

# **Check\_MK – Monitoringsystem für jedermann**

**Thorsten Bruhns**  
**OPITZ CONSULTING Deutschland GmbH**  
**Bad Homburg**

## **Schlüsselworte**

Check\_MK, Nagios, Open Monitoring Distribution, Oracle RDBMS

## **Check\_MK Monitoring System**

Das Check\_MK Monitoring System hat seinen Ursprung im Projekt Check\_MK, das 2008 ins Leben gerufen wurde und heute die wichtigste Komponente im gesamten System ist. Es entstand als eine Erweiterung für den Nagios-Core, um die Verwaltung von großen Systemumgebungen stark zu automatisieren und um bekannte Performance-Probleme von Nagios mit Hilfe einer innovativen Architektur zu lösen.

Der Vortrag wird sich mit der Architektur des Check\_MK Monitoring Systems befassen und dabei auf die Möglichkeiten beim Monitoring von Infrastrukturkomponenten konzentrieren. Es wird aufgezeigt, warum eine so umfangreiche Lösung, die Überwachung einer gesamten IT-Landschaft ermöglicht, dabei wenig Ressourcen in Anspruch nimmt, die Installation sehr einfach ist und der Administrationsaufwand so gering ist.

## **Architektur des Check\_MK Monitoring Systems**

Das Monitoring System besteht aus einer Vielzahl von Komponenten, die zusammen das Check\_MK Monitoring System bilden.

Nachfolgend werden die wichtigsten Komponenten kurz erläutert, um einen Überblick über das System zu erhalten. Alles zusammen wird mit Hilfe der Open Monitoring Distribution – kurz OMD – als 1 RPM für Intel x86 Linux bereit gestellt, so dass die Installation extrem einfach ist. Das System ist für alle gängigen Linuxdistributionen verfügbar. Es bietet die Möglichkeit, unterschiedliche Versionen und mehrere Sites gleichzeitig auf einem Host betreiben zu können. So ist eine hohe Flexibilität bei Upgrades sowie der Betrieb von mehreren Mandanten parallel möglich. Die Steuerung übernimmt hier OMD, was als Projekt unter der GPL 2010 gegründet wurde, um die Installation von nagiosbasierten Monitoringlösungen möglichst einfach zu gestalten. Ziel von OMD soll sein, dass sich der Administrator nicht um die Installation und Konfiguration der Teilkomponenten kümmern muß und zudem parallel verschiedene Versionen installiert werden können. Der Administrator soll sich primär um die Konfiguration der Ziele kümmern und sich keine Gedanken über die Softwareinstallation machen müssen. Im praktischen Betrieb bei OPITZ CONSULTING hat sich gezeigt, dass dieses Ziel vollständig erreicht wurde!

Der Monitoring Core ist im System die wichtigste Komponente, da hier alle Informationen zusammen laufen und verarbeitet werden. Hier hat Mathias Kettner mit dem Check\_MK Micro Core – kurz CMC – eine Alternative geschaffen, die viele Limitierungen des Nagios-Cores beseitigen. Über OMD hat der Administrator die Möglichkeit, zwischen CMC und Nagios als Core zu wechseln, wenn er einen bestimmten Core bevorzugt. Seitens Mathias Kettner wird der CMC als Standard verwendet, was sich in der Praxis als eine gute Entscheidung erwiesen hat. Insbesondere im Bereich Performance bietet der CMC erheblich schnellere Verarbeitungszeiten und kann problemlos mehr als 1000 Hosts überwachen.

2008 ist Check\_MK als Erweiterung für den Nagios-Core entstanden. Es sollte ein System entwickelt werden, das das Pflegen von Nagioskonfigurationen automatisiert, in dem entweder per snmpwalk oder über ein Agentenmodell Ergebnisse von den Zielsystemen eingeholt werden. Diese Daten werden in Check\_MK geparkt und in entsprechende Services umgewandelt, die dann als Konfigurationsdatei für den CMC bzw. Nagios bereit gestellt werden. So können automatisiert eine große Anzahl von Systemen ins Monitoring aufgenommen werden, ohne umfangreich Konfigurationen pflegen zu müssen. Als Nebeneffekt werden so auch neue Checks – z.B. neue Filesysteme – erkannt, da der Agent auf dem zu überwachenden System immer alle Informationen über alle erkannten Filesysteme liefert.

Die Definition von Schwellwerten erfolgt mit Regelwerken, die mit Hilfe von Tags und einer hierarchischem Model vererbt werden können. Die Regelwerke sind neben der automatischen Erkennung und das Erzeugen der Konfigurationsdateien die wichtigste Funktion von Check\_MK.

