Monitoring: Open Source vs Proprietäres Closed Source

AIOps mit der Freiheit von Open Source Monitoring

Zusammenfassung

Es mag den Anschein haben, dass sowohl Open- als auch Closed-Source Softwarelösungen gleichwertig sind denn beide haben ihre Vor- und Nachteile. Heute erscheinen jedoch Open-Source Lösungen immer kompetenter und sollten daher als echte Alternative zu Closed-Source Lösungen gesehen werden. Open-Source Lösungen sind nicht nur der meist kostenlose Ersatz für die bisher dominierenden Big Four sondern versprechen enorme Innovationsschübe geschuldet den wachsenden Communities und stellen mit ihren überwältigenden Vorteilen Closed-Source Lösungen immer mehr in den Schatten.

Kontakt: risetech@rise-world.com

RISE

Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektentwicklung GmbH

www.rise-world.com • welcome@rise-world.com

Vorwort

In einer IT-Welt, die zunehmend durch Komplexität, Geschwindigkeit und die schiere Menge an Daten geprägt ist, gewinnen flexible, skalierbare und kosteneffiziente Lösungen mehr und mehr an Bedeutung. Open-Source-Technologien haben sich in diesem Kontext als leistungsstarke Werkzeuge etabliert, die den Anforderungen moderner IT-Infrastrukturen gerecht werden. Besonders im Bereich des Monitoringsystems, einem der Herzstücke jeder IT-Umgebung, bieten Open-Source-Lösungen einen entscheidenden Vorteil gegenüber proprietären, Closed-Source Systemen.

Dieses Whitepaper beleuchtet, warum Open-Source-Monitoringsysteme eine attraktive Alternative zu proprietären Lösungen darstellen, und wie sie speziell in der Umsetzung einer AIOps-Strategie (Artificial Intelligence for IT Operations) eine Schlüsselrolle spielen können. Durch ihre Offenheit, Anpassungsfähigkeit und Innovationskraft bieten Open-Source-Lösungen die Grundlage, um den Anforderungen einer datengetriebenen und automatisierten IT-Betriebsstrategie gerecht zu werden.

Unser Ziel ist es, Ihnen aufzuzeigen, wie Sie mit Open-Source-Monitoring-Systemen die Kontrolle über Ihre IT-Umgebung verbessern, Betriebskosten senken und gleichzeitig die Grundlage für eine intelligente Automatisierung schaffen können. Dieses Whitepaper liefert Einblicke in den Einsatz von Open-Source-Lösungen und gibt Ihnen Grundlagen an die Hand, um Ihre AIOps-Strategie effektiv umzusetzen.

Wir hoffen, dass dieses Whitepaper Ihnen wertvolle Erkenntnisse liefert und Sie dazu inspiriert, die Potenziale von Open Source für Ihre Monitoring- und AIOps-Strategien zu erschließen.

Inhaltsverzeichnis

1 Das Zeitalter von Open-Source Monitoring

Viele Jahrzehnte über waren Monitoring Lösungen auf Basis der Big Four (HP, CA, IBM und BMC) die einzigen und daher dominierenden Werkzeuge um effizientes, sicheres und potentes Monitoring durchzuführen. Diese Tatsache hat sich aus verschiedensten Gründen in den letzten Jahren stark verändert und heute sehen wir immer mehr Plattformen basierend auf Open-Source Produkten.

Wir wollen zu Beginn kurz auf die mittlerweile fast schon historischen Big Four Lösungen eingehen bevor wir danach Open-Source- und Closed-Source Monitoring Werkzeuge vergleichen und zwar nicht mit dem Ziel eine endlose Diskussion zu entfachen, sondern eine Vorstellung davon zu bekommen welche Möglichkeiten es heute generell gibt. Obwohl Befürworter des einen typischerweise Feinde des anderen sind, ist es eine Tatsache, dass es in jeder Kategorie gute und schlechte Software gibt. Wie wir Sie sehen werden, gibt es viele gute Optionen in beiden Kategorien.

Wir wollen zuerst erklären, was Open-Source-Software ist, und vergleichen anschließend verschiedene Aspekte der einzelnen Vertriebsmodelle. Wir wollen uns detaillierter ansehen, wie sich Open-Source Monitoring Werkzeuge in Bezug auf den Preis, aber auch auf Support, Leistung und Zuverlässigkeit sowie Anpassungsmöglichkeiten unterscheiden. Dann gehen wir auf einige Sicherheitsbedenken im Zusammenhang mit Open-Source-Software ein, und schließen unseren Überblick damit ab, indem wir einige der besten kostenlosen und offenen Monitoring-Tools und einige kostenpflichtige Alternativen vergleichen.

Wir werden am Ende dieses Whitepapers beleuchten, warum wir bei COMPRISE auf COMMOC setzten, ein Open-Source Tool, das basierend auf Icinga2 und Grafana eine komplette, offene, kostengünstige und zukunftssichere Monitoring Plattform darstellt, die alle Vorzüge des modernen Open-Source basierten Monitorings bietet und offen ist für neueste Trends wie zum Beispiel AIOps.

2 Von den Big 4 Monitoring Plattformen zu Open Source Systemen

Einer der Hauptgründe für den Niedergang der alten ITOM-Softwareanbieter war deren übermäßiges Vertrauen in Akquisitionen. Die Big Four verbrachten die meiste Zeit damit, Deals zu verfolgen und die heißesten Technologie-Startups zu erwerben, anstatt ihre Produkte durch gezielte Entwicklung modern und relevant zu erhalten. Stattdessen hatten sie ein einfaches Rezept: die neueste Akquisition in bestehende Tools einbinden und ihre Vertriebsmitarbeitern dazu anzuspornen, die neue Lösung als integrierte Gesamtlösung zu verkaufen. Dies sowie die rasante Verbreitung von Open-Source Tools und die sich immer rascher ändernden Voraussetzungen heutiger IT führten in den letzten Jahren dazu, dass sich Monitoring-Landschaft, die einst von den "Big Four" (HP, CA, IBM und BMC) dominiert wurde, derzeit einer epochalen Veränderung befindet:

1. BMC wurde an eine Private-Equity-Firma verkauft
2. CA wurde von Broadcom übernommen und wird sich ausschließlich auf das Mainframe-Geschäft konzentrieren
3. IBM hat Tivoli vor fast einem Jahrzehnt übernommen, aber die Investitionen in Produktinnovationen sind kaum noch vorhanden
4. HP übergibt sein Kernportfolio an das Unternehmen Micro Focus

Daher müssen sich Unternehmen auf der ganzen Welt, die sich auf die "Big Four" verlassen haben, nach Ersatzanbietern umsehen. Auch wenn der Wechsel schockierend erscheint, ist diese Neubewertung des Marktes längst überfällig. Seit einigen Jahren sind viele große Monitoring Plattformen veraltet und wären schon längst ersetzt worden, wäre da nicht der Schmerz des "Rip and Replace" und des anschließenden Neuanfangs.

Weiters werden mit dem Aufkommen von Multiple Clouds, Containern und Microservices die "Big Four"-Plattformen weiter zunehmend in Frage gestellt, da diese Technologien die Plattformen über ihre Legacy-Fähigkeiten hinaus erweitern.

2.1 Der größte Kritikpunkt an den "Big Four" - mangelnde Flexibilität

Die "Big Four"-Plattformen, die oft als Flickenteppich aus zugekauften Produkten zitiert werden, machten es den Unternehmen aufgrund der unterschiedlichen Codebasen, Benutzeroberflächen und Datenformate schwer, ihre bestehende Technologie zu aktualisieren und zu integrieren. Während stückweise Korrekturen damit einhergehende Software-Updates das Problem vorübergehend beheben konnten und können, war dies aber keine langfristige, effiziente Lösung, um offensichtliche Lücken zu schließen und führte daher zu immer mehr Unzufriedenheit. Letztendlich kann nur eine Plattform, die einen ganzheitliches Monitoring bietet, die heute notwendigen und gewünschten Resultate liefern.

Wie Gartner in einem ihrer Forschungsartikel vom Juli 2018 mit dem Titel "Deliver Cross-Domain Analysis and Visibility With AIOps and Digital Experience Monitoring" schreibt:

"Monitoring-Lösungen bieten eine fragmentierte Schlüssellochansicht der IT-Realität. Jede Domäne, sei es eine Anwendung, ein Netzwerk oder eine Infrastruktur, wird überwacht, analysiert und manchmal sogar über automatisch generierte präskriptive Ratschläge behoben. Diese Prozesse finden jedoch pro Domäne statt und nicht ganzheitlich über digitale Business Services. Darüber hinaus haben die zunehmende Dynamik, die Modularität und die ephemere Natur moderner IT-Umgebungen diese Fragmentierung noch verstärkt. "

Gartner stellt weiter fest: "Trotz des Trends, diese Monitoring-Tools um neue Funktionen aus den anderen Domänen zu erweitern, können sie nicht die einheitliche Analyse liefern, die für den nachhaltigen Geschäftserfolg im heutigen und künftigen digitalen Geschäft erforderlich ist."

Unabhängig davon, ob es sich um eine Anwendungs-, Infrastruktur-, Netzwerk- oder virtualisierte Domäne handelt oder um eine neue Technologie, die noch gar nicht erdacht wurde, kann man sicher sein, dass die IT immer schneller, agiler und fehlerfreier arbeiten muss. Mit anderen Worten: Die IT wird ihren Weg in Richtung Automatisierung fortsetzen müssen.

2.2 Automatisierung als Zukunft der IT

Automatisierung funktioniert jedoch dann besonders gut, wenn sie Daten verwendet, die vereinheitlicht und kontextualisiert sind. Wie zu viele Unternehmen, die sich auf die "Big Four" verlassen haben feststellen, machen ihre Legacy-Plattformen und disparaten Tools die Automatisierung schwierig (oder fast unmöglich). Ohne jedoch verschiedenste Tools von Drittanbietern integrieren zu können ist die notwendige Automatisierung ein komplexes Unterfangen, das eine Menge teurer professioneller Dienstleistungen erfordert.

Eine effektive Überwachungsplattform im heutigen Ökosystem muss daher zumindest folgende Möglichkeiten bieten:

- Daten aus einem breiten Spektrum von Technologien zu sammeln (einschließlich der modernsten und dynamischsten) und dies mit einer Vielzahl von Erfassungsmethoden und nicht nur für Ereignisse. Sobald die Daten richtig gesammelt wurden, müssen diese auch kontextualisiert werden, damit sie als effektive Grundlage für die nachgelagerte Automatisierung dienen können.
- Eliminieren und/oder konsolidieren von bestehenden Tools und diese unter einen gemeinsamen Schirm bringen, damit die IT-Ops schneller Entscheidungen treffen kann. Laut einer EMA-AIOps-Umfrage aus dem Jahr 2018 verwendet das durchschnittliche Unternehmen 23 verschiedene Toolsets, um seinen Betrieb zu führen. Unnötig zu sagen, dass 23 verschiedene Toolsets mühsame Prozeduren zum Lesen, Extrahieren und Verarbeiten der Daten erfordern - ganz zu schweigen vom Personal- und Zeitaufwand.

