



Running the Atlassian Stack on Amazon Web Services

Scandio GmbH © 2018



scandio
TECHNOLOGY & CONSULTING

sales@scandio.de

Inhalt

1. Nutzung des Atlassian Stacks in der AWS Cloud.....	4
2. Der Atlassian Stack.....	5
2.1. Jira Software	5
2.2. Confluence	5
2.3. Bitbucket Server	5
2.4. Bamboo.....	6
2.5. Jira Service Desk	6
2.6. Crowd	6
3. Vergleich zur Atlassian Cloud	6
4. Ergänzende Tools.....	7
4.1. JFrog Artifactory	7
4.2. Jenkins CI Server.....	7
4.3. Sonarqube Code Quality.....	7
4.4. Matomo Web Analytics	7
5. Wichtige AWS-Dienste für den Atlassian Stack	8
5.1. Amazon Elastic Compute Cloud (EC2).....	8
5.2. Amazon Relational Database Service (RDS)	8
5.3. Elastic Load Balancing (ELB)	8
5.4. Amazon Virtual Private Cloud (VPC).....	9
5.5. Amazon Simple Storage Service (S3)	9
5.6. Route 53.....	9
5.7. AWS Certificate Manager (ACM)	9
5.8. Key Management Service (KMS)	9
5.9. Identity and Access Management (IAM)	9
5.10. CloudWatch Monitoring	9
5.11. Weitere Dienste.....	10
6. Hochverfügbarkeit und Skalierbarkeit.....	10
7. Netzwerkarchitektur.....	11
8. Installation und Migration.....	12
9. Monitoring, Alerting, Capacity Planning	14
10. Sicherheit & Datenschutz.....	15
11. Kostenoptimierung durch Entlastung der Infrastruktur und Kapazitäten.....	15
12. Zeitersparnis und Effizienzsteigerung.....	17
13. Anbieterinformationen.....	18
13.1. Amazon Web Services (AWS).....	18
13.2. Atlassian	18
13.3. Scandio GmbH	18

Executive Summary

Die Entscheidung, ein IT-System in einer eigenständig verwalteten Umgebung vor Ort oder in einer von einem Dienstleister betriebenen Umgebung zu hosten, ist für viele IT-Entscheider nicht einfach. Dieses Whitepaper beschäftigt sich mit dem Betrieb des Atlassian-Stacks in der AWS-Cloud und soll allen, die vor dieser Entscheidung stehen, einen ganzheitlichen Überblick bieten.

Der folgende Absatz fasst die aufkommenden Herausforderungen, die bei dieser Entscheidung entstehen und mögliche Lösungen für das Hosting der Atlassian-Produkte in der AWS Cloud kompakt zusammen:

- **Hohe Verfügbarkeit und Skalierbarkeit** - Skalierbarkeit ist dank Self-Service kein Problem mehr, da bei Bedarf eine neue Infrastruktur auf Knopfdruck bereitgestellt wird. "Elastic Load Balancing" verteilt den eingehenden Anwendungsverkehr auf mehrere Zielserverinstanzen. Es kann die variable Last der Zugriffe auf mehrere Zielserver verteilen.
- **Sicherheit** - Das Arbeiten im Umfeld von AWS-Diensten bedeutet nicht, dass alle Komponenten im Internet verfügbar sind. Die vollständige Isolierung und teilweise kontrollierte Öffnung ist über Netzwerke in der Virtual Private Cloud (VPC) einfach zu konfigurieren. Systeme können auch nach Unternehmensrichtlinien voneinander getrennt werden.
- **Kostenoptimierung** - Die Kosten der AWS-Dienste lassen sich leicht ermitteln. Vorlaufkosten werden eliminiert und ein komfortables Pay-as-you-go-Modell etabliert, das auf tatsächlichen Kosten und nicht auf Kapitalinvestitionen basiert. Durch weitere Optimierungsmaßnahmen wie "Auto Scaling" oder "Reserved Instances" können auch im laufenden Betrieb Kosten eingespart werden.
- **Zeitersparnis und Effizienzsteigerung** - Der Livegang kann schneller realisiert werden als mit Vor-Ort-Lösungen, da eine Abstimmung mit der internen Infrastruktur nicht mehr notwendig ist und nun vollständig in der Verantwortung des Cloud-Providers liegt. Effizienzsteigerungen werden weiterhin im laufenden Betrieb erzielt und können auf alle Instandhaltungs- und Modernisierungsarbeiten angewendet werden, da diese nun extern umsetzbar sind.