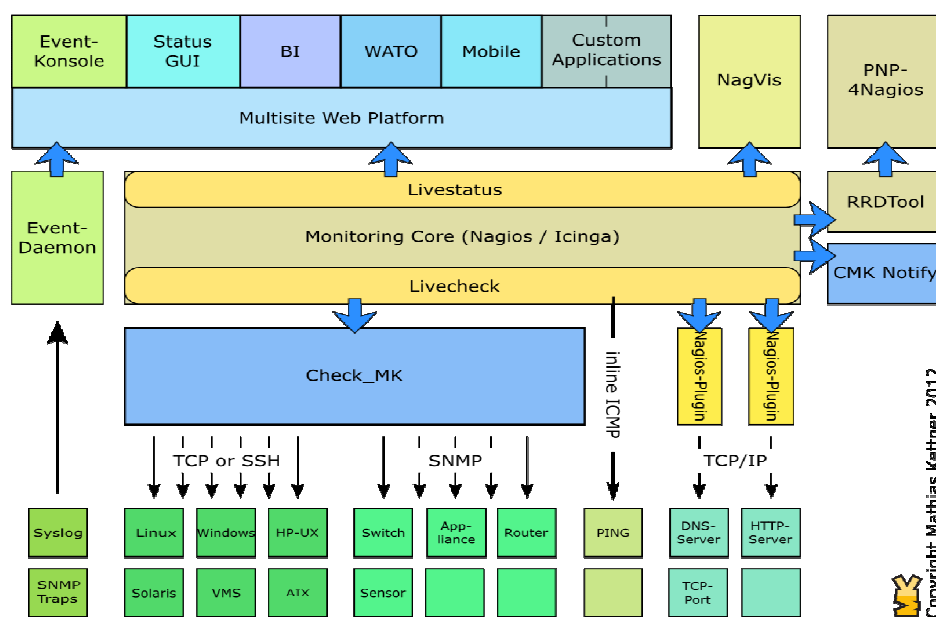


Abb. 1: Architekturschaubild (Quelle [https://mathias-kettner.de/check\\_mk.html](https://mathias-kettner.de/check_mk.html))

Livestatus und Livecheck dienen als Schnittstelle zu den anderen Komponenten, wobei sich Livestatus in zahlreichen nagiosbasierten Lösungen als Standard für die adhoc Abfrage des Monitoring-Cores etabliert hat. Livestatus wurde von Mathias Kettner entwickelt, weil er eine Lösung suchte, mit der eine möglichst schnelle und vor allem genaue Abfrage des Nagios-Cores möglich ist.

Die Multisite Web Platform beinhaltet eine Vielzahl von weiteren Modulen, von denen die Status GUI und WATO (Web Administration Tool) am wichtigsten sind. Über die GUI ist mittlerweile eine vollständige Administration der Regel und Erkennung von Zielsystemen möglich, so das im täglichen Betrieb kein Zugriff auf die Kommandozeile mehr erforderlich ist.

Eine Besonderheit im Check\_MK Monitoring System ist die Event-Server-Konsole. Sie bietet neben dem statusbasierten Monitorings die Möglichkeit, auch eine eventbasierte Überwachung zu ermöglichen, was die Möglichkeiten des System erheblich erweitert. Sie kann zudem als Empfänger für syslog-Meldungen genutzt werden, um Events aufgrund von Logmeldungen zu veranlassen. Die Status GUI

hat Modul, so das die Konfiguration der Event-Konsole auch vollständig über die GUI möglich ist. Eine Kopplung von status- zu eventbasiertem Monitoring ist möglich, so das ein rein eventbasiertes Monitoring ermöglicht wird. Diese Eventkonsole wurde ursprünglich für einen Großkunden entwickelt, der eine große kommerzielle Lösung ersetzen wollte. Auch hier hat sich der Einsatz bei verschiedenen Kunden bewährt und Weiterentwicklungen einfließen lassen, die einen stetigen Ausbau der Funktionalitäten zur Folge haben.

### **Was kann überwacht werden?**

Aus dem Schaubild ist im unteren Bereich ersichtlich, das unterschiedliche Methoden zur Überwachung von Zielsystemen zur Verfügung stehen.

Die Überwachung mittels SNMP ist einer der wesentlichen Bestandteile von Check\_MK. Hier wird eine Vielzahl von Endgeräten unterstützt, die mittels snmpwalk automatisch erkannt und entsprechend mit Checks eingebunden werden. Da auch hier das Packagekonzept für eigene Checks genutzt werden kann, ist eine Erweiterung für bisher unbekannte Endgeräte möglich.

