für die Planung und den Ausbau der Hardware ist es wichtig zu wissen, wie stark die Hardware in der Vergangenheit ausgelastet war.

Kunden wünschen oft einen Verfügbarkeitsreport. Oder vielleicht berechnen Sie Ressourcen je nach Verbrauch an Kunden. Auch das ist eine Aufgabe des Monitoring-Systems.

Die Anforderungen an ein IT-Monitoring-System können zusammenfassend in fünf Kategorien eingeordnet werden

1. **Zustand des Systems beobachten**
   - »End-to-End«-Monitoring, bei dem der ausgelieferte Dienst so nah wie möglich am Endbenutzer auf Funktionsfähigkeit geprüft wird

- Statuserfassung aller Dienste, Software und Hardware
- Langzeitspeicherung von Informationen über die Verfügbarkeit von Diensten und Komponenten

2. **Alarmierung**
   - das manuelle Eingreifen ins System verlangen
   - einen Mitarbeiter so gut wie möglich über die Ursache eines Fehlers informieren.
   - Reaktionszeiten und die Fehlerbehebung dokumentieren
3. **Diagnose**
   - genügend Informationen sammeln, um eine detaillierte Ursachenanalyse zu ermöglichen
   - Informationssammlung für Entscheidungen
4. **Qualitätsmessung**
   - Datensammlung über die Leistungsfähigkeit und den Durchsatz des Systems und Teilkomponenten
   - Erfassung von vereinbarten Grenzwerten und deren Einhaltung
   - Identifikation von Engpässen, Überlastungen und Implementierungsfehlern
5. **Konfiguration**
   - Überwachung von standardisierten Konfigurationen
   - Warnen bei Abweichungen von einem standardisierten Vorgehen

Besonders der letzte Punkt, die Überwachung von standardisierteren Konfigurationen, wird oft vernachlässigt. Eine Konfiguration gemäß des vereinbarten Standards ist aber für ein stabiles System essenziell. Oder anders formuliert: Die Ursache für Probleme sind häufig Änderungen an der Umgebung! Woher kommt der in IT-Kreisen oft zitierte Spruch »Never touch a running system«? Der Grund ist, dass einmal gut laufende Systeme oft jahrelang ohne Probleme weiterlaufen. Korrekt konfigurierte Systeme minimieren das Risiko von Ausfällen.

Ihr Monitoring-System sollte in der Lage sein, die folgenden Aspekte der Systemkonfiguration zu dokumentieren und bei Abweichungen zu alarmieren:

- Wann wurden Änderungen an der Konfiguration vorgenommen? Wenn beispielsweise die Änderung an einer Apache-Konfigurationsdatei und der spätere Ausfall des Webservers in ein gemeinsames kleines Zeitfenster passen, liegt die Vermutung nahe, dass die Änderung für den Ausfall verantwortlich ist.
- Wird die richtige (vereinbarte) Software eingesetzt? Manche Mitarbeiter experimentieren auch mit kritischen Systemen. Monitoren Sie nicht nur, dass irgendein Mailserver läuft. Monitoren Sie, dass der in Ihrer Firma vereinbarte Standardmailserver läuft.

- Wann wurden Updates und Patches eingespielt? Das Monitoring sollte also stets dokumentieren, welche Version und welches Release von einer Software im Einsatz war.
- Gibt es Sicherheitsupdates für Software und das Betriebssystem und wann wurden diese Updates eingespielt?

2.3 Zabbix, die Datenkrake

Die oben genannten Anforderungen an ein Monitoring-System klingen kompliziert? Mit der richtigen Software ist es das aber nicht. Zabbix ist eine Monitoring-Software, die diese Ziele erfüllt. Nun könnten Sie einwenden, dass man für die genannten Aufgaben keine spezielle Software braucht. Ein paar Skripte oder ein Internetdienst wie pingdom.com tun es doch auch. Wenn Sie einen einzelnen Webserver überwachen möchten, dann kommen Sie mit einem Skript sicher zu akzeptablen Lösungen. Wenn es aber um ein Netzwerk geht, reichen Skripte oder Internetdienste nicht aus. Eine Software wie Zabbix kann mehr:

