Lennart Betz · Thomas Widhalm

Icinga 2

Ein praktischer Einstieg ins Monitoring

iX EDITION

dpunkt.verlag

Lennart Betz arbeitet als Consultant und Trainer bei der Nürnberger NETWAYS GmbH. Seine Hauptarbeitsgebiete sind Planung, Aufbau und Betreuung von Monitoringlösungen, Konfigurationsmanagement und weitere Automatisierungsthemen. Schon früh während seines Mathematikstudiums beschäftigte er sich mit Freier Software und verfolgt dies auch seit dem Abschluss in seiner beruflichen Tätigkeit konsequent weiter.

Thomas Widhalm hilft als Lead Support Engineer Kunden der Netways GmbH beim Beheben von Problemen mit Icinga-Installation. Außerdem unterstützt er als Consultant Kunden bei der Planung, Umsetzung und weiteren Betreuung von Projekten im Bereich Monitoring und Logmanagement. Als Trainer zeichnet er sich für die Schulungen im Bereich Logmanagement verantwortlich. Im Icinga-Team arbeitet er an der Online-Dokumentation mit. Er ist überzeugt, dass Freie Software proprietärer Software überlegen ist und ihre Konzepte auch außerhalb der IT mehr Anwendung finden sollten.

Lennart Betz · Thomas Widhalm

Icinga 2

Ein praktischer Einstieg ins Monitoring

2., aktualisierte und erweiterte Auflage

dpunkt.verlag

Lennart Betz
lennart.betz@icinga-book.net

Thomas Widhalm
thomas.widhalm@icinga-book.net

feedback@icinga-book.net

Lektorat: Dr. Michael Barabas
Copy-Editing: Petra Kienle, Fürstenfeldbruck
Satz: Lennart Betz, Thomas Widhalm
Herstellung: Stefanie Weidner
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:
Print 978-3-86490-556-8
PDF 978-3-96088-425-5
ePub 978-3-96088-426-2
mobi 978-3-96088-427-9

2. Auflage 2018

Wieblinger Weg 17
69123 Heidelberg

5 4 3 2 1 0

This Book is the Property of the Half-Blood Prince.

Vorwort

Als wir Icinga im April 2009 zum Leben erweckten, konnten wir nur erahnen, wohin uns das Projekt führen würde. Natürlich waren wir von dem Potenzial des Projekts und der beteiligten Menschen überzeugt. Die Frage war jedoch, ob wir auch die Open-Source-Community von Icinga überzeugen können.

Das Feedback war schlichtweg überwältigend. Bereits nach den ersten Versionen erreichten uns unglaublich viel positives Feedback und viele User Stories über den erfolgreichen Einsatz von Icinga. Ausschlaggebend für den Einsatz von Icinga waren in der Praxis meist nicht das ein oder andere neue Feature, sondern das Vertrauen unserer Anwender. Vertrauen der Anwender in das Projekt, die Menschen dahinter und die Überzeugung, eine zukunftssichere Technologie einzusetzen.

Dieses Vertrauen war und ist seitdem unser Antrieb und auch die Hauptmotivation hinter Icinga 2. Zu behaupten, die Neuentwicklung von Icinga war rein altruistischi, wäre sicherlich etwas übertrieben, aber gegenüber unseren bestehenden Anwendern haben wir immer die größte Verantwortung. Icinga 2 und Icinga Web 2 sind die Folge unzähliger Entwicklungsjahre, aber auch zweier Grundfesten unserer Arbeit: das Bestreben, die Stärken von Icinga beizubehalten und gleichzeitig auch die aktuellen Bedürfnisse hinsichtlich Performance und Skalierbarkeit zu befriedigen.

Das Ergebnis dieser Arbeit wird in dem Buch, das Sie in Ihren Händen halten, vortrefflich beschrieben und erläutert. Dabei ist es weit mehr als eine Erweiterung der bestehenden Dokumentation. Es dient Ihnen als Nachschlagewerk und als roter Faden beim Einsatz von Icinga 2 in Ihrer Organisation. Bereits nach einigen Zeilen Lektüre werden Sie als Leser bemerken, dass keine Theoretiker für dieses Buch verantwortlich sind. Lennart und Thomas arbeiten seit vielen Jahren in den unterschiedlichsten Einsatzgebieten mit Icinga und wissen, worum es geht. Die Community kann sich glücklich schätzen, dass sie ihr Wissen mit diesem Buch weitergeben. Ich wünsche Ihnen damit mindestens genauso viel Freude wie mit Icinga selbst.