Für die meisten Unternehmen bietet die Tool-Konsolidierung eine einfache Lösung für den Wildwuchs, der sich mittlerweile in ihrer Umgebung befindet. Während die Tool-Konsolidierung sicherlich ihre Vorzüge und Vorteile für ITOps bringt, liefert diese aber möglicherweise nicht die angestrebten Ergebnisse.

2.3 AI/ML für intelligenteres Arbeiten

Als direkte Reaktion auf die Notwendigkeit, rascher zu reagieren und die organisatorische Agilität zu erhöhen, führen Unternehmen in aller Eile verschiedenste Technologien und serverlose Architekturen ein, die die rasch einzurichten sind, aber auch rasch wieder verschwinden können. Diese technologischen Fortschritte stellen eine große Veränderung im Vergleich zu ihren bisherigen sesshaften Gegenstücken dar, aber sie bringen auch eine zusätzliche Ebene der betrieblichen Komplexität mit sich, da ihre flüchtige Natur es schwierig machen kann, zu verfolgen, ob sie in Betrieb oder inaktiv sind. Es gab einmal eine Zeit, in der man mit manuellen Prozessen den Aufenthaltsort eines Geräts nachweisen konnte, aber diese Zeiten sind im Zeitalter von Mobility, Fog Computing und 5G längst vorbei.

Dank der Weiterentwicklung moderner neuronaler Netze wie künstlicher Intelligenz und Maschinellem Lernen (ML) können Sie die ephemeren Technologien von heute nachverfolgen und eine Echtzeit-Inventur verwendeter Cloud(s), Anbieter und Tools vornehmen. Der wichtigste Vorbehalt ist jedoch die Fähigkeit, Veränderungen in Echtzeit zu sehen, also noch während diese stattfinden, anstatt sich auf eine abgelaufene Momentaufnahme der Vergangenheit zu verlassen.

Zusätzlich zu einer Echtzeit-Sicht auf Infrastruktur und Anwendungen müssen Unternehmen heute AI/ML-Technologie so einsetzen, dass sie automatisch erkennen und darstellen können, wie ihr IT-Ökosystem und ihre domänenübergreifenden Ressourcen zusammenarbeiten. Nur durch die Identifizierung der Beziehungen, die innerhalb des IT-Ökosystems stattfinden, können Unternehmen in der Lage sein, Möglichkeiten zur Automatisierung zu erkennen, die Servicebereitstellung verbessern, die Effizienz steigern und Risiken minimieren - und das alles bei gleichzeitiger Unterstützung der Leistung und Verfügbarkeit kritischer Services.

2.4 Verwendung neue Plattform statt der Legacy Big Four

Es ist eine Tatsache, dass niemand eine Big-Four-Plattform über Nacht ersetzen kann und will. Zum einen ist die Plattform wahrscheinlich zu sehr mit vorhandenen Technologien integriert und mit Mitarbeitern und Prozessen verwoben. Wie wahrscheinlich bei jedem Upgrade, gibt es in der Regel einen langsamen und langwierigen Prozess, bei dem man sich ansieht, was kaputt oder veraltet ist, und versucht, diese Probleme zuerst einzeln zu beheben, ohne gleich das gesamte System zu wechseln.

Um den großen Wechsel dann erfolgreich zu schaffen, sollten neue Monitoring Plattformen neben bestehenden Lösungen Legacy Lösungen eingesetzt werden können. Idealerweise sollte auch die Integration von Multi-Cloud- und hybride IT-Umgebungen unterstützen werden.

2.5 Von klassischem Monitoring zu Open Source basiertem Monitoring

Der vielleicht wichtigste Grund, mehr Geräte und Technologien auf Open Source Monitoring Systeme zu verlagern, ist die Abkehr von einer infrastrukturzentrierten Sichtweise der IT auf ein Management auf Business-Service-Ebene. Sobald die Daten von allen Elementen eines IT-Services oder Business Services neu aufgesetzt sind, erlaubt dies einen Echtzeit-Einblick in den Zustand, die Verfügbarkeit und die Risiken der bereitgestellten Kerndienste.

Was früher ein intensiver manueller Prozess war, kann jetzt schnell mit IT-Service-Ansichten erstellt und Änderungen genau verfolgt werden - und das noch dazu automatisch. Es können auch Dashboards für die Geschäftsleitung entwickelt werden, um Drilldowns durchzuführen und die technischen Metriken den Teams zugänglich zu machen, die sie benötigen, ohne die Ansichten für die Geschäftsleitung mit zu vielen undurchsichtigen Details zu überlasten.

2.6 Was versteht man unter Open-Source Software

Wenn wir über Open-Source-Software sprechen, beziehen wir uns normalerweise auf ein breiteres Konzept das generell freie und quelloffene Software genannt wird. Das Freie bezieht sich in diesem Zusammenhang eher auf Freiheit der eingesetzten Systeme als auf das Fehlen von Kosten. Bei freier und quelloffener Software hat jeder die freie Lizenz, die Software zu verwenden, zu kopieren, zu studieren und zu verändern, und der Quellcode wird offen zugänglich gemacht, so dass Menschen ermutigt werden, das Design der Software freiwillig zu verbessern. Dies unterscheidet sich von proprietärer oder Closed-Source-Software, bei der die Software unter einer restriktiven Copyright-Lizenz steht und der Quellcode typischerweise vor den Anwendern versteckt ist.

Einige Vorteile der Verwendung von freier und quelloffener Software sind geringere Softwarekosten, erhöhte Sicherheit und Stabilität, Schutz der Privatsphäre, Bildung und mehr Kontrolle über die eigene Hardware für die Anwender. Heute finden wir freie und quelloffene Software überall. Zum Beispiel sind Betriebssysteme wie Linux und Abkömmlinge von BSD weit verbreitet und treiben Millionen von Servern an. Lizenzen für freie Software und Open-Source-Lizenzen werden auch von vielen Softwarepaketen verwendet. Außerdem sind die Free-Software Bewegung und die Open-Source-Software-Bewegung mittlerweile soziale Online-Bewegungen, die zur Verbreitung von freier und quelloffener Software beitragen.

3 Der Vergleich von Open-Source und Closed-Source

Bei der Entscheidung für eine Open- oder Closed-Source-Überwachungslösung gibt es mehrere Faktoren zu berücksichtigen. Der Kostenfaktor - oder das Fehlen eines solchen - kann zwar ausschlaggebend sein, jedoch sollte man immer alle Aspekte in Betracht ziehen. Daher sollten wir die Vor- und Nachteile der beiden Ansätze in Bezug auf verschiedene Faktoren wie Preis, aber auch Support, Leistung und Zuverlässigkeit sowie Anpassungsmöglichkeiten vergleichen. Das sollte uns helfen zu entscheiden, welchen Weg wir gehen wollen.

3.1 Preis

Die meisten Open-Source-Überwachungstools sind kostenlos erhältlich. Sie können daher

einen offensichtlichen Kostenvorteil für Unternehmen bieten, da sie scheinbar keine finanzielle Investition erfordern. Dies ist jedoch nicht immer der Fall, und es ist nicht

ungewöhnlich, dass eine Open-Source-Überwachungslösung von den Anwendern verlangt, dass sie für zusätzliche oder zusätzliche Funktionalitäten zu bezahlen.

Obwohl sie nicht direkt mit den Kosten von Überwachungs-Tools zusammenhängen, sind andere Faktoren zu berücksichtigen wie rechtliche Fragen und Compliance-Vorschriften. Einige rechtliche Rahmenbedingungen verbieten die Verwendung von Open-Source-Software. Außerdem kann manche Open-Source-Software nur für nicht-kommerzielle Anwendungen verwendet werden. Diesen Punkt sollte man im Hinterkopf behalten, denn Verstöße könnten am Ende sehr teuer werden.

Was die Closed-Source-Überwachungstools betrifft, so bieten viele Anbieter - wenn auch nicht alle - eine kostenlose Testphase an die es ermöglicht, die Produkte zu testen und sicherzustellen, dass sie den Anforderungen entsprechen. Nach Ablauf der Testphase

bieten die meisten kostenpflichtigen Überwachungs-Tools verschiedene Zahlungsstufen oder -ebenen an, typischerweise basierend auf der Anzahl der zu überwachenden Schnittstellen, Knoten oder Geräte.

Der Markt hat sich in den letzten Jahren stark verändert. Vor einiger Zeit kaufte man typischerweise ein Überwachungstool von einem Wiederverkäufer. Heute sind viele Anbieter zu einem direkten E-Commerce-Modell übergegangen und verkaufen direkt an Kunden über ihre Websites. Ein Vorteil dieses Geschäftsmodells ist, dass man oft von verschiedenen Werbeaktionen der Anbieter profitieren kann. Man sollten eine schnelle Internetrecherche für alle anwendbaren Promotion Codes durchführen, die man nutzen können, vor allem gegen Ende eines Quartals, wenn die Anbieter ihre Umsatzziele erreichen wollen.

3.2 Support

Support ist oft der Bereich, in dem Open-Source-Software den schlechtesten Ruf hat. Ohne

eine große Organisation im Rücken, ist es richtig, dass "offizieller" Support bei Open-Source-Software oft leider nicht vorhanden ist. Jedoch ist es die Unterstützung der Gemeinschaft, wo dieses Modell seine absoluten Stärken hat. Online-Support-Foren, die von der Gemeinschaft unterstützt werden, sind oft verfügbar und, obwohl Sie sicherlich kein Service Level Agreement (SLA) erhalten, ist die Unterstützung, die man von diesen Quellen erhält, oft ausreichend.

Man sollte sich bewusst sein, dass der Support für Open-Source-Software - und nicht nur für Überwachungs-Tools sehr unterschiedlich ist. Benötigt man unbedingt felsenfesten Support sollte man sicherstellen, dass die Hausaufgaben erledigt sind und der benötigte Support im Bedarfsfall auch geleistet wird.

Kostenpflichtige Lösungen hingegen bieten in der Regel einen Support, der durch Faktoren wie eine organisierte Struktur mit Agenten, SLAs oft rund um die Uhr Verfügbarkeit gegeben ist Man kann davon ausgehen, dass jedes Problem, das auftritt, schnell und zur vollen Zufriedenheit gelöst wird. Allerdings variiert der angebotene Support von Anbieter zu Anbieter sehr stark.

Dies ist ein Bereich, den man genau prüfen sollte, wenn Support eine hohe Priorität hat.