Das in diesem Whitepaper vorgestellte Szenario basiert auf der Nutzung von Server-Versionen von Atlassian-Anwendungen. Auch wenn Atlassian selbst eine Cloud-Version anbietet, hat die Server-Version einige Vorteile:

- **Speicherplatz** - Die Atlassian Cloud bietet bis zu 100 GB pro Anwendung. Eine in der AWS-Cloud installierte Server-Version ist nicht auf den Speicherplatz beschränkt und kann jederzeit erweitert werden.
- **Anzahl der Benutzer** - Die maximale Anzahl der gesamten Benutzer beträgt 5.000 in der Atlassian Cloud. Da die Produkte auch in Nicht-Software-Teams sehr beliebt sind, kann dies ein limitierender Faktor sein.
- **Datensicherung** - Atlassian bietet derzeit keine automatischen Backups an, um das System im Notfall wiederherzustellen. Dies muss vom Kunden manuell durchgeführt werden. Der Einsatz von AWS Services ermöglicht Backups ohne Ausfallzeiten und die vollautomatische, orchestrierte Erstellung von Testsystemen.

- **App-Verfügbarkeit** - Der [Atlassian Marketplace](#) bietet über 3.000 Apps zur Ergänzung der eigenen Produkte wie Confluence oder Jira an. Die Apps sind unerlässlich für die Integration in das Unternehmen und für die Abbildung komplexer Prozesse und Schnittstellen. Atlassian bietet für seine Cloud-Version bisher nur 1.200 Erweiterungen an. Da es sich bei der Installation in der AWS Cloud grundsätzlich um eine Server-Version handelt, können die Apps in vollem Umfang genutzt werden.
- **Anpassung** - Die Connect API für Atlassian Cloud macht die Produkte erweiterbar. Die Möglichkeiten sind jedoch durch das komplexe Cloud-Sicherheitskonzept deutlich eingeschränkt.

Natürlich müssen die Möglichkeiten jeweils einzeln, sauber und mit Mühe abgewogen werden. Dieses Whitepaper kann hierbei als Hilfsmittel dienen, um eine fundierte Entscheidung zu treffen.

1. Nutzung des Atlassian Stacks in der AWS Cloud

Die Entwicklung der letzten Jahre hat gezeigt, dass Software, Infrastruktur und auch Plattformen als Dienstleistung (SaaS, IaaS, PaaS) längst Einzug in Unternehmen aller Größen erhalten haben. Die Vorteile liegen klar auf der Hand: Pay-as-you-go Modelle ermöglichen geringe Einstiegskosten und bieten zumeist die Möglichkeit regelmäßig zu kündigen. Technisch müssen sich die Kunden eines Serviceproviders keine Gedanken um die Implementierung oder die Aktualität des Systems machen. Auch Skalierbarkeit ist durch den Self-Service kein Problem mehr, da bei Bedarf auf Knopfdruck eine neue Infrastruktur bereitsteht. Der Cloud-Computing Anbieter [Amazon Web Services](#) (AWS) hat sich durch seine Vielzahl an bereits vorhandenen Diensten und guten Bedienbarkeit als Marktführer durchsetzen können.

Auch Produkte des australischen Softwareherstellers [Atlassian](#) sind heute sowohl als Cloud-Version als auch als On-Premise-Variante verfügbar und seit mehr als zehn Jahren zu unersetzlichen Werkzeugen in der Softwareentwicklung und dem agilen Projektmanagement geworden. Aufgrund von eingeschränkter Anpassbarkeit und mangelnder Transparenz im Hinblick auf Datensicherheit und physischer Lagerung der Daten ist die bisher von Atlassian angebotene Cloud-Version für die meisten Unternehmen keine Option.

Für viele Atlassian Nutzer, die sich auf Ihre Kernkompetenzen beschränken möchten, stellen sich also folgende Fragestellungen, wenn sie die Vorteile von Cloud-Diensten nutzen möchten:

- Wie kann man sicherstellen, dass die Systeme bei stark steigenden Nutzerzahlen performant und dauerhaft verfügbar sind?
- Wie kann man den Betrieb möglichst kostengünstig in höchster Qualität gewährleisten, ohne die sowieso schon knappen internen Kapazitäten zu belasten?
- Wie ermöglicht es ein Unternehmen externen Partnern Werkzeuge zusammen mit den Mitarbeitern zu nutzen, um die für Innovationsprojekte notwendige Transparenz zu schaffen?

Aus der Erfahrung der letzten Jahre lässt sich ein Trend klar ableiten. Die sogenannte agile Toolchain kann optimal, hochverfügbar, sicher und [datenschutzkonform](#) in der AWS Cloud betrieben werden. Die von AWS zur Verfügung gestellten Dienste beschleunigen eine Inbetriebnahme beziehungsweise einen Umzug nicht nur, sondern steigern auch ohne großen Mehraufwand die Verfügbarkeit und Skalierbarkeit der Plattform.

Im Folgenden wird detailliert auf den Atlassian Stack und die AWS Technologien, die dessen hochverfügbaren und skalierbaren Betrieb ermöglichen, eingegangen. Zudem finden Sie

neben Ausführungen zur Erweiterbarkeit der Toolchain durch andere Anwendungen sowie zu Sicherheit und Datenschutz innerhalb der Cloud auch technische Details zu Infrastruktur, Architektur und Monitoring in AWS.