Bernd Erk
Icinga Co-Founder

Vorwort zur 2. Auflage

Als mich Lennart und Thomas bei der ersten Auflage dieses Buchs um ein Vorwort gebeten haben, bin ich dem natürlich sehr gerne nachgekommen. Dass ich bei der nun bereits zweiten Auflage wieder die Gelegenheit habe, freut mich ganz besonders und daher gilt mein Dank dafür den beiden Autoren. Sowohl für die Möglichkeit, aber vor allem für den hohen persönlichen Einsatz und die endlosen Abend- und Wochenendstunden für dieses Werk.

Dass der Untertitel »Ein praktischer Einstieg ins Monitoring« dem Inhalt des Buchs nicht gerecht wird, zeigt sich in der aktualisierten Ausgabe noch deutlicher als beim ersten Buch. Denn genau dieser Einstieg ist nach einem Drittel eigentlich erledigt und die Autoren gehen auf viele Spezialfälle, Anbindung externer Komponenten und erweiterte HA-Szenarien ein. Auch dem Icinga Director, der sich in den letzten Jahren quasi zum Standard für Konfiguration und Verwaltung der Monitoring-Umgebung entwickelt, wurden ebenso wie Graphing und der REST-API viel Zeit und Detailtiefe gewidmet.

Was das Buch jedoch wirklich besonders macht, ist die Tatsache, dass es sich nicht um eine erweiterte Dokumentation der Software handelt. Die Autoren haben neben dem Schreiben viel Zeit in Szenarien, Installation und praktische Ausarbeitung der Komponenten investiert. Das macht dieses Buch zu einem praktischen Nachschlagewerk für die Installation, aber auch die fortwährende Pflege und Erweiterung von Icinga 2 und seinen Komponenten.

Sollten Sie zu meiner großen Überraschung nicht bereits die erste Ausgabe dieses Buchs besitzen, wünsche ich Ihnen viel Freunde beim Erlernen und der praktischen Umsetzung des in diesem Buch erarbeiteten Wissens. Der Wiederholungstäter erhält jedoch nicht nur eine überarbeitete Version, sondern auch viele hundert Seiten, auf denen er Icinga 2 und seine Welt wieder oder neu entdecken kann. Dabei wünsche ich Ihnen ein glückliches Händchen und viel Freude!

Bernd Erk
CEO – Icinga

Einige Zeilen zum Buch selbst

Das vorliegende Buch richtet sich vorwiegend an Administratoren, die Icinga 2 einsetzen, mit dem Gedanken spielen, dies zu tun, oder in absehbarer Zeit von Icinga in der ersten Version auf die aktuelle migrieren wollen. Aber wir hoffen, mit der zweiten Auflage auch erfahrene Monitorverantwortliche zu unterstützen und mit dem ein oder anderen Wissen zu bereichern.

Struktur dieses Buchs

Dieses Buch besteht aus vier Teilen, die sich wiederum in einzelne Kapitel gliedern. Der erste Teil gibt eine kleine Einführung in das Thema Monitoring und stellt die einzelnen Software-Komponenten vor, die Icinga 2 als Gesamtheit bilden. Von der Installation über die grundsätzliche Konfiguration und einen ersten Blick auf die Benutzeroberfläche Icinga Web 2 werden alle wichtigen Begrifflichkeiten erkärt.

Im zweiten Teil geht es um zu ermittelnde Daten auf unterschiedlichen Betriebsystemen, vor allem Linux und Windows. Es befasst sich überwiegend damit, wie diese Daten lokal auf dem zu überwachenden System ermittelt werden und dem Transport zum Icinga-Server. Dies sind grundlegende Werte wie die CPU-, Hauptspeicher- oder Festplattenauslastung. Hier unterstützt Icinga 2 unterschiedliche Transportverfahren wie den mit Icinga 2 eingeführten Icinga-Agenten, aber auch alte Methoden wie NRPE, SSH oder SNMP.

Der dritte Teil vertieft Wissen, z. B. was Icinga 2 betrifft, erweitert dies aber auch durch die Themenkomplexe Benachrichtigungen, Verteilte Überwachung und Hochverfügbarkeit. Einen großen Abschnitt nehmen Beispiele aus der Praxis ein. Dort wird an Beispielen erläutert, wie Dienste bzw. Services mittels unterschiedlicher Plugins überwacht werden können.