Außerdem bieten die Hersteller von Closed-Source-Überwachungswerkzeugen in der Regel eine bessere Dokumentation an als ihre Open-Source-Gegenstücke, was den Bedarf und die Notwendigkeit an Support schon im Vorhinein reduziert. Und genau wie im Open-Source-Bereich haben auch einige Closed-Source Software-Plattformen Community-gesteuerte Foren, in denen Benutzer Tipps austauschen und sich gegenseitig helfen.

3.3 Leistung und Verlässlichkeit

Leistung und Zuverlässigkeit ist wahrscheinlich der Bereich, in dem es die geringsten Unterschiede zwischen Open- und Closed-Source-Software gibt. Einige werden argumentieren, dass die Leistung von Open-Source-Tools größtenteils von den Beiträgen der Community abhängt und daher unmöglich so gut sein kann wie Closed-Source, das typischerweise von kommerziellen Interessen angetrieben wird. Andere werden sagen, dass Open-Source-Software häufiger aktualisiert und gepatcht werden muss.

Die Erfahrung zeigt jedoch, dass nichts davon stichhaltig ist. Es gibt grundsolide Open-Source-Software und absolut schlechte kommerzielle. Von einer großen kommerziellen Organisation unterstützt zu werden garantiert in keiner Weise Qualität, Leistung oder Zuverlässigkeit. Es gibt gute Software und schlechte Software, genauso wie es Open-Source- und Closed-Source-Software gibt, aber es gibt absolut keine Korrelation zwischen den beiden.

Natürlich ist kommerzielle Closed-Source-Software in der Regel einfacher zu bedienen und ausgefeilter als die Open-Source-Software. Schließlich müssen ihre Hersteller etwas haben, um Kunden zu überzeugen, riesige Summen Geld auszugeben. Aber auch das muss notwendigerweise nicht unbedingt der Realität entsprechen.

3.4 Anpassungsfähigkeit

Open-Source-Software gibt Endbenutzern Zugriff auf den Quellcode. Das wiederum erlaubt die Software an spezielle Bedürfnisse anzupassen. Auf den ersten Blick mag das als die ultimative Stufe der Anpassung erscheinen, man muss allerdings bedenken, dass das Anpassen von Open-Source-Software auch das Schreiben von Code erfordert, was natürlich entsprechende Kenntnisse voraussetzt.

Im Gegensatz dazu bietet Closed-Source-Software oft verschiedene Stufen der Anpassung, die angewandt werden können, ohne dass man Code schreiben müssen. Man kann zwar nicht einfach extra Funktionalität hinzufügen aber oft können kleine Anpassungen über vorhandene Dashboards durchgeführt werden.

4 Was ist mit Sicherheit?

Ob Open-Source-Software - oder Closed-Source-Software sicherer ist bleibt eine offene und wahrscheinlich nie endende Diskussion. Kritiker von Open-Source-Software argumentieren oft, dass solche Software durch die Offenlegung des Quellcodes angreifbarer ist. Die Erfahrung zeigt jedoch, dass für quelloffene Software im Allgemeinen weniger Malware geschrieben wird. Außerdem argumentieren die Befürworter von Open-Source-Software, dass es weniger Exploits gibt, da häufiger Patches durchgeführt werden und auch die große Anzahl der Entwickler ständig zur Sicherheit des Projekts beitragen.

Es wird jedoch oft argumentiert, dass Closed-Source-Software sicherer ist, da diese in einer kontrollierten Entwicklungsumgebung bei einem vertrauenswürdigen Anbieter entsteht. Das nächste Argument ist dann, dass, wenn eine Sicherheitslücke entdeckt wird, zuverlässig Entwickler rasch daran arbeiten diese Lücke zu finden, rasch Patches und Updates zur Verfügung zu stellen um letztlich ihre Kunden vor Problemen zu bewahren. Vereinfacht gesagt wird dann wird mit dem hohen Sicherheitsaufwand argumentiert, der in Closed-Source-Lösungen gesteckt wird, mit dem angeblich Open-Source Lösungen nicht mithalten können.

Ob das in den meisten Fällen tatsächlich der Wahrheit entspricht, sei dahingestellt und sollte in jedem Fall individuell beantwortet werden. Sicher ist, dass Open-Source Lösungen heute dank der großen Community die dahinter steht oft wesentlich rascher, flexibler und letztendlich dann auch sicherer sind als Closed-Source-Lösungen bei denen das Finden und Beseitigen von Problemen sehr oft lange dauert und man von den Herstellern abhängig ist die nur dann tatsächlich an Lösungen arbeiten, wenn ihre Kunden den Druck erhöhen.

5 Die besten Open-Source Monitoring Tools (und einige Closed-Source Alternativen)

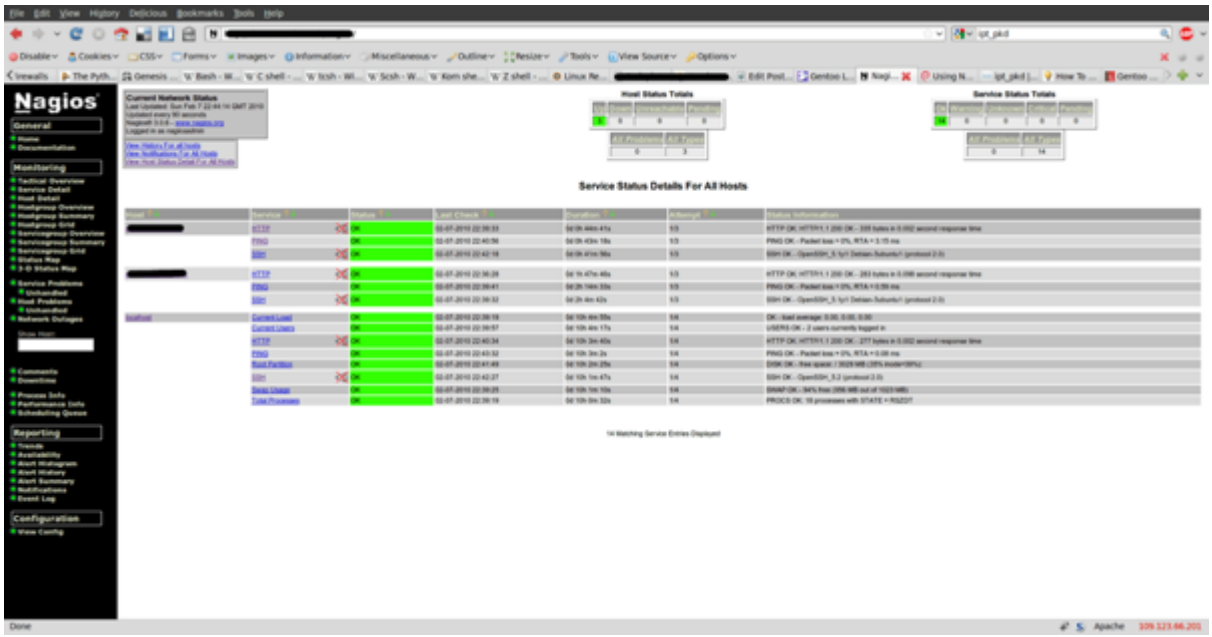
Wenn man den aktuellen Markt nach einigen der besten Open-Source-Monitoring-Tools durchforstet, findet man, dass bereits eine Menge derartige Tools zur Verfügung stehen.

Aber um die Sache besser abzurunden werden wir auch einige kommerzielle Alternativen betrachten. Man sollte sich keine Feature-für-Feature Übereinstimmung zwischen Open-Source und Kommerziellen Alternativen erwarten, denn alle Monitoring Werkzeuge sind sehr unterschiedlich und daher gleichen auch keine 2 Möglichkeiten einander in allen oder den meisten Punkten. Stattdessen beziehen die Vergleiche auf die allgemeine Qualität der einzelnen Werkzeuge.

5.1 Nagios Core

Nagios ist eines der ältesten und etabliertesten Netzwerküberwachungssysteme auf dem Markt. Seine freie Open-Source-Version - Nagios Core - kann als eine großartige Ressource für jede Organisation dienen. Es sind zwei Versionen von Nagios verfügbar. Es gibt das kostenlose und quelloffene Nagios Core und das kostenpflichtige Nagios XI. Beide nutzen die gleiche zugrunde liegende Engine, aber die Ähnlichkeit hört dort auf.

Nagios Core ermöglicht es Anwendern, den Status jedes Hosts und jedes Dienstes, der zu einem Netzwerk gehört, in Echtzeit zu überwachen. Es bietet außerdem verschiedene Arten von Alarmen, um Administratoren zu helfen, Probleme schneller zu lösen und ist in hohem Maße anpassbar. Leider kann der Dienst einschränkend sein. Seine Textbox-Konfiguration und veraltete Web-Oberfläche können bei der Verwaltung frustrierend sein. Da der Dienst jedoch schon so lange im Einsatz ist, finden man jedoch meistens online Community-Support für alle auftretenden Probleme.

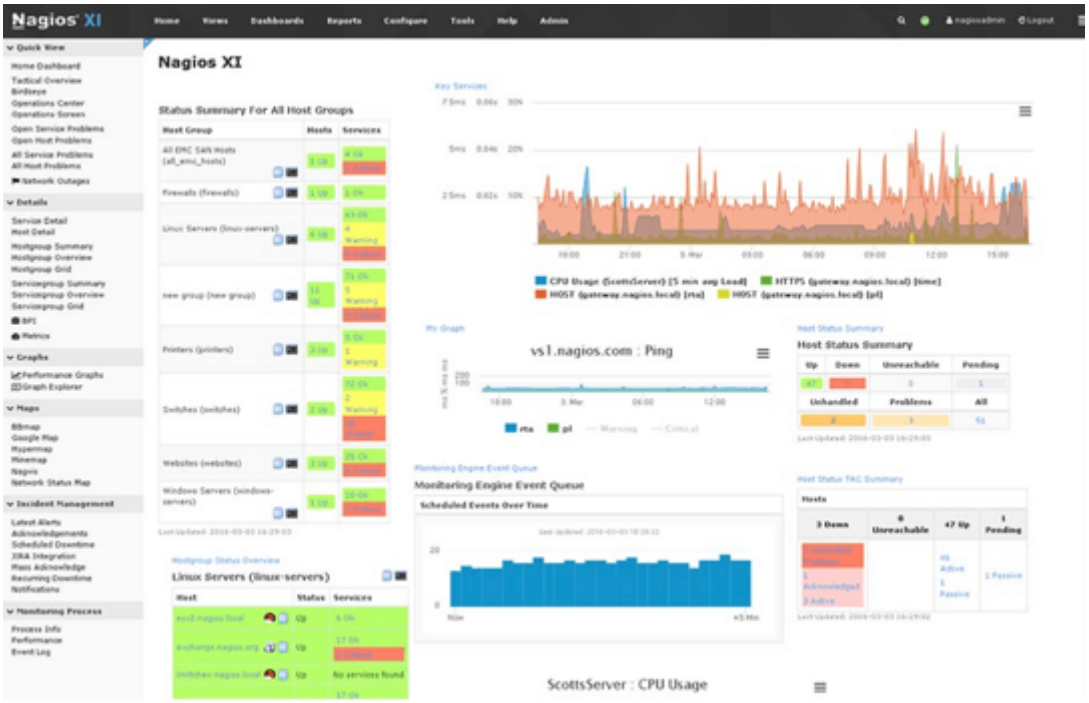


Der modulare Ansatz geht weit über das Backend des Tools hinaus. Das Frontend des Werkzeugs ist genauso modular, wenn nicht noch mehr. Verschiedene von der Community entwickelte Frontend-Optionen stehen ebenfalls zum Download bereit. Der Nagios Core, die Plugins und das Frontend bilden zusammen ein ziemlich komplettes Überwachungssystem. Dieses modulare Konzept hat allerdings auch einen Nachteil, denn das Einrichten von Nagios Core kann sich als eine anspruchsvolle Aufgabe herausstellen. Dies wird jedoch teilweise durch den verfügbaren Community-Support kompensiert.