- Es wird nicht nur das Endprodukt, zum Beispiel die Verfügbarkeit einer Webseite, überwacht, sondern alle Teilkomponenten, wie Hard- und Software, Betriebssysteme und Netzwerkinfrastruktur.
- Durch das Überwachen von vielen Teilkomponenten wie zum Beispiel des freien Festplattenplatzes kann Fehlern vorgebeugt werden.
- Routineaufgaben werden nicht mehr vergessen.
- Ressourcenengpässe werden frühzeitig erkannt.
- Ein einheitliches Setup wird gewährleistet. Das Monitoring erkennt sofort, wenn ein Kollege sich bei der Installation eines neuen Servers nicht an die vereinbarten Konventionen gehalten hat. Das Monitoring liefert eine To-do-Liste, *was* zu ändern ist.
- Die Alarmierung erfolgt zielgerichtet. Nur die relevanten Daten werden verschickt. Der Admin weiß sofort, wo er mit der Fehlerbehebung beginnen muss. (Ein Router fällt aus. Sie wollen in der Regel dann nicht noch unzählige SMS bekommen, die Sie darüber informieren, welche Webseiten nun auch offline sind, weil der entsprechende Webserver hinter dem ausgefallenen Router hängt.)

Die Hauptfunktionen von Zabbix decken alle Anforderungen an ein Monitoring-System ab:

- Daten sammeln inklusive automatischer Erkennung von Komponenten und Webseitenmonitoring
- effiziente Datenspeicherung

- effektiver Zugriff auf Daten
- Alarmierung per E-Mail, SMS, Chat oder beliebige Programme
- Visualisierung der Daten per Dashboard, Graphen, Karten und Übersichten

2.4 Was leistet Zabbix?

Die Firma Zabbix LLC umschreibt ihr Produkt so: »Zabbix is an enterprise-class open source distributed monitoring solution.« Konkret bedeutet diese Aussage Folgendes:

- **Zabbix ist Enterprise!**
  Die Software ist für den professionellen Einsatz in geschäftskritischen Bereichen gemacht. Die Funktionsvielfalt deckt alles ab, was professionelle Administratoren und ganze Teams brauchen. Besonderen Wert legen die Entwickler von Zabbix auf die Unterstützung von fast allen Betriebssystemen, einen robusten Softwarekern und eine verständliche Bedienung mit einem modernen grafischen Interface.
- **Zabbix ist Open Source!**
  Die Software ist komplett unter der GPL veröffentlicht. Sie können Zabbix kostenlos downloaden und beliebig oft installieren. Egal, wie viele Hosts Sie überwachen. Es werden keine Lizenzgebühren fällig. Und wenn Sie möchten, können Sie sich den Quellcode von Zabbix anschauen und verändern.
- **Zabbix ist für große Umgebungen!**
  Wenn Sie nur einen einzelnen Server überwachen möchten, dann schießen Sie mit Zabbix sprichwörtlich mit Kanonen auf Spatzen. Zabbix ist für den Einsatz in Netzwerken konzipiert. Das Überwachen von mehreren Tausend Hosts stellt kein Problem dar. Durch Techniken wie Proxys und Nodes können große Netzwerke und an verschiedenen Standorten überwacht werden.

Eine detaillierte Liste mit allen Funktionen von Zabbix finden Sie auf der Zabbix-Webseite[1].

Zabbix wird seit über 10 Jahren von der Firma Zabbix LLC in Riga, Litauen entwickelt. 2004 erschien die erste stabile Version von Zabbix. Die Entwicklung wird sehr aktiv vorangetrieben. Bugs werden schnell behoben, und ca. alle drei Monate werden Updates veröffentlicht.

Zabbix LLC bietet kommerziellen Support für Ihr Produkt. Es gibt ein weltweites Netz von lizenzierten Partnern, die Support-, Trainings- und Consultingleistungen rund um Zabbix anbieten.

Unter http://www.zabbix.com erfahren Sie mehr.

1. *http://www.zabbix.com/features.php*

2.5 Die Grenzen und Schwächen von Zabbix

Auch wenn Zabbix für große Netzwerke konzipiert ist, skaliert das System nicht ins Unendliche. Im Zabbix-Forum werden regelmäßig Fragen zur maximalen Anzahl von überwachten Hosts gestellt. Mitglieder berichten häufig davon, dass die Überwachung von 8.000 Hosts problemlos möglich ist. Im Zabbix-Blog[2] finden Sie einen Bericht über ein Zabbix-Setup mit fast 700.000 Messpunkten. Da Zabbix auf eine Datenbank angewiesen ist, ist der Skalierung eine Grenze gesetzt. Wenn die Datenbank die eintreffenden Daten nicht mehr speichern kann, weil die Hardware an der Grenze der Leistungsfähigkeit ist, dann erreicht auch Zabbix seine Grenzen. Doch mit jeder neuen Version von Zabbix verbessert sich die Performance. Cache-Mechanismen wurden implementiert, um die Last der Datenbank zu reduzieren.