Integration ist das Thema des vierten Teils. Es werden einige Erweiterungen vorgestellt, sowie andere Software, die mit Icinga 2 zusammenarbeitet. Auch die REST-API von Icinga 2 als Schnittstelle zum Datenaustausch mit beliebigen anderen Komponenten wird eingehend vorgestellt. Das Kapitel stellt einige Projekte aus dem Bereich Graphing vor, die Icinga 2 mit Daten beliefern kann, und erklärt, wie diese wiederum in Icinga Web 2 visualisiert werden. In Logmanagement geht es um die Alarmierung bei Anomalien, die in Logfiles erscheinen und ausgewertet werden müssen. Der Director als grafisches Konfigurationswerkzeug wird ebenfalls in diesem Teil behandelt, da er in der Lage ist, Daten aus unterschiedlichen Datenquellen zu beziehen, um daraus eine Überwachungskonfiguration zu erzeugen.

Den Abschluss bildet der Anhang mit Tipps zum Troubleshooting, durchzuführenden Updates und wichtigen anzustellenden Überlegungen. Zusätzlich befinden sich hier viele Codebeispiele, die die vorangegangenen Kapitel unterstützen.

Neues in der zweiten Auflage

Alle Kapitel wurden überarbeitet und größenteils komplett neu geschrieben. Dies hatte massive Umstrukturierungsmaßnahmen zur Folge. So befindet sich der Themenkomplex rund um Icinga Web 2 nicht mehr in einem Kapitel, sondern er verteilt sich auf deren drei in unterschiedlichen Teilen

dieses Buchs. Umfangreiche Erweiterungen erfuhren z. B. Icinga Web 2 und Graphing. Neu hinzugekommen sind die Themen Director, Hochverfügbarkeit und die REST-API. All diesem ist der Umstand geschuldet, dass die zweite Auflage den doppelten Umfang im Vergleich zum Vorgänger hat.

In diesem Buch behandelte Versionen

Dieses Buch behandelt hauptsächlich Icinga 2 in der Version 2.8 und Icinga Web 2 2.5. Alle Beispiele zu Installationen beziehen sich, wenn nicht anders angegeben, auf die Distributionen RHEL/CentOS 7 bzw. Debian 9. Dabei wird RHEL wie auch CentOS mit RedHat synonym verwendet.

Das in mehreren Kapiteln eingesetzte und in seiner Benutzung beschriebene MySQL wird ebenfalls als Synonym für MariaDB benutzt.

Typografische Konventionen

In diesem Buch werden folgende typografischen Konventionen verwendet:

- `Nichtproportionalschrift`
  Wird benutzt für Namen von Programmen, Befehlen sowie für Codebeispiele.
- *Kursivschrift*
  Kommt zum Einsatz bei spezifischen Wörtern in Konfigurationen wie Schlüsselwörtern, Objektnamen, deren Attribute oder Custom-Attribute.
- *`Nichtproportionalschrift kursiv`*
  Wird bei Datei- und Verzeichnisnamen verwendet.

> Kommandos oder Codezeilen, die dem Format dieses Buchs geschuldet einem unnötigen oder falschen Zeilenumbruch unterworfen sind, haben am Ende der Zeilen einen Backslash »\«.

Danksagungen

Thomas Widhalm

Ich möchte die Chance nutzen und folgenden Leuten danken: Dr. Michael Barabas, Stefanie Weidner und Miriam Metsch vom dpunkt.verlag für die Unterstützung beim Schaffen dieses Buchs. Sie ließen uns alle Freiheiten und waren doch da, wenn wir Hilfe brauchten. Das ging sogar so weit, dass sie oft vermittelnd eingriffen, wenn weitere Leute benötigt wurden, um das Projekt voranzutreiben. Daher kennen wir teilweise die guten Geister nicht namentlich, denen wir es verdanken, dass dieses Buch nun gedruckt vor uns liegt. Das betrifft insbesondere einige der Reviewer und Lektoren, denen ich gerne ganz besonders danken möchte. Es war sicher nicht immer leicht, dieselben missachteten Rechtschreibregeln immer und immer wieder ausbessern zu müssen. Vielen Dank für das Feedback und die Geduld.