5.2 Kostenpflichtige Alternative Nacios XI

Nagios XI ist eine unternehmenstaugliche Server- und Netzwerküberwachungssoftware, die eine umfassende Überwachung von Anwendungen, Diensten und Netzwerken in einer zentralen Lösung bietet. Das Produkt ist ein direkter Nachfahre von Nagios Core und verwendet die gleiche Core Engine. Mit diesem Produkt können alle geschäftskritischen Infrastrukturkomponenten überwachen, wie Anwendungen, Dienste, Betriebssysteme, Netzwerkprotokolle, Systemmetriken und Netzwerkinfrastruktur.

Die leistungsfähigen Dashboards von Nagios XI bieten auf einen Blick Zugriff auf leistungsstarke Überwachungs Informationen und Daten von Drittanbietern. Verschiedene Ansichten ermöglichen dem Benutzer einen schnellen Zugriff auf die Informationen, die man am nützlichsten finden. Das GUI des Tools ist in hohem Maße anpassbar und sein Layout, das Design und die Einstellungen des Tools können benutzerspezifisch angepasst werden.



Nagios XI ist sehr einfach zu bedienen, dank der integrierten webbasierten Konfigurationsoberfläche mit der Administratoren die Überwachungskonfiguration, Systemeinstellungen und vieles mehr verwalten können. Die Plattform bietet außerdem Konfigurationsassistenten, die den Benutzer durch den Prozess der Überwachung neuer Geräte, Dienste und Anwendungen zu führen, ohne dass sie komplexen Überwachungskonzepten.

Nagios XI ist in einer Standard Edition und einer Enterprise Edition erhältlich.

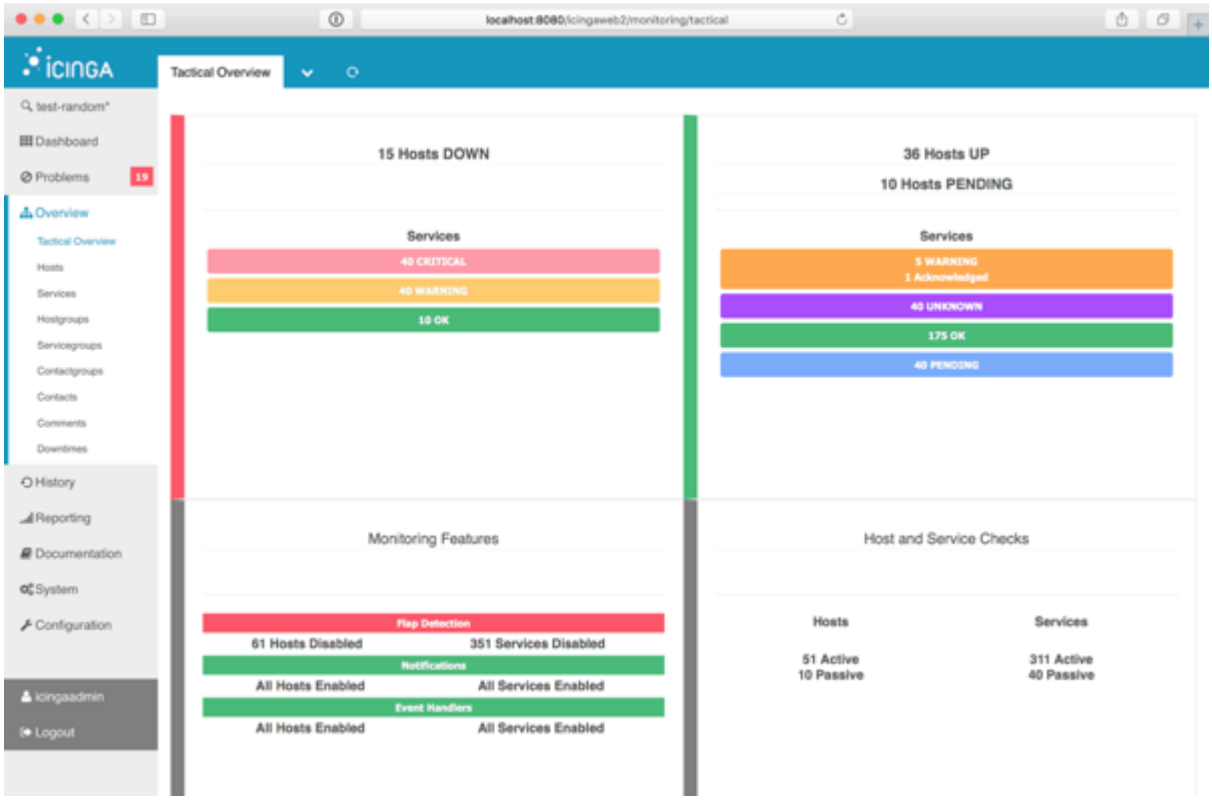
Die Enterprise Edition bietet zusätzliche Funktionalität und beinhaltet Features für die Unterstützung von groß angelegter Konfiguration, Prognosen und zeitgesteuerte Berichterstellung. Jede Lizenz beinhaltet zwölf Monate Wartung und E-Mail-Support.

5.3 Icinga

Icinga ging als Produkt der Nagios-Entwickler hervor, die der Nagios Core Suite mehr Funktionalität hinzufügen wollten. Seit seiner Abspaltung von der Muttergesellschaft hat es sich als leistungsfähiges Überwachungswerkzeug mit einer Reihe von wünschenswerten Funktionen entwickelt. Es ist einfach zu installieren, und seine grundlegenden Überwachungsfunktionen sind leicht zu konfigurieren.

Es gibt sowohl eine Core-Installation, als auch eine Web-Installation. Icinga verwendet textbasierte Konfigurationsdateien, und in Anbetracht des robusten Kerns entpuppt es sich als sehr mächtig und flexibel.

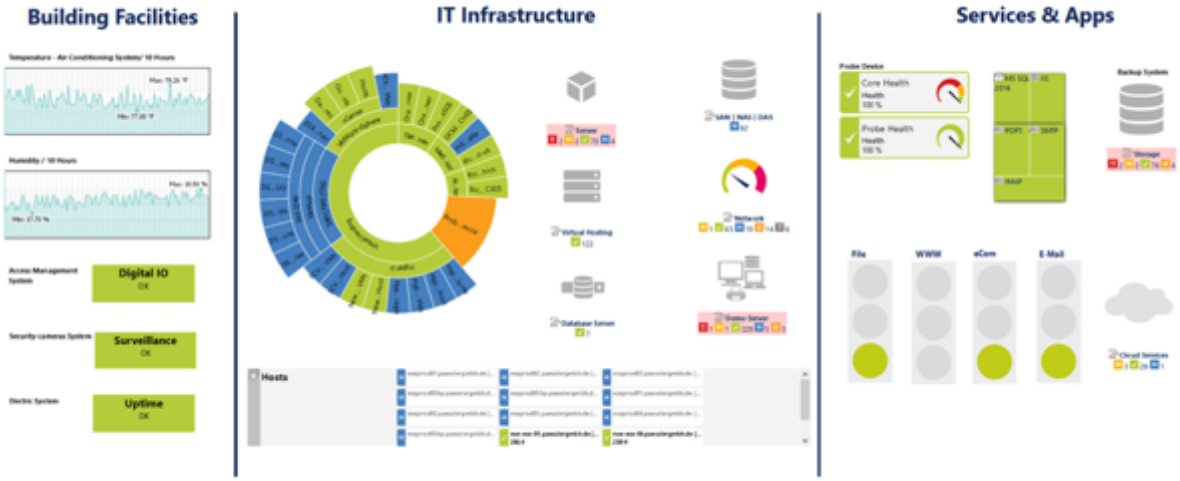
Icinga ist eine hervorragende Überwachungsplattform. Sie hat eine einfache und saubere Benutzeroberfläche und, was noch wichtiger ist, einen Funktionsumfang, der es mit einigen kommerziellen Produkten aufnehmen kann. Wie die meisten Bandbreitenüberwachungsplattformen verwendet diese SNMP, um Daten zur Bandbreitenauslastung von Netzwerkgeräten abzurufen und zu berechnen. Aber einer der Bereiche, in denen dieses Tool besonders hervorsticht, ist die Verwendung von Plugins. Es gibt Tausende von in der Community entwickelten Plugins die verschiedene Überwachungsaufgaben übernehmen können und so die Funktionalität des Produkts erweitern. Und für den unwahrscheinlichen Fall, dass man nicht das richtige Plugin für seine individuellen Bedürfnisse findet, kann man selbst eines schreiben und es der Community zur Verfügung stellen.



Alerting und Benachrichtigung gehören ebenfalls zu den besten Funktionen von Icinga. Alarme sind vollständig konfigurierbar in Bezug darauf, was sie auslöst und wie sie übermittelt werden. Das Tool bietet auch die so genannte segmentierte Alarmierung. Mit dieser Funktion kann man einige Alarme an eine Gruppe von Benutzern und andere Alarme an andere Personen senden. Dies ist nützlich, wenn verschiedene Systeme überwacht werden, die von unterschiedlichen Teams verwaltet werden. Es kann sicherstellen, dass Alarme nur an die richtige Gruppe gesendet werden.