Das Erstellen von Berichten wird von vielen Benutzern als verbesserungswürdig bezeichnet. Die Konfiguration der Berichte sei umständlich und die Berichte könnten etwas besser aussehen.

2.6 Bestandteile und Funktionen von Zabbix

Die Funktionen von Zabbix teilen sich auf folgende wesentliche Bereiche auf:

- Daten sammeln
- Daten verarbeiten
- reagieren und Aktionen auslösen
- Konfiguration vornehmen
- Daten anzeigen

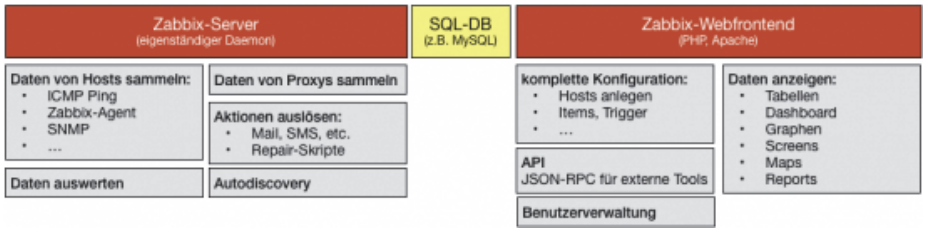

Abb. 2–1 *Die Funktionen und Komponenten von Zabbix*

2. *http://blog.zabbix.com/scalable-zabbix-lessons-on-hitting-9400-nvps/2615/*

2.7 Die Basisterminologie

2.7.1 Host und Item: Daten sammeln

Das Sammeln von Daten ist immer der erste Schritt beim Einrichten eines Monitorings.

In Zabbix wird das Sammeln der Daten durch die sogenannten Items gesteuert. Ein Item bezeichnet eine Messgröße (Was soll gemessen werden?). Der sogenannte Item-Value ist der Messwert.

Items können Informationen von beliebigen Formaten (Typen) enthalten, zum Beispiel den Festplattenverbrauch in Prozent, die Systemuhrzeit als Datum (Unix-Timestamp), einen Log-Eintrag als Text oder den CPU-Verbrauch als Fließkommazahl.

Alle Itemwerte werden als chronologische Liste mit Datum und Uhrzeit der Messung in der Zabbix-Datenbank gespeichert. Hierbei verwendet Zabbix keine eigene interne Datenbank, sondern eine externe SQL-Datenbank, wie zum Beispiel MySQL.

Aus verschiedenen Quellen sammelt der Zabbix-Server die Daten. Als Datenquellen stehen zur Verfügung:

- Zabbix-Agent: Dieser ist auf dem zu überwachenden Host installiert und greift direkt auf die Kennwerte des Betriebssystems zu.
- Simple Check: Tests, die der Zabbix-Server eigenständig durchführen kann, zum Beispiel Ping-Checks oder Portscans
- SNMP: Der Zabbix-Server fungiert als lesender SNMP-Manager, der Daten von einem SNMP-Agenten auf dem überwachten Host oder Gerät abfragt.
- Zabbix-Aggregate: Daten aus mehreren Quellen werden zusammengefügt, zum Beispiel addiert, und dann als neues Item gespeichert.
- IPMI-Agent, der auf dem zu überwachenden Host oder Gerät installiert ist. Der IPMI-Daemon wird in der Regel vom Hardwarehersteller zusammen mit den Remote-Management-Konsolen bereitgestellt, zum Beispiel Dell iDRAC oder HP iLO.
- Database Monitor: Der Zabbix-Server fragt Datenbanken ab und speichert die Resultate als Item-Values.
- External Check: Skripte, die auf dem Zabbix-Server ausgeführt werden und deren Rückgabewerte als Item-Values gespeichert werden
- Zabbix-Trapper: Daten, die per Zabbix-Sender vom Client an den Server geschickt werden
- Zabbix-Internal: Auswertungen der internen Zabbix-Server-Daten