Im Weiteren möchte ich mich bei der Firma NETWAYS GmbH bedanken, die es uns nicht nur ermöglicht, uns täglich mit Projekten rund um Icinga 2 und die anderen in diesem Buch erwähnten Tools zu beschäftigen, sondern uns auch sehr aktiv beim Schaffen dieses Buchs unterstützt hat, sei es durch Zeit zum Schreiben oder Hardware für Teststellungen. Aber die NETWAYS hat auch indirekt ihren Teil zum Buch beigetragen: Ohne einen Arbeitgeber und Kollegen, bei denen man sich derartig wohlfühlt, hätte zumindest ich nicht die Muße, noch Freizeit in ein Projekt dieser Größenordnung zu stecken. NETWAYS – just awesome.

Auch das Icinga-Team hat natürlich seinen Anteil an der Entstehung dieses Buchs. Ohne seine Arbeit gäbe es nichts, worüber wir schreiben könnten. Aber einige der Teammitglieder haben uns auch direkter unterstützt: mit Reviews und dem Beantworten einiger Fragen, die sich im Laufe des Schreibens ergeben haben. Ihren Teil beigetragen haben alle, aber namentlich nennen möchte ich vor allem Bernd, Michi, Gunnar, Eric und Tom, die besonders unter uns zu leiden hatten.

Bedanken möchte ich mich ebenfalls bei einigen meiner Kunden, mit denen ich mich ausgiebig über das Buch unterhalten habe und in deren Umgebung der eine oder andere Codeschnipsel seinen Ursprung hat. Ihr wisst hoffentlich, dass ich euch meine.

Nicht vergessen möchte ich meine Eltern. Sie haben immerhin viel dazu beigetragen, dass ich zu dem geworden bin, der ich heute bin. Ohne ihre Unterstützung hätte ich mich nicht dahin entwickeln können, wo ich jetzt stehe. Vielen Dank dafür, dass ihr mir geholfen habt, wo ich es brauchte, ohne mich daran zu hindern, meinen Weg zu gehen.

Ebenso danke ich meinen Freunden aus früherer und heutiger Zeit. Auch sie haben ihren Anteil daran, dass ich jetzt in der Lage bin, zu tun, was ich tue. Dankbar bin ich vielen, aber namentlich erwähnen möchte ich den Hias, Asi und Babsi, die mir gezeigt haben, wie schön es ist, enge Freunde zu haben. Andi danke ich dafür, dass er mir in einer sehr dunklen Zeit beigestanden hat und immer noch mein Freund ist. Max dafür, dass er so vieles nachvollziehen konnte. Und Benny »sleepless« dafür, dass er mir bewiesen hat, dass enge Freundschaften auch über das Internet möglich sind. Joe dafür, dass er ein lebendes Beispiel dafür ist, dass man verwandt und befreundet zugleich sein kann. Pazi dafür, dass sie einem immer das Gefühl gibt, willkommen und geschätzt zu sein, egal, wie lang man sich mal wieder nicht gesehen hat. Dem Plainer dafür, dass er die ritterlichste Person ist, die ich kenne. Daniel dafür, dass er mir gezeigt hat, dass man Gleichgesinnte in den unterschiedlichsten Menschen finden kann. Meinen Schwiegereltern dafür, dass sie mich so offen aufgenommen haben.

Danken möchte ich den »Drei ???« für endlose Stunden voller Hörspiele während Zugfahrten und beim Einschlafen, George Lucas für »Star Wars« und Extrema Ratio für die besten Messer der Welt.

Natürlich möchte ich auch Lennart dafür danken, dass wir gemeinsam dieses Projekt gestemmt haben. Es war sicher nicht immer leicht mit mir und ohne ihn wäre das Buch wohl nie Realität geworden. Danke dafür und beileibe nicht nur dafür! Unter anderem auch für viele erheiternde und erhellende Gespräche, gemeinsame Videoabende und Diskussionen über den Unterschied zwischen Deutsch und Österreichisch. Dafür, dass du Kollege und Freund bist.

Auch unserer Hündin Afra möchte ich danken. Sie hilft mir immer wieder, den Kopf bei einem Spaziergang freizubekommen oder mich aufzuheitern, wenn mich mal wieder was »anzipft«.