5.4 Kostenpflichtige Alternative: PRTG Network Monitor

Der PRTG Network Monitor der Paessler AG ist ein großartiges Produkt. Es ist im Prinzip ein SNMP-Überwachungswerkzeug. Dank eines Konzepts namens Sensoren - eine Art von Plug-ins, die bereits in das Produkt integriert sind, können zusätzliche Metriken überwacht werden. Es gibt etwa zweihundert Sensoren, die mit dem Produkt verfügbar sind. Laut Paessler kann man es in ein paar Minuten einrichten. Auch wenn es nicht so schnell geht, so ist es doch schneller als die meisten Mitbewerbern, unter anderem dank der automatischen Erkennung des Tools.



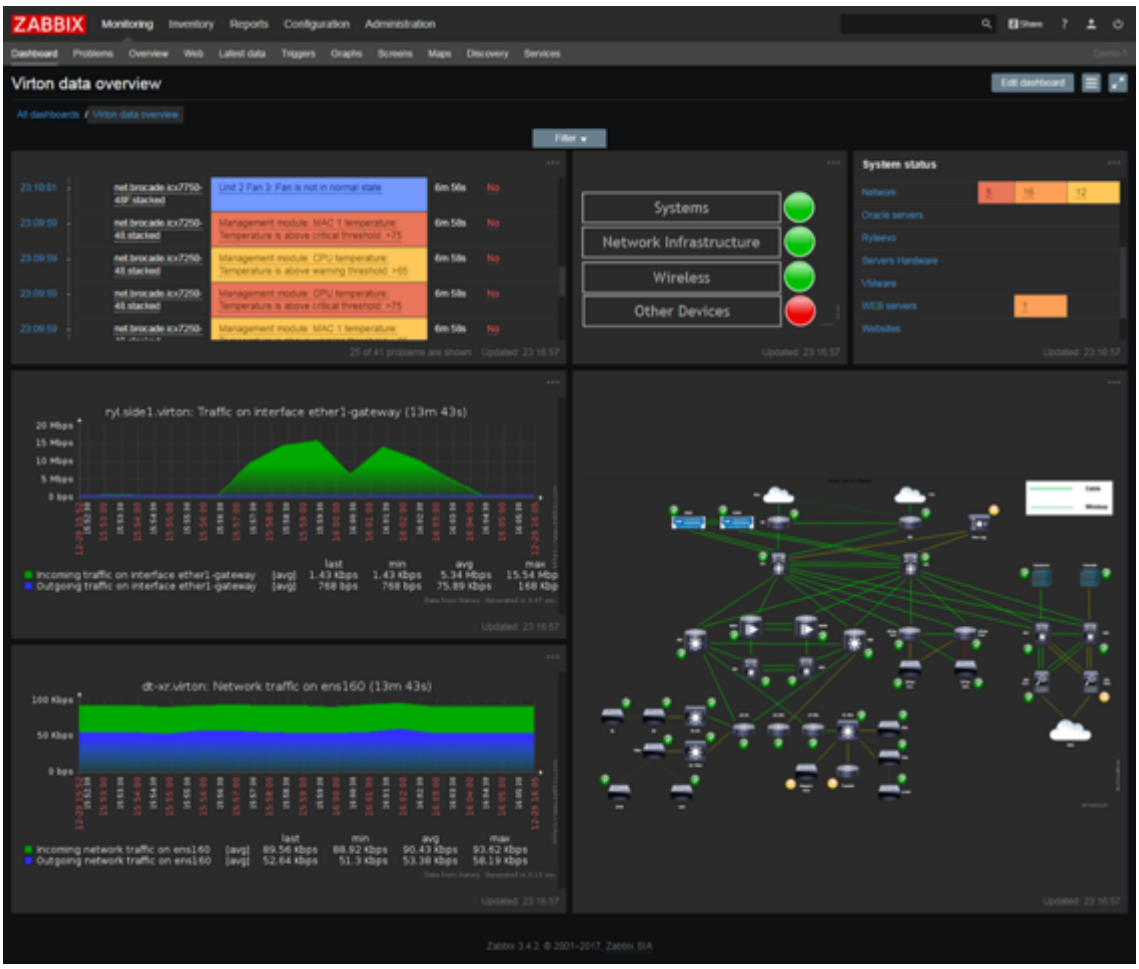
PRTG ist ein funktionsreiches Produkt, bei dem man zwischen einer nativen Windows Enterprise-Konsole, einer Ajax-basierten Web-Oberfläche und mobilen Apps für Android und iOS wählen kann. Sowohl die Alarmierung als auch die Berichterstellung sind hervorragend und das Produkt verfügt über eine große Auswahl an Berichten die als HTML oder PDF angezeigt oder zur externen Weiterverarbeitung in CSV oder XML exportiert und extern weiterverarbeitet werden können.

PRTG ist in einer kostenlosen Version erhältlich, mit einer Überwachung von maximal 100 Sensoren. Jeder Parameter, den man überwachen möchten, zählt als ein Sensor. Ein Beispiel, die Überwachung der Bandbreite auf jeder Schnittstelle eines 4-Port-Routers sind 4 Sensoren und die Überwachung der CPU und des Speichers desselben Routers beansprucht 2 weitere Sensoren. Jeder zusätzliche Sensor, den man installieren, zählt ebenfalls. Für mehr als 100 Sensoren - die man höchstwahrscheinlich benötig, benötigen man eine Lizenz.

5.5 Zabbix

Wie Nagios gibt es auch Zabbix schon seit langer Zeit. Manche finden dieses Open-Source-Netzwerküberwachungtool einfacher zu handhaben als andere Open-Source-Tools, da es viele Out-of-the-Box-Funktionen bietet. Dies bedeutet, dass die Benutzer sich nicht mit einer Flut von Plugins herumschlagen müssen.

Obwohl Zabbix eine ausgereifte Plattform auf Unternehmensebene ist, die eine Echtzeit-Überwachung von Metriken in großen Netzwerken bietet, sind die Anzeigen zur Problemerkennung und Metriksammlung nicht einfach konfigurierbar. Und obwohl es skalierbar ist - was es zu einer guten Lösung für komplexe Netzwerke macht - ist es ein wenig schwieriger zu implementieren als andere Lösungen.

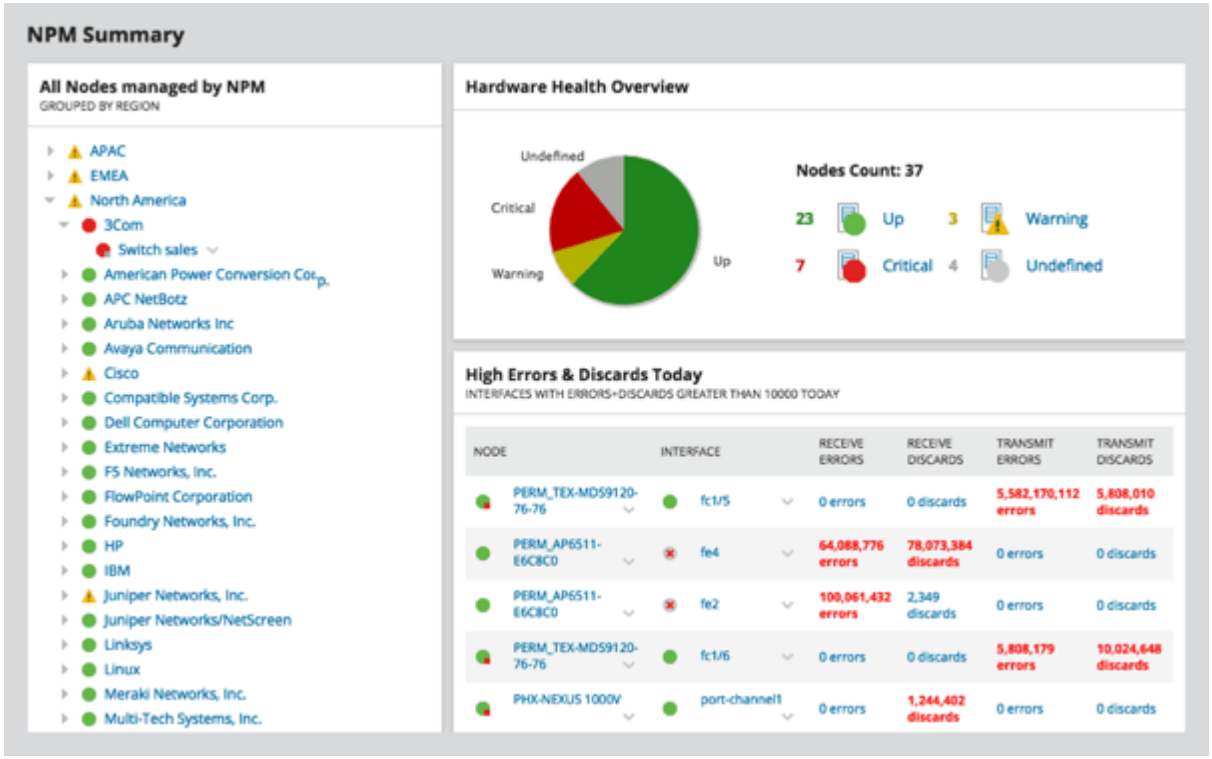


Zabbix verwendet sowohl SNMP als auch das Intelligent Platform Monitoring Interface (IMPI) zur Überwachung von Geräten. Mit der Software können die Bandbreite, die CPU- und Speicherauslastung, der allgemeinen Gerätezustand und die Leistung sowie Konfigurations Änderungen angezeigt werden, eine ziemlich einzigartige Funktion innerhalb dieser Liste. Dieses Tool kann weit mehr als nur die Überwachung der Netzwerk-Bandbreitenauslastung. Es verfügt auch über ein beeindruckendes und vollständig anpassbares Warnsystem, das nicht nur E-Mail- oder SMS-Warnungen verschickt, sondern auch lokale Skripte ausführt, mit denen einige Probleme automatisch behoben werden können.

5.6 Kostenpflichtige Alternative: SolarWinds Network Performance Monitor

SolarWinds, der Hersteller des Network Performance Monitors, existiert bereits seit 20 Jahren und genießt den Ruf, einige der besten Netzwerk- und Systemadministrations-Tools zu entwickeln. Viele der Produkte des Unternehmens haben begeisterte Kritiken erhalten und zählen zu den besten in ihren jeweiligen Bereichen. Das Unternehmen ist auch berühmt für seine kostenlosen Tools, die jeweils einen bestimmten Bedarf von Netzwerkadministratoren adressieren.

Der SolarWinds Network Performance Monitor ist in erster Linie eine SNMP-Bandbreiten Überwachung, aber er kann noch viel mehr. Im Kern bietet das Produkt ein umfassendes Fehlerüberwachungs- und Leistungsmanagement mittels SNMP und ist damit mit den meisten Geräten kompatibel. Mit der NetPath-Funktion des Tools kann man auch den kritischen Netzwerkpfad zwischen zwei beliebigen überwachten Punkten in Ihrem Netzwerk anzeigen.