2. Der Atlassian Stack

Eine agile Toolkette beschreibt eine Applikationslandschaft, die für eine erfolgreiche Durchführung agiler Projekte benötigt wird. Die Produkte von Atlassian spielen hier zunehmend eine wichtige Rolle.

Die hierfür essentiellen Produkte sind:

- [Jira Software](#)
- [Confluence](#)
- [Bitbucket Server](#)
- [Bamboo](#)
- [Jira Service Desk](#)
- [Crowd](#)

Miteinander verzahnt, zeigen die Produkte ihre volle Stärke und können im agilen Projektmanagement, in der Team-Kollaboration, im Wissensmanagement und im Bereich Continuous Integration beziehungsweise Continuous Delivery gewinnbringend für das gesamte Unternehmen eingesetzt werden.

2.1. Jira Software

Jira Software ist das Herzstück des agilen Projektmanagements. Frei von Vorgaben in der Methodennutzung kann Jira Software für alle Arten von Projekten genutzt werden. Scrum und Kanban, aber auch Wasserfall-getriebene Projekte sind möglich. Erweiterungen wie Jira Portfolio ermöglichen Multiprojektmanagement und unterstützen große Unternehmen dabei, ihre neu gewonnene Agilität zu skalieren. Jira Software kann nicht nur für zeitlich begrenzte IT-Projekte genutzt werden, sondern ermöglicht auch die Abwicklung des gesamten Aufgaben-, Fehler- und Testfallmanagements. Vorgangstypen, Arbeitsabläufe, Benachrichtigungen und Berechtigungen sind frei definierbar und für jedes Projektszenario anpassbar.

2.2. Confluence

Mit Confluence, dem zweiten großen Produkt von Atlassian, werden in der Regel alle unstrukturierten text- und dateibasierten Informationen aus den Projekten, beziehungsweise aus dem gesamten Unternehmen, verwaltet. Mit Confluence ist ein Unternehmen in der Lage, eigene Communities zu schaffen, das Requirements Engineering für Projekte zu verwalten und den Single Point of Truth für das Wissensmanagement zu schaffen. Confluence und Jira ergänzen sich hierbei sehr gut und verfügen über eine tiefe funktionale Integration. Confluence ermöglicht es zudem, Dokumentationen auditfähig zu verwalten.

2.3. Bitbucket Server

Bitbucket Server ist das Source-Code-Management-System von Atlassian. Basierend auf dem Git-Standard ermöglicht Bitbucket alle generellen Git-Funktionen auf einem Enterprise-Level. Berechtigungen und das Nutzermanagement sind vollständig integriert

und die Verknüpfung mit Jira Software ermöglicht einen komplett transparenten Überblick. Git-Erweiterungen wie Pull Requests oder Forks gehören ebenfalls zum Standard von Bitbucket.

2.4. Bamboo

Bamboo ist der Continuous Integration Server von Atlassian. Mit Bamboo kann Software aus der Quellcodeverwaltung erstellt, automatisch getestet und auf die Stage- und Produktivumgebung ausgeliefert werden. Komplexe Builds und Releases können vollständig in Bamboo abgebildet werden, wodurch potenzielle Fehlerquellen, wie systemspezifische Unterschiede, gänzlich ausgeremert werden.

2.5. Jira Service Desk

Mit Jira Service Desk ist es möglich Jira zu erweitern, sodass interne und externe Kunden Jira entweder als ITIL-konformen Service Desk oder als simplen Help Desk nutzen können. Durch die Verknüpfung von Jira Service Desk mit Jira Software können IT- und Entwicklerteams auf einer gemeinsamen Plattform zusammenarbeiten, um Vorfälle schneller beheben und Änderungen zuverlässig umsetzen zu können

2.6. Crowd

Alle Atlassian-Produkte können über die zentrale Benutzerverwaltung Crowd gesteuert werden. Mittels Crowd haben Unternehmen die Möglichkeit, verschiedene Benutzerverwaltungen wie Office 365, LDAP/Active Directory oder ein lokales Benutzermanagement gleichzeitig zu verwenden. Crowd erlaubt zudem die Implementierung verschiedener Single-Sign-On-Lösungen, und seit der Version 3.3 ist es mit Crowd möglich, die Gruppenverwaltung an die Projektverantwortlichen zu delegieren.

3. Vergleich zur Atlassian Cloud

Atlassian ist nicht nur Hersteller von On-Premise-Software. Viele Produkte können auf der Cloudplattform von Atlassian direkt genutzt werden. Das Angebot ist umfangreich und komfortabel und entwickelt sich rasant weiter. Viele Neuerungen der Kernprodukte stehen erst in der Atlassian Cloud zur Verfügung und werden nach erfolgreichem Massentest auch in den On-Premise-Produkten sichtbar.