Zu guter Letzt möchte ich mich bei meiner Frau Ina bedanken. Für mehr, als ich hier aufzählen kann, aber vor allem auch dafür, dass sie meinen Job als Consultant akzeptiert und dabei so oft auf mich verzichtet. Dass sie immer da ist, wenn ich Unterstützung und ein offenes Ohr brauche, und nie gemurrt hat, wenn es wieder mal »ums Buch« ging. Aber auch für die vielen wunderbaren gemeinsamen Jahre, weshalb auch sie maßgeblich daran beteiligt ist, dass ich so ein Projekt überhaupt angehen konnte. Vielen, vielen Dank!

Danke euch allen, dass ihr euch meine endlosen »Ich schreib jetzt mein eigenes Buch!«- und »Ja, es ist eh bald fertig«-Vorträge angehört und ertragen habt. Und danke auch einigen von euch für die Kommentare, Meinungen und Reviews, die alle dieses Buch besser gemacht haben, als es ohne euch geworden wäre.

Für die zweite Auflage möchte ich noch mal all jenen danken, die unser erstes »Baby« so aufmerksam gelesen und uns unheimlich wertvolles Feedback gegeben haben. Ich hoffe, wir haben alles erwischt und berücksichtigt. Es ist immer wieder schön, mit Lesern zu reden und zu sehen, wenn es tatsächlich jemandem genützt hat.

Vielen Dank für alles.
Thomas Widhalm

Lennart Betz

Da hat mir der Thomas nicht viel übrig gelassen. Ich möchte all denen in meiner Familie und meinem Freundeskreis danken, die unter diesem Projekt gelitten haben.

Ein besonderen Dank an Bernd, Michael und Bodo. An Bernd, der das Vorwort auch zur zweiten Auflage verfasste, Michael Friedrich, der das Kapitel über Dashing beisteuerte, und Bodo Schulz, der sich mit einem Abschnitt über die von ihm geschriebene Ruby-Bibliothek beteiligte.

Servus
Lennart

Feedback

Die Qualität jedes Fachbuchs misst sich am Nutzen, den es für seine Leser hat. Wir würden uns freuen, davon zu hören, was Sie als Leser nützlich im Buch fanden und wo wir uns noch verbessern können. So wie sich die beschriebene Software weiterentwickelt, soll es auch unser Buch tun und hiermit geben wir Ihnen die Chance, die Richtung zu beeinflussen, in die es geht.

Für Rückmeldungen zum Buch freuen wir uns über E-Mails an feedback@icinga-book.net.

Inhaltsverzeichnis

Teil I

Einführung

1 Einleitung

Mit dem Begriff »Monitoring« werden Systeme bezeichnet, die den Zustand von Geräten und Programmen überwachen und beim Abweichen vom gewünschten Zustand Alarmmeldungen verschicken.[1]

Ohne Monitoring können die Betreuer von IT-Systemen nur dann reagieren, wenn ein Anwender eine Störung meldet oder sie selbst durch sehr zeitaufwendige manuelle Kontrolle oder per Zufall ein Problem feststellen. Beim heute üblichen Zahlenverhältnis zwischen Systemen und Betreuern ist eine manuelle Kontrolle nicht mehr zu realisieren und wenn ein Anwender ein Problem feststellt, ist es eigentlich schon zu spät, da genau diese Probleme ja verhindert werden sollen.

Um diese Problematik zu lösen, werden Monitoring-Systeme benötigt, die versuchen, Schwierigkeiten frühzeitig zu bemerken, damit sie behoben werden können, bevor sie größeren Schaden anrichten können oder bevor Benutzer davon betroffen sind. Dafür gibt es verschiedene Ansätze:

- Ermitteln von Ergebnissen einer eigenen Statusprüfung und Logs von Anwendungen oder Hardware.
- Ende-zu-Ende-Checks wie das Versenden einer E-Mail und Prüfen, ob sie auch ankommt.
- Simulieren einer Nutzung eines Dienstes wie das Aufrufen einer Website.
- Prüfen von Eckdaten eines Systems wie das Abfragen der Festplattenauslastung mit Bordmitteln.

Icinga 2 bietet dabei die Möglichkeit, alle oben genannten Verfahren abzudecken, spezialisiert sich jedoch auf die letzten beiden Ansätze. Diese Flexibilität rührt daher, dass Icinga 2 selbst keine Funktionalität zur direkten Überwachung enthält, aber sehr gut darin ist, »Plugins«, also ausführbare Dateien, die ein paar Anforderungen erfüllen, laufen zu lassen und die Ausgabe zu interpretieren. Falls sich also eine Überwachungsmöglichkeit in einer ausführbaren Datei realisieren lässt, kann sie auch in Icinga integriert werden.