- SSH oder Telnet: Kommandos werden über den integrierten SSH- oder Telnet-Client vom Zabbix-Server auf entfernten Hosts ausgeführt. Die Ausgaben der Kommandos werden als Item-Values gespeichert

Items sind immer an Hosts gebunden. Der Zabbix-Server bekommt immer den Auftrag, Wert X auf Host Y zu messen. Alles, was eine IP-Adresse oder einen DNS-Namen hat, kann in Zabbix ein Host sein. Hosts und Items bilden eine klassische Eins-zu-N-Beziehung. Ein Host kann beliebig viele Items haben. Ein Item kann aber nur einem Host zugeordnet werden.

Wenn Sie nach der Lektüre dieser Einführung sofort mit der Konfiguration des Monitorings beginnen wollen, merken Sie sich:

- Schritt 1: Anlegen eines Hosts. Für wen oder was sollen Daten gesammelt werden?
- Schritt 2: Anlegen der Items für die Hosts. Welche Daten werden gesammelt?

Base Checks (1 Items)			
Ping check	05 Sep 2011 18:45:48	1	-
Linux Base Information (15 Items)			
CPU IDLE AVG5	05 Sep 2011 18:45:58	99.91	-0.004179
CPU IOwait AVG5	05 Sep 2011 18:45:59	0.002503	+0.000834
CPU load AVG5	05 Sep 2011 18:45:57	0	-
CPU Softirq AVG5	05 Sep 2011 18:46:00	0	-
CPU User AVG5	05 Sep 2011 18:46:01	0.014181	+0.000836
Free disk on / (percent)	05 Sep 2011 18:46:07	83.59	-
Free disk on /var (percent)	05 Sep 2011 18:46:08	87.79	-0.001715
Net Usage eth0 IN	05 Sep 2011 18:45:54	3.13 Kb	+94.89 b
Net Usage eth0 OUT	05 Sep 2011 18:45:55	386.44 b	+15.31 b
Number of processes	05 Sep 2011 18:45:56	106	-
RAM available	05 Sep 2011 18:46:09	3.75 Gb	+356.35 Kb
RAM Free	05 Sep 2011 18:46:10	1.6 Gb	-
RAM Free Percent	05 Sep 2011 18:46:11	38.35	-
RAM Total	05 Sep 2011 18:46:12	4.16 Gb	-
Used Swap Space	05 Sep 2011 18:46:03	0 b	-

Abb. 2–2 *Tabellarische Darstellung der Messpunkte (Items) und der letzten Messwerte (Item-Values)*

2.7.2 Trigger: Daten verarbeiten

Sobald der Zabbix-Server Daten gesammelt hat, stehen die Item-Values für die Auswertung zur Verfügung. Die Weiterverarbeitung der Daten erledigen sogenannte Trigger.

Die Werte der Items werden zum Beispiel mit einem Schwellenwert verglichen. Trigger sind eine der wichtigsten Kernfunktionen von Zabbix, denn nur sie können eine Aktion auslösen.

Zabbix bietet viele Funktionen zum Auswerten der Messergebnisse. Darunter das Anwenden von regulären Ausdrücken und mathematischen Funktionen. Mehrere Funktionen können mit den logischen Operatoren AND und OR verbunden werden.

Nachdem der Messwert eines Triggers ausgewertet wurde, nimmt der Trigger den Status wahr (TRUE) oder falsch (FALSE) an. Der Status TRUE bedeutet, dass ein Problem vorliegt. Der Status des Triggers wird in der Datenbank gespeichert und wartet dort auf eine weitere Verarbeitung. Die Zabbix-Trigger werden ähnlich wie Datenbank-Trigger in dem Moment ausgeführt, in dem ein Messwert neu im Zabbix-Server eintrifft.

Verwechseln Sie Trigger nicht mit Alarmierung. Der Trigger ist der Auslöser für zahlreiche nachfolgende Aktionen. Der Trigger bestimmt dabei nicht, welche Aktion ausgeführt wird. Die Aktionen haben eigene Bedingungen, die festlegen, ob diese ausgeführt werden oder nicht. Suchen Sie also in der Konfiguration der Trigger nicht nach Menüs oder Einstellmöglichkeiten, über die Sie auswählen, welcher Alarm ausgelöst werden soll. Wann welcher Alarm ausgelöst wird, stellt man in den Aktionen ein.