Worin liegen aber die Unterschiede dieser Lösung zu einem selbstorganisierten oder extern gesteuerten Betrieb in der AWS Cloud? Hier gibt es mehrere Kriterien zu beachten:

- **Speicherplatz** - In der Atlassian Cloud stehen je nach Nutzerzahl bis zu maximal 100 GB pro Applikation zur Verfügung. Dies ist nicht für alle Unternehmen ausreichend und muss bei einer Entscheidung berücksichtigt werden. Bei Installation in der AWS-Cloud gibt es keine Limitation in der Applikationsgröße und diese lässt sich jederzeit aufstocken.
- **Nutzeranzahl** - Zwar wurde die maximale Anzahl der Gesamtnutzer (alle Produkte) im September 2018 von 2.000 auf 5.000 Benutzer erweitert, jedoch erfreuen sich die Produkte auch in Teams fernab der Softwareentwicklung großer Beliebtheit. Deshalb sind Nutzerzahlen jenseits der 5.000 Nutzer in einem Unternehmen keine Seltenheit mehr. Bei Installationen in der AWS Cloud, gibt es im Gegensatz dazu keine Beschränkung der Nutzerzahlen.

- **Datensicherung** - Momentan bietet Atlassian noch keine automatisch erstellten Back-ups an, die im Notfall der Wiederherstellung des Systems dienen. Dies muss manuell durch den Kunden erfolgen. Die Nutzung der AWS Services erleichtert zero-downtime Backups und ermöglicht die vollautomatisch orchestrierte Erstellung von Testsystemen.
- **Appverfügbarkeit** - Im Atlassian Marketplace stehen als Ergänzung zu den eigenen Produkten wie Confluence und Jira, über 3.000 Apps zur Verfügung. Die Apps sind essentiell für die Integration in das jeweilige Unternehmen und für die Abbildung komplexer Prozesse und Schnittstellen, jedoch stehen für die Atlassian Cloud derzeit nicht alle Apps zur Verfügung. Das Angebot ist in dieser Kategorie auf knapp 1.200 Erweiterungen reduziert. Da es sich bei der Installation in der AWS Cloud prinzipiell um eine On-Premise-Version handelt, können die Apps in vollem Umfang genutzt werden.
- **Anpassungsmöglichkeiten** - Durch die Connect API für Atlassian Cloud sind die Produkte zwar erweiterbar, jedoch sind die Möglichkeiten durch das komplexe Cloud-Sicherheitskonzept deutlich eingeschränkt.

Aus Sicht des europäischen Datenschutzes kann die Atlassian Cloud noch nicht vollumfänglich eingesetzt werden. Atlassian arbeitet derzeit an einer GDPR/EU-DSGVO-konformen Lösung. Diese ist für 2019 geplant. Ein Rechenzentrum, das die eindeutige Speicherung der Daten in der europäischen Union sicherstellt, besteht bisher nur in der Planung. Insofern bietet sich die Nutzung der Atlassian Software in der AWS Cloud an, da in dieser Umgebung alle Bedingungen der europäischen Datenschutzverordnung erfüllt werden. Die AWS Services sind zudem nach ISO 27001, ISO 27017 und ISO 27018 zertifiziert.

4. Ergänzende Tools

Als Ergänzung der Atlassian Tools eignen sich aus dem Bereich der Softwareentwicklung insbesondere die folgenden weiteren Dienste:

4.1. JFrog Artifactory

[Artifactory](#) von [JFrog](#) ermöglicht die Speicherung einer Vielzahl an verschiedenen Build-Artefakt-Typen, die während der Entwicklung entstehen.

4.2. Jenkins CI Server

Der [Jenkins CI Server](#) ist der führende Open Source Build Server, mit dem nahezu alle Aufgaben im CI/CD-Umfeld umgesetzt werden können. Durch die große Auswahl an Erweiterungen können vielfältige Softwareprojekte gebaut und unkompliziert mit verschiedensten Diensten integrieren werden.

4.3. Sonarqube Code Quality

[Sonarqube](#) ist ein verbreitetes Tool für das Qualitätsmanagement von Source Code, das mögliche Fehler mithilfe statischer Quellcodeanalyseverfahren bereits während des Entwicklungsprozesses aufdecken kann.

4.4. Matomo Web Analytics

Ehemals bekannt als Piwik, kann [Matomo](#) DSGVO- und betriebsratskonform konfiguriert werden und ermöglicht eine Zugriffsanalyse innerhalb der Web-Anwendungen. So können

z.B. Seitenaufrufe in Confluence nachvollzogen und darauf basierend gezielt in Themenbereiche investiert werden, die innerhalb der Organisation besondere Aufmerksamkeit erhalten.

5. Wichtige AWS-Dienste für den Atlassian Stack

Für den Betrieb des Atlassian Stacks werden einige der mehr als hundert AWS-Dienste benötigt. Sie bilden das Rückgrat eines einfachen und kostenoptimierten Betriebs. Diese sind:

- Amazon Elastic Compute Cloud (EC2)
- Amazon Relational Database Service (RDS)
- Elastic Load Balancing (ELB)
- Amazon Virtual Private Cloud (VPC)
- Amazon Simple Storage Service (S3)
- Route 53
- AWS Certificate Manager (ACM)
- Key Management Service (KMS)
- Identity and Access Management (IAM)
- CloudWatch Monitoring

Jeder AWS-Dienst bietet hierbei die passende Leistung an und die tiefgehende Integration der Dienste untereinander vereinfacht die Konfiguration. Die folgende Beschreibung der AWS-Dienste gibt einen entsprechenden Überblick.