Weitere Stärken des Produkts sind die erweiterte Alarmierung und das PerfStack Dashboard zur Leistungsanalyse. Eine weitere exklusive Funktion ist die Network Insights Funktionalität, die eine komplexe Geräteüberwachung ermöglicht. Das Tool kann auch überwachen Software Defined Networks (SDN) überwachen und verfügt über integrierte Cisco ACI-Unterstützung sowie die Fähigkeit drahtlose Netzwerke zu überwachen und Netzwerk-Performance-Baselines zu generieren.

Der SolarWinds Network Performance Monitor hat eine recht einfache Preisstruktur.

Die Lizenzierung basiert auf der Anzahl der überwachten Elemente. Fünf Lizenzierungsstufen sind für 100, 250, 500, 2000 und unbegrenzte Elemente verfügbar.

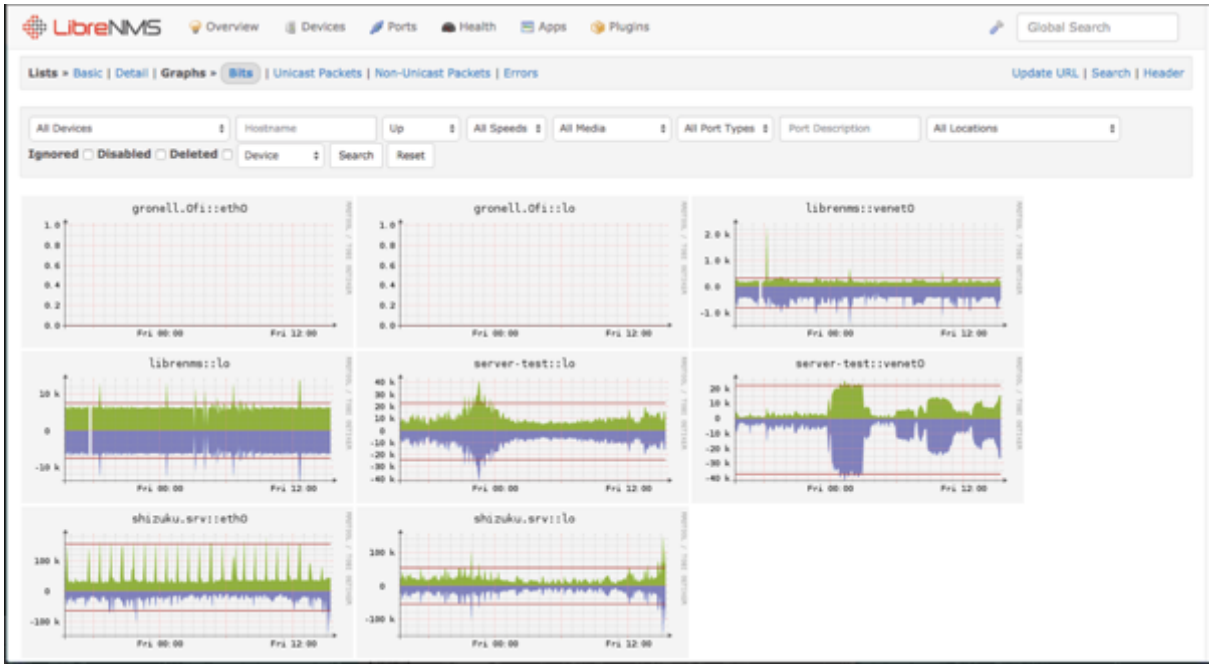
5.7 LibreNMS

LibreNMS ist eine Open-Source-Portierung von Observium, einer sehr potenten kommerziellen Netzwerk Überwachungsplattform. Es ist ein voll ausgestattetes Netzwerküberwachungssystem, das eine Fülle von Funktionen und Geräteunterstützung bietet. Eine der besten Eigenschaften ist die automatische Erkennungs Engine, die sich nicht nur auf SNMP verlässt, um Geräte zu finden. Es kann automatisch ein gesamtes Netzwerk mit CDP, FDP, LLDP, OSPF, BGP, SNMP und ARP erkannt werden. Was die Automatisierungsfunktionen des Tools betrifft, so verfügt es auch über automatische Updates, so dass es immer aktuell bleibt.

LibreNMS verwendet das Simple Network Management Protocol (SNMP), was bedeutet, dass auf den zu überwachenden Geräten SNMP-Agenten installiert oder aktiviert sein müssen. Es unterstützt eine breite Palette von Betriebssystemen, darunter Linux und FreeBSD, sowie Netzwerkgeräte von Cisco, Juniper, Brocade, Foundry und Hewlett-Packard, was es zu einer der besten verfügbaren Open-Source-SNMP-Überwachungssoftware macht.

Die besten Eigenschaften sind das Auto-Discovery-System und die benutzerdefinierte Alarmierung, die dem Benutzer viel Autonomie bei der Überwachung bieten. Außerdem verfügt es über eine mobilfreundliche Web-Benutzeroberfläche mit anpassbaren Dashboards, die den Benutzern den Zugriff von unterwegs erleichtern.

Leider kann LibreNMS ohne integrierte Cloud-Integration den lokalen Speicher stark beanspruchen. Und da es keine kostenpflichtige Option gibt, kann es fast unmöglich sein, Support zu bekommen, wenn Probleme auftreten.



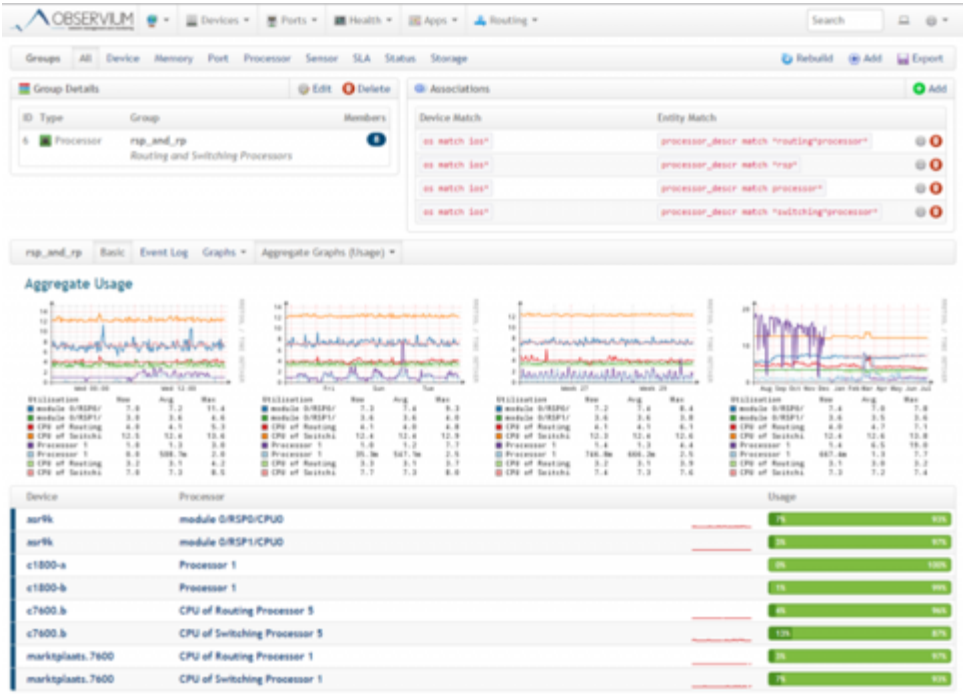
Ein weiteres wichtiges Merkmal des Produkts ist sein hochgradig anpassbares Alarmierungsmodul. Es ist sehr flexibel und kann Alarmbenachrichtigungen über mehrere Technologien senden, z. B. per E-Mail, wie die meisten seiner Konkurrenten, aber auch IRC, Slack und mehr. Wenn Sie ein Service-Provider sind oder Ihre Organisation jeder Abteilung die Nutzung des Netzwerks in Rechnung stellt, wird die Abrechnungsfunktion des Tools interessant. Es kann Bandbreitenrechnungen für Segmente eines Netzwerks basierend nach Nutzung oder Übertragung erstellen.

Bei größeren Netzwerken und verteilten Organisationen ermöglichen die verteilten Polling-Funktionen von LibreNMS eine horizontale Skalierung, um mit Ihrem Netzwerk zu wachsen. Eine vollständige API ist ebenfalls vorhanden die es ermöglicht, Daten aus der Installation zu verwalten, grafisch darzustellen und abzurufen. Schließlich sind mobile Apps für iPhone und Android verfügbar, ein ziemlich einzigartiges Feature bei Open-Source Werkzeuge.

5.8 Observium

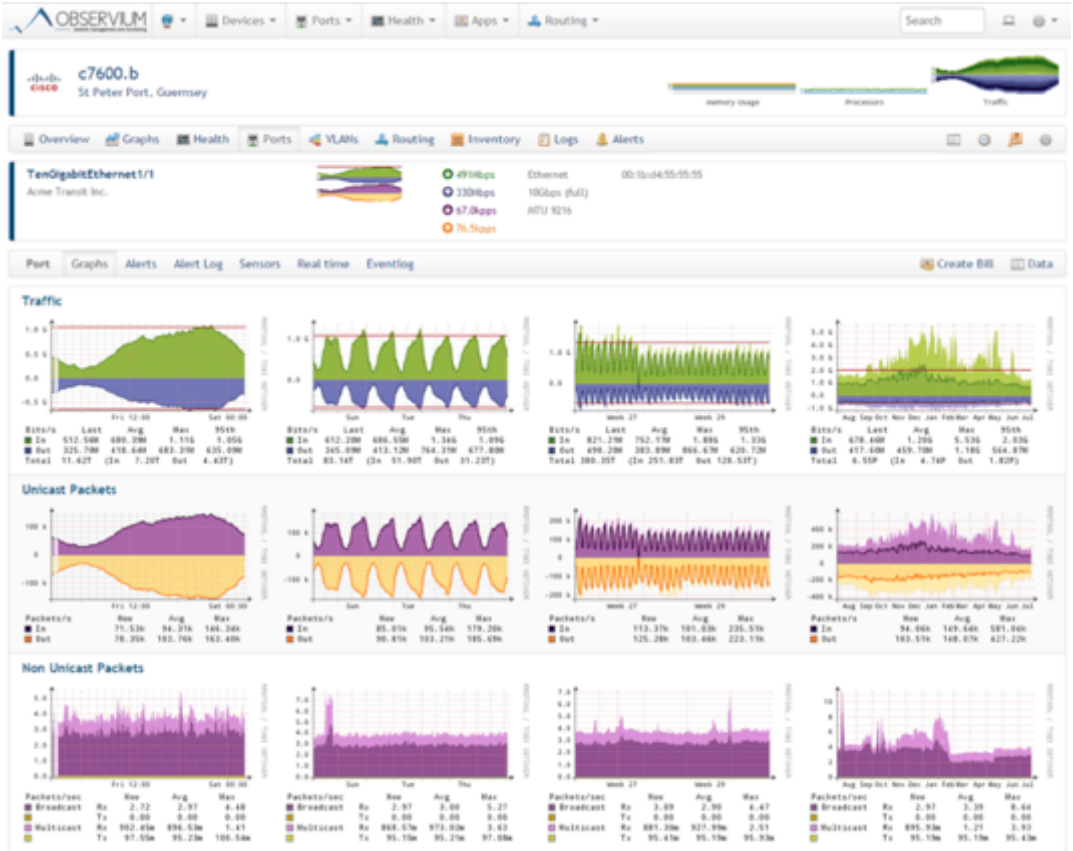
In Bezug auf Open-Source-Tools mit Auto-Discovery-Funktionen ist Observium eine der wartungsärmeren Netzwerk-Überwachungslösungen. Es unterstützt eine breite Palette von Gerätetypen, Plattformen und Betriebssystemen, darunter Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, NetScaler und NetApp.