2.7.3 Graphen und Screens: Daten anzeigen

Eine große Stärke von Zabbix liegt in den vielfachen Möglichkeiten, Daten anzuzeigen. Das übersichtliche Anzeigen von Daten war von Anfang an ein wichtiges Ziel der Zabbix-Entwickler. Dementsprechend ist das Visualisieren von Daten direkt im Kern von Zabbix integriert. Sie brauchen keine zusätzlichen Tools oder Add-ons.

Über das Hauptmenü *Monitoring|Latest Data* erhalten Sie immer einen Überblick über alle Daten, die Zabbix sammelt. Host-Gruppen und Itemgruppen (Applikationen) erleichtern dabei das Auffinden von Hosts und Messpunkten. Über eine Freitextsuche können Sie sofort zu einzelnen Hosts springen.

Von jedem Messwert können Sie sich die Daten aus der Vergangenheit als Graph oder Tabelle anzeigen lassen. Neben diesen sogenannten »spontanen Graphen« können Sie verschiedene Graphen mit mehreren Werten auf einer gemeinsamen Zeitachse konfigurieren.

Und damit Sie bei den vielen und manchmal sehr großen Zahlen nicht den Überblick verlieren, rechnet Zabbix alle Zahlen mit Einheiten in verständliche Werte um. Sie sehen nicht, dass noch 5985456712 Bytes auf Ihrer Festplatte frei sind. Zabbix zeigt diesen Wert automatisch als 5,57 GB an.

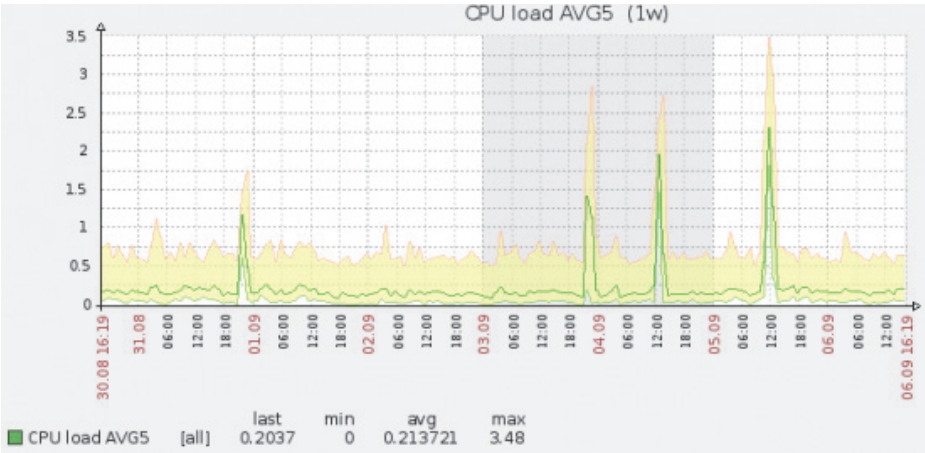

Abb. 2–3 *Beispiel für einen »spontanen Graphen«*

2.7.4 Medien und Aktionen

Auch wenn die meisten Benutzer Zabbix zum Alarmieren im Störfall einsetzen, findet man nirgendwo in den Menüs das Wort »Alarm«.

In Zabbix gibt es stattdessen Aktionen. Ein Alarm kann eine von vielen Aktionen sein. Streng genommen ist ein Alarm die Kombination aus einer Aktion (schicke eine Nachricht) und einem Medium (per E-Mail).

Aktionen werten den Zustand der Trigger aus. Nimmt der Trigger den Zustand TRUE an, das heißt, wenn ein Problem vorliegt, dann wird die Aktion ausgelöst. Es gibt zwei Aktionsformen:

- Nachricht über eines der eingerichteten Medien schicken oder
- Skript auf dem betroffenen Host oder dem Zabbix-Server ausführen. Zabbix versucht, das Problem zu lösen, ohne den Benutzer zu alarmieren.

Die Aktionen können selbstverständlich kombiniert und zu Aktionsketten zusammengefügt werden.

Wenn Sie also einen Alarm einrichten wollen, richten Sie zuerst ein Medium ein, zum Beispiel »E-Mail«. Solange keine Medien eingerichtet sind, können Sie keine Aktion vom Typ »Sende Nachricht« anlegen.

Das Einrichten der Aktion ist also der letzte Schritt zur Alarmierung.