5.1. Amazon Elastic Compute Cloud (EC2)

Der Web-Service Amazon [Elastic Compute Cloud](#) (Amazon EC2) stellt sichere, skalierbare Rechenkapazitäten in der Cloud bereit. Mit EC2 ist es möglich, alle klassischen Serverdienste für Linux und Windows zu erstellen. Eine Auswahl an vorgefertigten Images vereinfacht die Nutzung.

5.2. Amazon Relational Database Service (RDS)

Amazon [Relational Database Service](#) (Amazon RDS) stellt schnell und unkompliziert relationale Datenbanken in der Cloud zur Verfügung, die zeitaufwändige Verwaltungsaufgaben automatisieren. Die RDS-Datenbanken sind out-of-the-box hochverfügbar und können annähernd beliebig skaliert werden.

5.3. Elastic Load Balancing (ELB)

[Elastic Load Balancing](#) verteilt eingehenden Anwendungsdatenverkehr auf mehrere Ziele wie Amazon-EC2-Instanzen, Docker Container und IP-Adressen. Es kann die variable Last des Anwendungsdatenverkehrs in eine einzelne Availability Zone oder in mehrere Availability Zones leiten. ELB ersetzt alle Reverse-Proxy-Systeme mit der höchsten Verfügbarkeit.

5.4. Amazon Virtual Private Cloud (VPC)

Die Amazon [Virtual Private Cloud](#) (Amazon VPC) ermöglicht die Bereitstellung eines logisch isolierten Bereichs der AWS-Cloud, indem AWS-Ressourcen in einem definierten virtuellen Netzwerk ausgeführt werden. VPC ermöglicht zudem die Verwendung von stateless sowie stateful Firewalls (Security Groups) und Subnetzen, um Verbindungen gezielt zu erlauben und zu verbieten. Auch eine VPN-Verbindung in das lokale Rechenzentrum kann über diesen Service gewährleistet werden.

5.5. Amazon Simple Storage Service (S3)

[Amazon S3](#) ist ein auf eine 99,99999999%ige Haltbarkeit ausgelegter Objektspeicher zum Speichern und Abrufen beliebiger Datenmengen aus allen Speicherorten: von Websites und mobilen Apps, Unternehmensanwendungen sowie Daten von IoT-Sensoren oder -Geräten.

5.6. Route 53

Amazon [Route 53](#) ist ein hochverfügbarer und skalierbarer Domain Name System (DNS)-Web-Service für die Cloud. Somit ist es für das Unternehmen möglich, das DNS Routing auf einfache Weise zu erweitern.

5.7. AWS Certificate Manager (ACM)

Der AWS [Certificate Manager](#) ist ein Service, mit dem problemlos öffentliche und private SSL- und TLS-Zertifikate (Secure Sockets Layer/Transport Layer Security) zur Verwendung mit AWS-Services und den internen verbundenen Ressourcen bereitgestellt und verwaltet werden können.

5.8. Key Management Service (KMS)

Der AWS [Key Management Service](#) (KMS) ist ein verwalteter Service, der die Erstellung und die Kontrolle der für die Datenverschlüsselung verwendeten Encryption Keys erleichtert und zum Schutz der Sicherheit der Schlüssel FIPS 140-2-validierte Hardwaresicherheitsmodule einsetzt.

5.9. Identity and Access Management (IAM)

Mit AWS [Identity and Access Management](#) (IAM) kann der Zugriff auf AWS-Services und -Ressourcen sicher verwaltet werden. Mithilfe von IAM können AWS-Benutzer und -Gruppen angelegt, verwaltet und mittels Berechtigungen der Zugriff auf AWS-Ressourcen zugelassen oder verweigert werden.

5.10. CloudWatch Monitoring

Amazon [CloudWatch](#) ist ein Überwachungs- und Managementdienst für Entwickler, Systembetreiber, Site Reliability Engineers (SRE) und IT-Manager. Über diesen lassen sich Metriken direkt über AWS-Dienste wie zum Beispiel EC2 und RDS auslesen, Alarme über SNS beispielsweise als E-Mail verschicken oder andere Aktionen wie Auto Scaling triggern.