[1] Dies ist keine offizielle Definition, zeigt aber Sinn und Zweck des in diesem Buch beschriebenen Tools Icinga 2.

1.1 Es war einmal...

Icinga 2 ist ein sehr modernes Monitoring-System, das keinen Code von seinen geistigen Vorgängern enthält, aber fast alle bewährten Konzepte weiterverwendet. Diese Ähnlichkeit erleichtert vor allem Umsteigern die Arbeit mit Icinga 2 deutlich. Die folgenden Zeilen sollen einen kurzen Überblick über die bisherige Entwicklung geben.

1.1.1 Icinga

Im April 2009 wurde das Icinga-Projekt gegründet, das einen Fork des Nagios-Monitoring-Systems entwickeln sollte, da viele Community-Mitglieder unglücklich über den Umgang mit eingereichten Patches und den Umgang von Nagios Enterprises mit der Nagios-Community waren. Bei einem Fork wird der aktuelle Stand des Quellcodes eines Programms von verschiedenen Entwicklerteams in unterschiedliche Richtungen weiterentwickelt. Häufig wird dabei das bisherige Team aufgespalten und je ein Teil entwickelt vom gleichen Ausgangspunkt aus in verschiedene Richtungen weiter. Üblicherweise behält dabei ein Team den Namen des Produkts bei und das andere sucht sich einen neuen. Beim Icinga-Team fiel die Wahl auf »Icinga«, das Zulu-Wort für »Ausschau halten«.

Der Fork, und damit auch die weiteren Schritte wie die Evolution von Icinga zu Icinga 2, war insbesondere auch möglich, da einige Firmen bereit waren, Entwicklern Zeit zu sponsern, um die Entwicklung von Icinga voranzutreiben. Dies geschah meist aus Eigeninteresse, da sie Monitoring auf Nagios-Basis bei sich oder ihren Kunden erfolgreich einsetzten und eine Lösung für die schleppende Entwicklung suchten. Der Fork war nötig, da zuvor zwar entwickelt wurde, die daraus resultierenden Patches jedoch nicht in Nagios einflossen. Das Icinga-Team bemüht sich, schneller auf Input aus der Community zu reagieren, und hat auch genug »Stammmitglieder«, um die Entwicklung voranzutreiben. Eine dieser Firmen ist die NETWAYS GmbH[2] aus Nürnberg in Deutschland, die einige der Icinga-Kernentwickler angestellt hat, die entweder im Kundenauftrag oder als Dienst an der Community weiter an Icinga, Icinga 2 und anderen Tools aus diesem Ökosystem arbeiten. Auch die Autoren dieses Buchs haben von der NETWAYS GmbH Zeit gesponsert bekommen, um dieses Projekt zu verwirklichen.

[2] http://www.netways.de

1.1.2 Icinga 2

Um einige sehr tief im Code verwurzelte Einschränkungen aufzulösen, hat sich das Icinga-Team entschlossen, mit dem Code bei null zu beginnen und alles komplett neu zu schreiben. Das Resultat ist das Release von Icinga 2 Version 2.0 vom 16. Juni 2014. Darin wurden die bekannten Konzepte in der Bedienung weitergeführt, aber auch einige sehr wichtige Neuerungen eingeführt.

Diese Neuerungen umfassen unter anderem:

- eine Domain Specific Language (DSL) zur Konfigurationi,
- den integrierten Cluster-Stack, zur Kommunikation von verschiedenen Icinga-Instanzen untereinander,
- das Verteilen von Teilen der Konfiguration an beliebig viele andere Icinga 2 Instanzen,
- besseres Ausnutzen der verfügbaren Ressourcen durch Multithreading,
- der Einsatz als Agent,
- die API, mit der u. a. zu überwachende Objekte zur Laufzeit hinzugefügt werden können.

Die neue regelbasierte Sprache erlaubt eine deutlich flexiblere Konfiguration. Viele Objekte, die früher einzeln definiert werden mussten, können nun automatisch durch Auswerten von Regeln und Funktionen angegeben werden. Das spart nicht nur sehr viel Tipparbeit, sondern schützt auch vor Fehlern, da einmal definierte Regeln natürlich auch für neue Objekte gelten.