Observium konzentriert sich vor allem darauf, eine einfache und intuitive Oberfläche anzubieten. Dies ist hilfreich für kleinere Organisationen, die Einblicke in den Zustand und Status ihrer Netzwerke erhalten wollen. Es hat auch ein einheitliches Web-Interface, so dass die Benutzer von überall aus einfach auf Kontrollen zugreifen und Netzwerkstatus und -statistiken einsehen können. Allerdings ist Observium in der kostenlosen Version nicht skalierbar, und der Support von ist sehr mangelhaft.



5.9 Kostenpflichtige Alternative: Observium Professional

Observium ist eine wartungsarme Monitoring-Plattform mit Auto-Discovery. Sie unterstützt eine Vielzahl von Gerätetypen, Plattformen und Betriebssystemen, u.a., Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp. Der primäre Fokus des Tools ist eine schöne, intuitive und einfache, aber leistungsfähige Benutzeroberfläche zu bieten, die den Zustand und Status des Netzwerks zeigt.



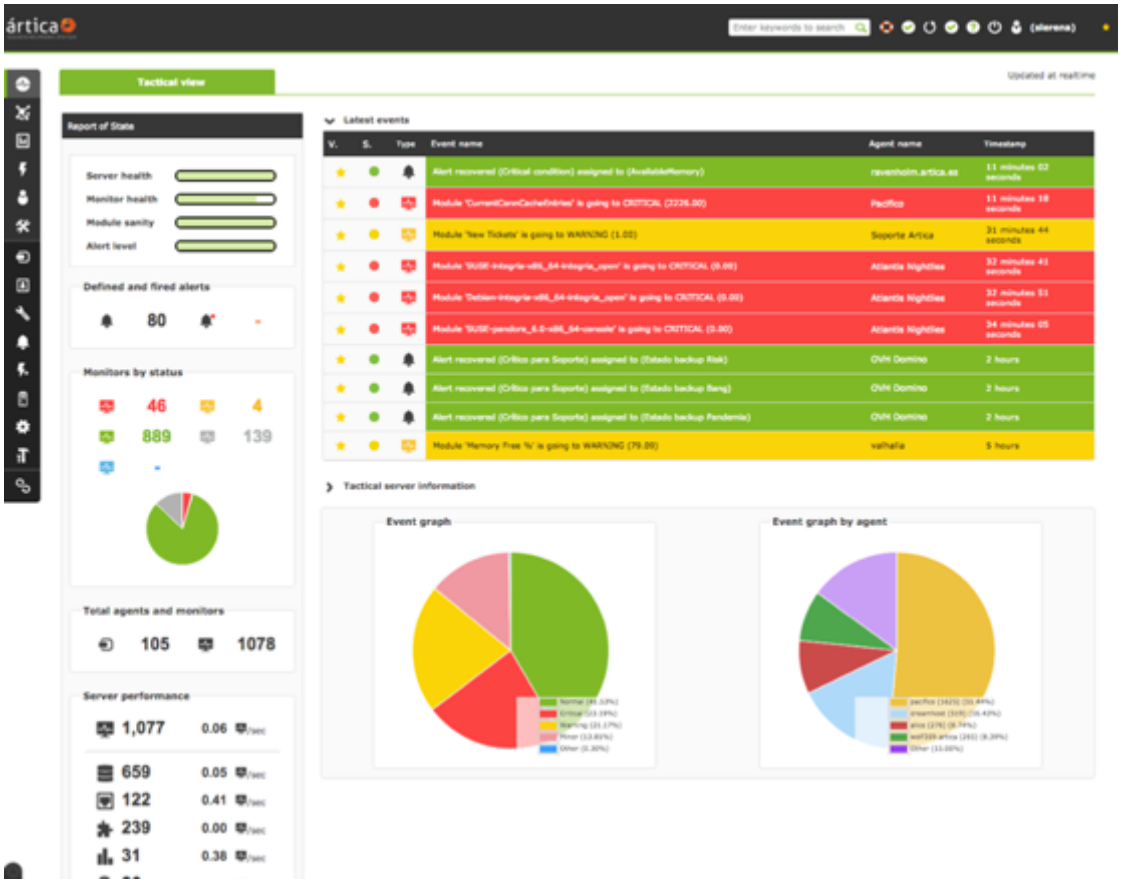
Observium bietet mehr als nur Bandbreitenüberwachung. Zum Beispiel gibt es ein Abrechnungssystem, das die gesamte monatliche Bandbreitennutzung im 95.Perzentil oder in insgesamt übertragenen Bytes misst. Es hat auch eine Alarmierungsfunktion mit benutzerdefinierten Schwellenwerten. Darüber hinaus lässt sich das Produkt mit anderen Systemen integrieren und kann deren Informationen abrufen und in seiner Oberfläche anzeigen.

Es ist einfach einzurichten und konfiguriert sich fast von selbst. Obwohl es auf der Website des Herausgebers keinen Download-Bereich zu geben scheint, gibt es detaillierte Installationsanweisungen für verschiedene Linux-Distributionen, die auch die Links, um das richtige Paket für jede Distribution zu erhalten. Die Anweisungen sind sehr detailliert und die Installation der Software sollte einfach sein.

5.10 Pandora FMS

Pandora FMS ist ein Open-Source-Überwachungstool für das IT-Infrastrukturmanagement. Es zeichnet sich als eine der flexibleren Überwachungslösungen auf dem Markt aus, meist ideal für mittlere und große Umgebungen (100 Geräte oder mehr).

Mit Pandora FMS können Anwender jedes Gerät, jede Infrastruktur, jede Anwendung oder jeden IT- und Geschäftsprozess oder Dienst überwachen. Und weil die Software zentralisiert und einfach zu navigieren ist, ist sie ein nützliches Werkzeug für Unternehmen um ihre Überwachungsberichte mit technisch nicht versierten Mitarbeitern zu teilen. Allerdings neigt es zu Fehlern, und obwohl das Support-Team für die Unternehmenslösung schnell Patches bereitstellt, kann es bei Open Source Bugs eine Weile dauern, bis sie behoben sind.



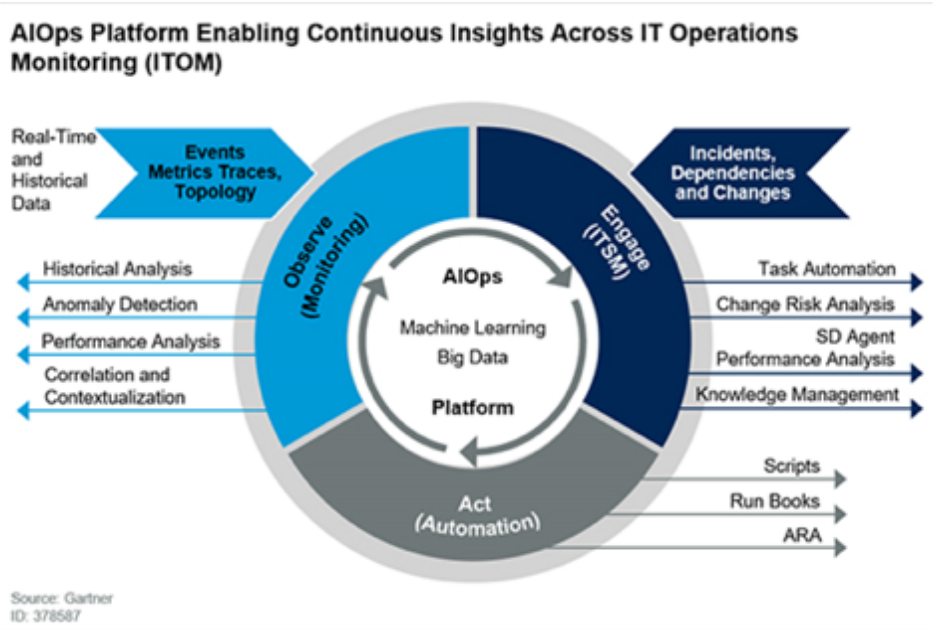
6 AIOps

Artificial Intelligence (AI) treibt den nächsten Innovationszyklus in der Unternehmenssoftware voran, ermöglicht ein neues Maß an intelligenter Automatisierung und vertikaler Integration. Da die heutigen Unternehmenssysteme immer größer werden, gehen die Vorteile von Digitalisierung und Cloud Computing mit technologischer Komplexität und betrieblichen Risiken einher. AI-gestützte Software-Intelligenz verspricht diese Herausforderungen zu bewältigen und eine neue Generation von autonomen Cloud-Unternehmenssystemen zu unterstützen indem es autonome Abläufe ermöglicht, sowie Innovationen fördert und damit neue Formen der Kundenbindung durch vollständige Automatisierung ermöglicht.

6.1 Was bedeutet AIOps

AIOps ist die Abkürzung für Artificial Intelligence for IP Operations (Künstliche Intelligenz für den IT-Betrieb). Es bezieht sich auf mehrschichtige Technologieplattformen, die den IT-Betrieb durch Analysen und maschinelles Lernen (ML) automatisieren und verbessern. Eine gute Erklärung für die Funktionsweise von AIOps liefert Gartner mit folgender Definition (siehe auch Diagramm):

AIOps-Plattformen nutzen Big Data, modernes maschinelles Lernen (ML) und andere fortschrittliche Analysetechnologien, um IT-Betriebsfunktionen (Überwachung, Automatisierung und Service Desk) direkt und indirekt durch proaktive, persönliche und dynamische Einblicke zu verbessern. AIOps-Plattformen ermöglichen die gleichzeitige Nutzung mehrerer Datenquellen, Datenerfassungsmethoden, Analysetechnologien (in Echtzeit und in der Tiefe) und Präsentationstechnologien.