5.11. Weitere Dienste

„Hinter den Kulissen“ kommen viele weitere AWS-Dienste zum Einsatz, deren Äquivalente jedoch im lokalen Rechenzentrum erhebliche Herausforderungen mit sich bringen. Die wichtigsten sind im Folgenden genannt:

- **CodeDeploy** - AWS [CodeDeploy](#) ist ein verwalteter Service, der Deployments unter anderem auf EC2-Instanzen automatisiert und dokumentiert. Mit CodeDeploy können neue Funktionen leichter und rascher freigegeben werden, Ausfallzeiten während der Anwendungsbereitstellung vermieden und komplexe Aktualisierungen von Anwendungen einfacher gehandhabt werden. AWS CodeDeploy kann zudem genutzt werden, um Softwarebereitstellungen zu automatisieren.
- **Lambda** - Mit AWS [Lambda](#) kann Code ausgeführt werden, ohne Server bereitstellen und verwalten zu müssen. Hierbei muss nur für die Rechenzeit bezahlt werden, die tatsächlich verbraucht wird – es entstehen keine Kosten, wenn der Code nicht ausgeführt wird.
- **SES** - Amazon [Simple Email Service](#) (Amazon SES) ist ein beliebig skalierbarer, cloudbasierter Service zum Senden von E-Mail, der einen SMTP-Endpunkt zur Verfügung stellt.
- **WorkMail** - Amazon [WorkMail](#) ist ein sicherer, verwalteter E-Mail- und Kalenderservice für Unternehmen, der durch seine IMAP-Anbindung vorhandene Desktop- und mobile E-Mail-Anwendungen sowie die Atlassian-Produkte unterstützt.
- **SNS** - Amazon [Simple Notification Service](#) (SNS) ist ein langlebiger, sicherer, vollständig verwalteter Pub/Sub-Messaging-Dienst der es ermöglicht, Mikroservices, verteilte Systeme und serverlose Anwendungen zu entkoppeln. Amazon SNS unterstützt eine große Anzahl an Subscriber-Endpunkten wie SQS, Lambda-Funktionen, HTTP/S-Webhooks und Mail.
- **CloudFront** - Amazon [CloudFront](#) ist ein schneller Content-Delivery-Service (CDN), der Daten, Videos, Anwendungen und APIs sicher, mit niedriger Latenz und hoher Übertragungsgeschwindigkeit an Kunden auf der ganzen Welt liefert.

6. Hochverfügbarkeit und Skalierbarkeit

Die Softwareprodukte von Atlassian können - Bamboo ausgenommen - als hochperformante, ausfallsichere Data-Center-Varianten implementiert werden. Jede Applikation kann somit in verschiedenen Rechenzentrumsabschnitten gleichzeitig auf beliebig vielen Knoten betrieben werden. Durch Loadbalancer sowie ausfallsichere Datenbanken und Storage-Systeme kann eine Verfügbarkeit von über 99 % erreicht werden. Updates und Backups können mit der Data-Center-Variante ohne geplante Downtimes durchgeführt werden. Dies ermöglicht einen einfachen und hocheffizienten Betrieb.

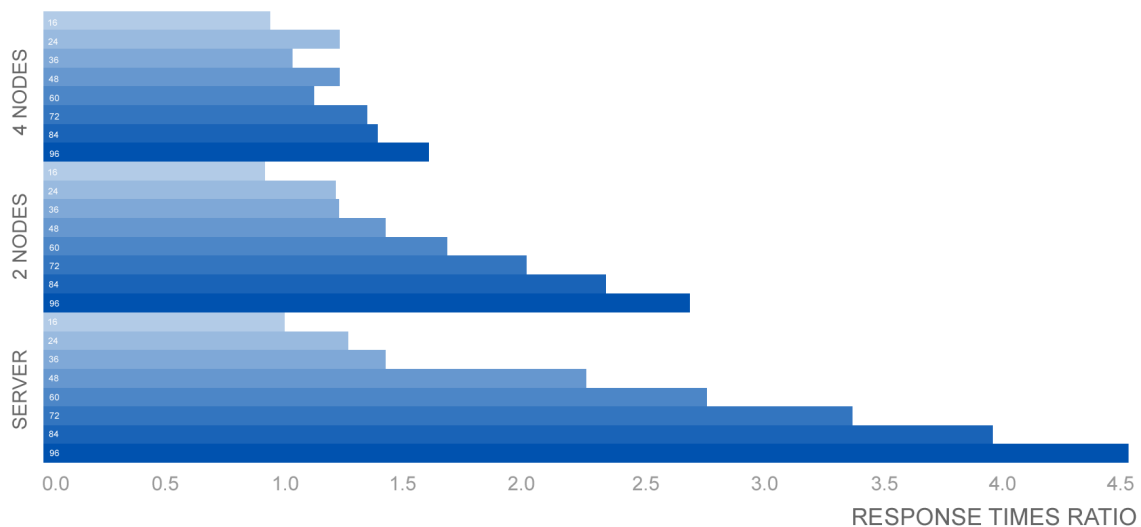


Abbildung 1 Relative Antwortzeiten verschiedener Confluence-Installationen. Getestet wurden Zugriffe mit 16, 24, 36, 48, 60, 72, 84 und 96 Browsern auf einer Single-Server- und auf zwei Data-Center-Installationen mit jeweils zwei und vier Nodes.