Um Demilitarized Zones (DMZs) oder entfernte Netzwerke zu überwachen, wurden auch bei den Vorgängern von Icinga 2 schon mehrere Instanzen verwendet, die miteinander kommunizieren. Allerdings enthielten diese keinen nativen Weg, mehrere Instanzen miteinander zu verbinden, weshalb verschiedenste Lösungen dafür entwickelt wurden. Diese waren jedoch teilweise kompliziert zu konfigurieren und oft auch nicht performant genug, um die Zeit zwischen Auftreten einer Störung und der Alarmierung ausreichend kurz zu halten. Dieses Verbinden von Instanzen wurde auch genutzt, um die auftretende Last zwischen mehreren Hosts zu verteilen und in Verbindung mit Clustertools wie `corosync`[3] und `pacemaker`[4] Hochverfügbarkeit zu erreichen.

Durch die neue Clusterfunktionalität können nicht nur lastverteilte und hochverfügbare Cluster mit Icinga 2 Bordmitteln erreicht werden, auch untergeordnete Icinga 2 Instanzen in anderen Netzsegmenten können Ergeb-

[3] http://corosync.github.io/corosync
[4] http://clusterlabs.org/pacemaker

nisse von Checks, die sie ausführen, an zentrale Instanzen weiterschicken. Diese zeigen einen Gesamtüberblick an und alarmieren.

Über die Clusterverbindung kann auch von zentralen Systemen aus eine Konfiguration an untergeordnete Instanzen ausgebracht werden.

Die Vorgänger von Icinga 2 liefen als ein einziger Thread und konnten so auch nur einen CPU-Kern ausnutzen. Zwar waren die gestarteten Plugins immer schon eigene Threads, dennoch wurde dadurch einer Installation eine Obergrenze an zu überwachenden Systemen gesetzt. Icinga 2 ist nun multithreaded und kann die zur Verfügung stehenden Ressourcen tatsächlich ausnutzen.

Durch den geringen Ressourcenverbrauch des Icinga 2 Kerns, die Clusterverbindung und die Konfigurationsverteilung hat sich eine neue Anwendungsmöglichkeit als Agent ergeben. Dabei wird eine Icinga 2 Instanz auf einem zu überwachenden Host installiert, die nur eben diesen überwacht. Die Ergebnisse leitet sie über die Clusterverbindung an eine zentrale Instanz weiter, die die Checks aller angeschlossenen Icinga 2 Instanzen sammelt und eine Übersicht zur Verfügung stellt. Konfiguriert wird sie von der zentralen Instanz aus. Für einen Vergleich aus Anwendersicht bietet die Icinga 2 Onlinedokumentation[5] einen umfassenden Überblick an.

1.1.3 Namen und Versionen

Aktuell wird nur noch die Version 2.x weiterentwickelt. Dieses Buch behandelt ausschließlich den 2.x-Zweig der Entwicklung. Mit dem Versionssprung von 1.x auf 2.x geht aber auch eine Umbenennung einher, daher heißt das Tool nun tatsächlich »Icinga 2 Version 2.x«.

Gleiches gilt für das moderne Webinterface Icinga Web 2. Es ist übrigens zu beiden existierenden Icinga-Varianten kompatibel, weshalb man durchaus Icinga 2 2.8.1 wie auch Icinga 1.13.3 mit Icinga Web 2 2.5.1 betreiben kann.

Die hier genannten Versionen waren zum Zeitpunkt, als die zweite Auflage dieses Buchs entstand, die jeweils aktuellsten.

1.2 Software-Komponenten

Ein Monitoring-System auf Basis von Icinga 2 besteht aus mehreren Teilkomponenten, so bildet der Core »Icinga 2« das Grundgerüst. Er regelt alle Abläufe, unter anderem z. B., wann was wie zu überwachen ist.

Die eigentliche Arbeit der Überwachung wird dann durch sogenannte Plugins erledigt, die vom Core aufgerufen werden und deren Ergebnisse

[5] https://www.icinga.com/docs/icinga2/latest/doc/23-migrating-from-icinga-1x/

dann verarbeitet werden. Plugins werden gesondert angeboten und nicht vom Icinga-Team betreut.

Die Komponente Icinga Web 2 ist ein in Hypertext Preprocessor (PHP) geschriebenes Framework zur Darstellung der ermittelten Ergebnisse der Überwachung mit Icinga 2. Als Schnittstelle zwischen Core und dem in einem Webserver laufenden Icinga Web 2 muss eine Datenbank verwendet werden. Unterstützt werden ausschließlich MariaDB respektive MySQL oder PostgreSQL. Das Beschicken dieser Datenbank ist über ein explizit einzuschaltendes Core-Feature zu aktivieren.