AIOps hat zwei Hauptkomponenten: Big Data und ML. Es erfordert eine Abkehr von siloartigen IT-Daten, um Beobachtungsdaten (wie sie in Überwachungssystemen und Job-Protokollen zu finden sind) zusammen mit Eingriffsdaten (die normalerweise in Ticket-, Incident- und Event-Aufzeichnungen zu finden sind) innerhalb einer Big-Data-Plattform zu aggregieren.

AIOps implementiert eine umfassende Analytik- und ML-Strategie für die kombinierten IT-Daten. Das gewünschte Ergebnis sind dann automatisierungsgesteuerte Erkenntnisse, die zu kontinuierlichen Verbesserungen und Korrekturen führen. AIOps kann man sich als kontinuierliche Integration und Bereitstellung (CI/CD) für IT-Kernfunktionen vorstellen.

Um das Ziel kontinuierlicher Erkenntnisse und Verbesserungen zu erreichen, benutzt AIOps drei verschiedene IT-Disziplinen:

- Service Management ("Engage")
- Leistungsmanagement ("Observe")
- Automatisierung ("Act")

6.2 Die Grundelemente von AIOps

Wir wollen nun anhand des Gartner Diagramms die Bestandteile von AIOps beschreiben.

6.2.1 Umfangreiche und vielfältige IT-Daten

AIOps basiert auf der Zusammenführung verschiedener Daten aus dem IT Operations Management (ITOM) (Metriken, Ereignisse usw.) und dem IT Service Management (ITSM) (Vorfälle, Änderungen usw.). Dies wird auch als "Aufbrechen von Datensilos" bezeichnet, das Zusammenführen von Daten aus unterschiedlichen Tools, damit sie miteinander "sprechen" und die Identifizierung von Ursachen beschleunigen oder eine Automatisierung ermöglichen können.

6.2.2 Aggregierte Big-Data-Plattform

Das Herzstück der Plattform sind Big Data. Sobald die Daten aus den einzelnen Silo Tools extrahiert sind, müssen sie zusammengeführt werden, um Analysen am nächsten Level zu unterstützen. Dies muss nicht nur offline geschehen - wie bei einer forensischen Untersuchung unter Verwendung historischer Daten - sondern auch in Echtzeit, während die Daten eingelesen werden.

6.2.3 Machine Learning (ML)

Big Data ermöglicht die Anwendung von maschinellem Lernen, um riesige Mengen unterschiedlicher Daten zu analysieren. Dies ist weder vor der Zusammenführung der Daten noch durch manuelle menschliche Arbeit möglich. ML automatisiert bestehende, manuelle Analysen und ermöglicht neue Analysen auf neuen Daten - alles in einem Umfang und einer Geschwindigkeit, die ohne AIOps nicht möglich sind.

6.2.4 Beobachten (Observe, Monitoring)

Dies ist die Weiterentwicklung der traditionellen ITOM-Domäne, die Entwicklungsdaten (Traces) und andere Nicht-ITOM-Daten (Topologie, Geschäftsmetriken) integriert, um neue Modalitäten der Korrelation und Kontextualisierung zu ermöglichen. In Kombination mit Echtzeitverarbeitung wird die Identifizierung wahrscheinlicher Ursachen gleichzeitig mit der Problemerzeugung möglich.

6.2.5 Einbinden (Engage)

Die Evolution der traditionellen ITSM-Domäne umfasst die bidirektionale Kommunikation mit ITOM-Daten, um die oben genannten Analysen zu unterstützen und automatisch Dokumentationen für Audits und Compliance-/Regulierungsanforderungen zu erstellen. AI/ML äußert sich hier in kognitiver Klassifizierung plus Routing und Intelligenz an der User Schnittstelle, z.B. Chatbots.

6.2.6 Handeln (Act)

Dies ist die "letzte Meile" der AIOps-Wertschöpfungskette. Die Automatisierung von Analyse, Workflow und Dokumentation ist nutzlos, wenn die Verantwortung für das Handeln wieder in menschliche Hände gelegt wird. „Handeln" umfasst die Kodifizierung des menschlichen Domänenwissens in die Automatisierung und Orchestrierung von Abhilfemaßnahmen und Reaktionen.

6.3 Die Zukunft von AIOps

Einer der Hauptmotivationen hinter AIOps ist die Tatsache, dass sich die heutige und künftige IT über das von Menschen noch sinnvoll verständliche Maß hinausbewegt. Daher müssen sich auch IT Tools diesen

Gegebenheiten anpassen. Unternehmen die dies erkennen und auf AIOps setzen nehmen heute schon die Herausforderungen der IT Zukunft an und setzten damit die notwendigen Schritte um künftig zu wachsen, sich weiterzuentwickeln, zu innovieren und die notwendigen Änderungen zeitgerecht durchzuführen.

Wir können heute folgende Möglichkeiten erkennen, wie Organisationen die AIOps verwenden (werden) ihr Geschäft in den kommenden Jahren ändern werden.

1. Technologie wird menschlicher: Analytics und Orchestrierung ermöglichen reibungslose Erfahrungen, die einen alles umfassenden Self-Service erlauben
2. Automatisierung von Technologie und damit von Geschäfts Prozessen: sinkende Kosten, steigende Geschwindigkeit, Reduzierung von Fehlern, während gleichzeitig Humankapital für höhere Leistungen freigesetzt wird
3. Enterprise ITOps bekommt DevOps-Agilität: Kontinuierliche Lieferung erstreckt sich auf den Betrieb und das Geschäft
4. Daten als Währung: Der enorme Reichtum an ungenutzten Geschäftsdaten wird kapitalisiert und erlaubt neue, hochwertige Anwendungsfälle und Möglichkeiten zur Geldgewinnung

7 COMMOC auf Basis von Icinga2

Bevor wir im Detail auf diesen Sachverhalt eingehen wollen wir nochmals kurz die Vor- und Nachteile von Open-Source und Closed-Source Lösungen besprechen und gegeneinander abwiegen. Wir haben gesehen, dass heute ein eindeutiger Trend zu Open-Source Lösungen besteht, und das mit gutem Grund basierend vor allem auf der Freiheit bei den einzusetzenden Systemen, den leichter optimierbaren und meist geringeren Kosten, dem offenen Quellcode der Zusätze und Änderungen nicht nur regelrecht animiert, sondern auch leicht ermöglicht und damit eine rasche und effiziente Anpassung an sich immer rasanter ändernde Gegebenheiten und Vorgaben im täglichen Business ermöglicht. Darüber hinaus ermöglichen offene Systeme mehr Kontrolle über die eigene Hardware und Software für die Anwender und daraus resultierend erhöhte Sicherheit und Stabilität für die Benutzer.

Fazit aus diesen Trends ist, dass heute Open-Source Lösungen in den allermeisten Fällen zu bevorzugen sind.

Wie wir aus dem Vergleich der unterschiedlichen Open-Source Monitoring Tools gesehen haben ist man mit Icinga 2 in allen oder zumindest den meisten Disziplinen heute am besten aufgestellt. Daher haben wir uns bei COMPRISE entschieden COMMOC auf Icinga2 und Grafana aufzubauen.

Icinga geht ja wie wir gesehen haben aus der Nagios Core Suite – einer der bewährtesten Monitoring Lösungen - hervor und hat sich mittlerweile zu einem mehr als leistungsfähigen Überwachungswerkzeug mit vielen Funktionen entwickelt. Icinga welches auf SNMP basiert um Daten von zu überwachenden Geräten und Einheiten abzurufen bietet eine einfache, gut strukturierte und saubere Benutzeroberfläche und gleichzeitig einen Funktionsumfang der seinesgleichen sucht und es ganz sicher mit kommerziellen Produkten aufnehmen kann.

Ein wesentlicher Vorteil von Icinga 2 ist jedoch, dass es die Verwendung von Plugins besonders effizient unterstützt. Es gibt von diesen Plugins mittlerweile Tausende, die von der Community ständig neu generiert und weiterentwickelt werden und damit die Funktionalität und Überwachungsmöglichkeiten des Produktes immens erweitern. Die Überwachungsmöglichkeiten reichen von VMware Umgebungen über Oracle, DB2, mySQL Datenbanken bis hin zu Linux, Windows Servern und USVs, Netzwerkdruckern uvm.

Mit Grafana welches mittlerweile die weltweit beliebteste Technologie ist, um Observability-Dashboards mit allem von Prometheus- und Graphite-Metriken über Logs und Anwendungsdaten aller erdenklichen Art zusammenzustellen ermöglicht COMMOC eine hochmoderne, zukunftsfähige Visualisierungs- und Auswertungsplattform hunderttausender Messwerte.

COMPRISE bietet ihren Kunden die Vorteile von Open-Source Produkten und löst dabei die üblicherweise hohe Lernkurve derartiger offener Produkte indem es diese in ihrer Verwendung so einfach macht wie von kommerziellen Produkten gewohnt, ohne wiederum in die Falle geschlossener Lösungen zu fallen.

Mit COMMOC ist man daher optimal vorbereitet ein zukunftssicheres, offenes, günstigeres und besonders umfangreiches Monitoring aufzubauen, das ganz sicher viele kommerziellen Lösungen in den Schatten stellt, wesentlich rascheres Deployment neuer Features und Anforderungen ermöglicht und wegen seiner besonders logischen und einfachen Bedienbarkeit auch optimal für effizientes Monitoring genutzt werden kann, ohne dabei die hohe Lernkurve die üblicherweise bei Open-Source Produkten notwendig ist zu durchlaufen.

8 Conclusion

Ob man sich für ein Open-Source- oder ein Closed-Source-Überwachungstool entscheiden, bleibt letztlicher jeder einzelnen Organisation überlassen. Wir haben die Unterschiede zwischen den beiden erklärt und die Vor- und Nachteile der beiden Typen beschrieben. Außerdem haben wir einige der besten kostenlosen Open-Source-Tools, sowie einige kommerzielle Gegenstücke, beschrieben, um zu zeigen was heute verfügbar ist.

Es mag den Anschein haben, dass sowohl Open- als auch Closed-Source-Softwarelösungen gleichwertig sind, denn beide haben ihre Vor- und Nachteile. Heute erscheinen jedoch Open-Source Lösungen immer kompetenter und sollten daher als echte Alternative zu Closed-Source Lösungen gesehen werden. Open-Source Lösungen sind nicht nur meist kostenlos und versprechen enorme Innovationsschübe geschuldet den wachsenden Communities, sie können auch mit ihren überwältigenden Vorteilen Closed-Source Lösungen immer leichter in den Schatten stellen.

Concorde Business Park F
2320 Schwechat
Austria, Europe

Firmenbuch: FN 280353i
Landesgericht Korneuburg
UID: ATU62886416

www.rise-world.com
welcome@rise-world.com

RISE