(Quelle: Atlassian (<https://confluence.atlassian.com/enterprise/confluence-data-center-performance-656408756.html>))

Die **Abbildung 1** zeigt einen Vergleich der Antwortzeiten einer Server-Installation, einer Data-Center-Variante mit zwei und einer mit vier Nodes. Dazu wurde bei 16 Browsern die Ladezeit der Server-Installationen mit einem Referenzwert von 1,0 definiert. Es ist klar ersichtlich, dass die Antwortzeiten mit der Zahl der gleichzeitigen Zugriffe zunehmen. Diese Zunahme ist durch mehrere Nodes leicht aufzufangen und somit ist für den User bei einem Betrieb von vier Nodes kaum ein Unterschied spürbar.

Werden die Atlassian-Produkte in der AWS Cloud betrieben, können die AWS-Dienste für Datenbanken (Relational Database Service **RDS**), Storage-Systeme (Elastic Block Store **EBS**, Elastic Files System **EFS**), Loadbalancer (Elastic Load Balancer **ELB**) und automatische Skalierung (Auto Scaling Group **ASG**) vollständig genutzt werden. Ob sich ein Data Center Deployment für ein Unternehmen lohnt, kann durch die Kernanforderungen

- Anzahl der aktiven (gleichzeitigen) Benutzer
- allgemeine Verfügbarkeit in verschiedenen Zeitzonen
- System Performance bei hoher Auslastung
- vollständige Ausfallsicherheit

erkannt, bewertet und entschieden werden. Die zur Verfügung stehenden AWS-Dienste für Skalierung und Hochverfügbarkeit reduzieren dabei die Aufwendungen der Umsetzung enorm.

7. Netzwerkarchitektur

Gerne unterschätzt, da in der Praxis sehr aufwändig, ist die Einrichtung einer Anwendungsumgebung samt Integration der benötigten Dienste und deren Konnektivität. Die Überlegungen beginnen meist mit der grundsätzlichen Netzwerkarchitektur:

Dürfen die Dienste nur über das Firmennetzwerk oder eine VPN-Verbindung erreichbar sein oder ist eine freie Verfügbarkeit über das Internet gewünscht, um ein einfaches On-Boarding von neuen Mitarbeitern und externen Partnern zu ermöglichen?

Im ersten Fall bietet sich eine VPN-Verbindung zwischen einem abgeschotteten AWS-Netzwerkbereich und dem Firmennetzwerk an, im zweiten Fall werden die Dienste für die allgemeine Erreichbarkeit über das Internet konfiguriert. Eine weitere zentrale Fragestellung ergibt sich bei der Thematik der Benutzerverwaltung, die je nach Bedarf an ein bestehendes LDAP- oder ActiveDirectory-System angeschlossen oder aber durch eine Single-Sign-On (SSO)-Lösung realisiert werden kann. Weitere Herausforderungen stellen sich bei den Themen DNS, den Zertifikaten für die Transportverschlüsselung und bei der Anbindung für E-Mail-Services zum Versenden von Benachrichtigungsmails und, im Falle von Jira Service Desk, dem Empfang von Antworten von Nutzern.

Im Umfeld der AWS-Dienste zu arbeiten bedeutet nicht, dass alle Komponenten im Internet verfügbar sind. Eine vollständige Abschottung und eine teilweise gesteuerte Öffnung ist mittels der virtuellen Netze zu konfigurieren. Auch Systeme untereinander können abgekapselt werden. Durch die Vielfalt der AWS-Dienste lassen sich die genannten Anforderungen komplett in der Cloud umsetzen, können jedoch nach Bedarf auch durch das Firmenrechenzentrum bereitgestellt werden. Erfahrungsgemäß ist jedoch dann mit Mehraufwand durch Kommunikation und Implementierung der Konnektivität zwischen lokalem Rechenzentrum und AWS zu rechnen. Dadurch entsteht letztlich ein erhöhter Zeitaufwand bei der Umsetzung.

8. Installation und Migration

Nach heutigen Maßstäben gilt eine manuelle Installation als veraltet. Stattdessen werden Systeme zum Beispiel mit Hilfe von Cloud Formation oder Terraform Infrastruktur als Code provisioniert (IaC) und versioniert. Ebenso bietet sich bei der Anwendungsinstallation und -konfiguration eine Automatisierung mit CodeDeploy und Ansible an. Zur Beschleunigung der Installationen kann auch die Erstellung von individuellen EC2-Instanz-Abbildern (AMIs) beispielsweise durch Packer erledigt und der Installations- und Konfigurationsanteil beim Start einer neuen Instanz minimiert werden.

Diese Versionierung der Infrastruktur und die Verwendung fertiger Instanz-Abbilder führt zu einer Unveränderlichkeit der Infrastruktur, einer sogenannten Immutable Infrastructure, die sich dadurch auszeichnet, dass zum Beispiel Änderungen der Server-Konfiguration via SSH unterbunden werden. Die Vorteile einer Immutable Infrastructure sind neben der Versionierung der Serverinstallationen, wodurch Änderungen nachverfolgt und im Fehlerfall gezielt rückgängig gemacht werden können, vor allem die beschleunigte Bereitstellung von Updates und eine Steigerung der Stabilität des Systems.