- Icinga 2
- Plugins, z. B. die Monitoring-Plugins[6]
- MariaDB-, MySQL- oder PostgreSQL-Datenbank
- Icinga Web 2
- Webserver mit PHP, standardmäßig Apache

Alle Komponenten werden in eigenen Projekten gepflegt und weiterentwickelt, somit wird auch jede unter einer eigenen Versionierung geführt. Darüber hinaus existieren viele weitere Komponenten, die über das bis hierher Erwähnte hinausgehen. So existiert mit dem Director eine Integration in Icinga Web 2 zur grafisch unterstützten Konfiguration oder diverse Projekte, die zeitliche Verläufe von Daten aus anderen Projekten wie Graphite oder InfluxDB einbinden.

1.3 Grundlagen

Icinga 2 ist wie auch sein Vorgänger auf Verfügbarkeitsüberwachung ausgelegt. Hierbei wird primär mit aktiven Checks gearbeitet. Als ein Check wird der Test eines Hosts oder Services bezeichnet. Jedes Gerät mit einer IP-Adresse wird als Host-Objekt betrachtet. Ein Service ist immer einem Host zugeordnet, ist also z. B. ein auf einem Host laufender Dienst oder eine zu überwachende Hardwarekomponente. Die Logik, wie Tests zu erfolgen haben, ist in sogenannten Plugins implementiert. Plugins sind externe Programme, die für jeden aktiven Check aufgerufen werden und über ihren Returncode den ermittelten Status zurückgeben.

Plugins können somit auch durch den Benutzer zu Testzwecken aufgerufen werden. Zu beachten ist, dass dies durch den Benutzer erfolgen sollte, unter dem der Icinga 2 Prozess ausgeführt wird. Auf RedHat-Systemen ist das *icinga*, auf Debian hingegen historisch bedingt der Benutzer *nagios*.

```
$ sudo -u icinga /usr/lib64/nagios/plugins/check_procs
PROCS OK: 100 processes | procs=100;;;0;
```

[6] http://www.monitoring-plugins.org

So ermittelt z. B. das Plugin `check_procs` durch einen Aufruf ohne Parameter die momentan auf dem System lauffähigen Prozesse. Die Ausgabe informiert über den ermittelten Status und die Anzahl der Prozesse. Der Text nach dem senkrechten Strich (Pipe) enthält Metriken, die das Plugin ermittelt hat, die sogenannten Performance-Daten. Eine genaue Erläuterung erfolgt in Kapitel 20 ab Seite 470.

Plugins sollten auch immer eine Hilfsfunktion bieten, damit ein Anwender dessen Funktionsumfang kennenlernen kann.

```
$ cd /usr/lib64/nagios/plugins
$ sudo -u icinga ./check_procs --help
check_procs v2.1.4 (nagios-plugins 2.1.4)
Copyright (c) 1999 Ethan Galstad <nagios@nagios.org>
Copyright (c) 2000-2014 Nagios Plugin Development Team
  <devel@nagios-plugins.org>

  Checks all processes and generates WARNING or CRITICAL
  states if the specified metric is outside the required
  threshold ranges. The metric defaults to number of
  processes. Search filters can be applied to limit the
  processes to check.

Usage:
check_procs -w <range> -c <range> [-m metric] [-s state]
 [-p ppid] [-u user] [-r rss] [-z vsz] [-P %cpu]
 [-a argument-array] [-C command] [-k] [-t timeout] [-v]

Options:
 -h, --help
    Print detailed help screen
 -V, --version
    Print version information
 --extra-opts=[section][@file]
    Read options from an ini file. See
    https://www.nagios-plugins.org/doc/extra-opts.html
    for usage and examples.
 -w, --warning=RANGE
   Generate warning state if metric is outside this range
 -c, --critical=RANGE
   Generate critical state if metric is outside this range

[...]
```

Plugins müssen vier Zustände zurückliefern können, OK, WARNING, CRITICAL und UNKNOWN. Diese werden als Returncode vom Plugin zurück gegeben. Kann ein Zustand nicht ermittelt werden, weil z. B. das Plugin nicht ausführbar ist oder eine gewisse Laufzeit überschreitet und damit in