Als Zielplattformen werden alle bekannten Linux-Distributionen, MS Windows, Solaris, AIX, HP/UX, z/OS und einiges mehr unterstützt. Da die Agenten alle in Shell und für Windows in C geschrieben sind, ist eine Portierung auf andere Plattformen und Distributionen möglich. Es wird bewusst darauf geachtet, die Agenten möglichst überschaubar zu halten, damit sie wenig Ressourcen beanspruchen und die Pflege des Codes weiterhin möglich ist.

Mit Hilfe eines Plugin-Konzeptes können zusätzliche Module in Agenten eingebunden werden, so das der normale Agent nur die Standardhostinformationen wie CPU, Memory, Filesysteme, Volume-Manager und Prozesse liefert, während für Oracle (mk\_oracle), MySQL (mk\_mysql) usw. zusätzliche Plugins eingebunden werden.

Neben dem Agentmodell können alle ggf. bereits existierenden Nagios-Plugins weiter genutzt werden, so das einerseits eine Migration möglich ist, darüber hinaus aber auch eine sehr große Auswahl an individuellen Checks zur Verfügung stehen. Der Check\_MK-Agent bietet eine Schnittstelle, die ein Einbinden von NRPE-Checks mit automatischer Erkennung der Checks in Check\_MK ermöglicht. So wird sicher gestellt, das jeder neue Check auch automatisch erkannt wird und nichts mehr übersehen werden kann.

Spezialagenten, die u. a. für VMware vSphere und NetApp zur Verfügung stehen, ermöglichen eine individuelle Überwachung von Komponenten, wo die SNMP oder Check\_MK-Agenten nicht möglich sind. Auch diese können bei Bedarf durch Individualentwicklungen erweitert werden.

Mit mk\_jolokia steht als weiteres Beispiel ein Plugin für den Agenten zur Verfügung, das die Überwachung von deployten Anwendungen in Tomcat, JBoss oder WebLogic ermöglicht.

Die Checksammlung umfaßt mittlerweile mehr als 600 Checks. Sie wird ständig erweitert und bietet über ein dokumentiertes Packagekonzept die Möglichkeit, eigene Checks zu entwickeln und in Check\_MK zu integrieren. Mit Check\_MK Exchange ([https://mathias-kettner.de/check\\_mk\\_exchange.php](https://mathias-kettner.de/check_mk_exchange.php)) steht eine Plattform zu Verfügung, wo bereits zahlreiche zusätzliche Checks veröffentlicht wurden.

## **Fazit**

Das Check\_MK Monitoring System hat sich im Laufe der Jahre zu einer vollständigen Monitoringlösung entwickelt, die sich durch einfache und schnelle Installation auszeichnet und über das Webinterface intuitiv administrierbar ist. Das modulare Konzept bietet genug Freiraum für Erweiterungen, wenn die Checksammlung für die eigenen Bedürfnisse mal nicht ausreichend sein sollte.

Das System steht mit Ausnahme von einigen Komponenten, wie die Bakery und Check\_MK Micro Core unter der GPL, so dass eine Verfügbarkeit des Codes und eine Beteiligung an der Weiterentwicklung möglich ist. Da Mathias Kettner Support- und Dienstleistungen rund um Check\_MK anbietet, ist über diesen Weg auch die Erweiterung bzw. Entwicklung von zusätzlichen Modulen möglich. Ein wesentlicher Teil der Weiterentwicklungen haben so den Weg in das Check\_MK Monitoring System gefunden.

Zum Test kann jederzeit eine Demoversion mit allen Möglichkeiten oder die Community-Edition auf der Homepage ([www.mathias-kettner.de](http://www.mathias-kettner.de)) heruntergeladen werden. Letztere kann uneingeschränkt genutzt werden, bietet dafür aber nicht den vollen Funktionsumfang, der für die meisten Installationen nicht erforderlich ist.

Für den produktiven Einsatz ist der Abschluss eines Supportvertrages zu empfehlen, der im Vergleich zu kommerziellen Monitoringlösungen sehr preiswert ist.

OPITZ CONSULTING setzt das Check\_MK Monitoring System im Rahmen von Managed Services bei zahlreichen Kunden erfolgreich ein. Über die Partnerschaft mit Mathias Kettner erfolgt die Pflege und Weiterentwicklung des mk\_oracle-Plugins zur Überwachung von Oracle Datenbanken.

### **Kontaktadresse:**

Thorsten Bruhns  
Solution Architect

OPITZ CONSULTING Deutschland GmbH

Telefon: +49 (0) 6172 66 26 0 – 15 41  
Fax: +49 (0) 6172 66 26 0 – 45 00  
E-Mail: [thorsten.bruhns@opitz-consulting.com](mailto:thorsten.bruhns@opitz-consulting.com)  
Internet: [www.opitz-consulting.de](http://www.opitz-consulting.de)