Aus der Erfahrung vergangener Migrationsprojekte dürfen einige Themen nicht vergessen werden.

- Das frühe Verringern der time-to-live des Domain Name Systems (DNS) ist essenziell, da sonst die Propagierung einige Stunden oder gar Tage in Anspruch nehmen kann. Im schlimmsten Fall wäre somit für manche Nutzer der Dienst in dieser Zeit nicht zu erreichen.
- Beim Anfertigen von Backups aus der alten Installation ist besonders zu beachten, dass es nicht genügt, ein Backup über die Anwendungsoberfläche zu erstellen. Es sollte stattdessen eine Kopie von Datenbankinhalt und Festplatte erstellt werden, da nicht alle Elemente im nativen Backup enthalten sind, beziehungsweise das Backup bei großen Installationen sogar fehlschlagen kann.

- Mit diesem Thema eng verknüpft ist das Ziel der Downtime-Minimierung: bei Installationen mit großem Platzbedarf auf einer Festplatte (mehrere hundert GB) bietet es sich an, vorab eine inkrementelle Kopie zu starten, um Downtimes von vielen Stunden oder Tagen zu verhindern.

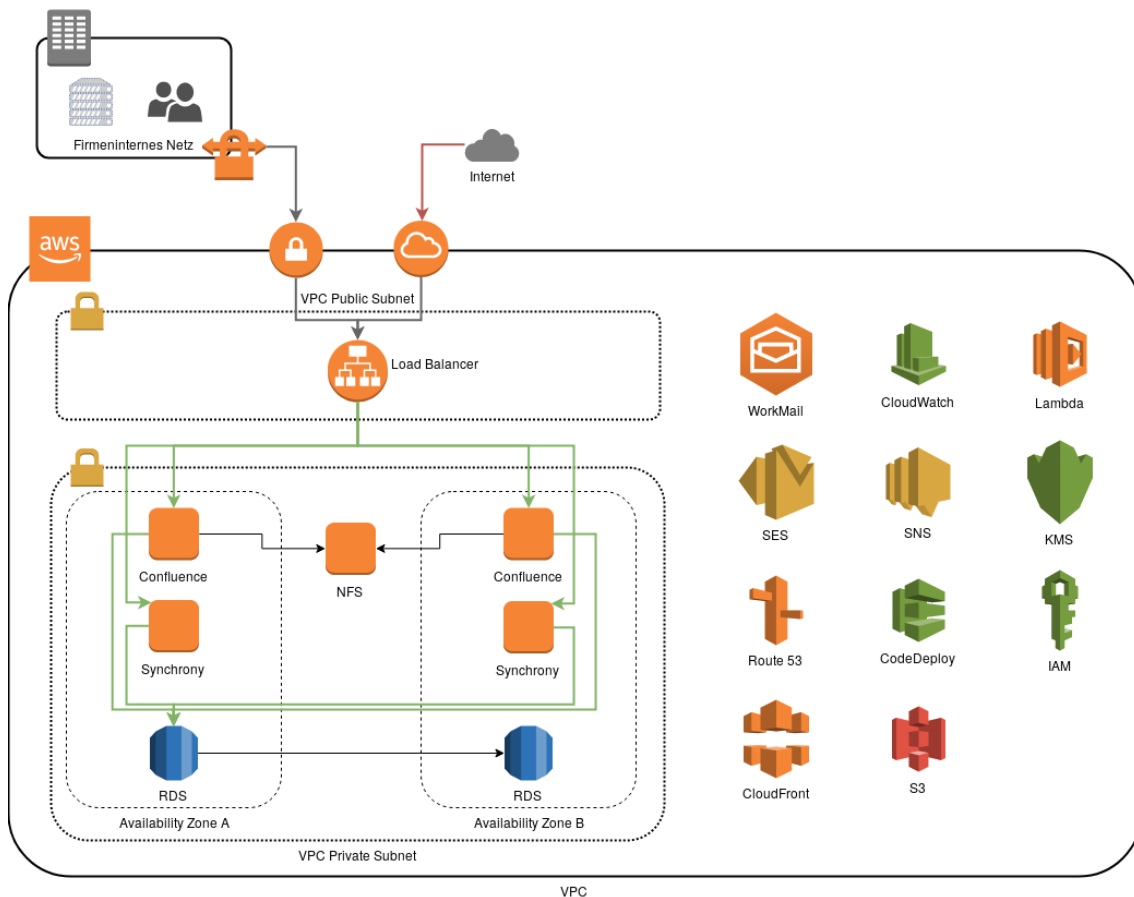


Abbildung 2 Übersicht der AWS-Architektur für den Betrieb eines Confluence in der Data-Center-Variante mit auf zwei separaten Server ausgelagertem Synchrony.

(Quelle: Scandio GmbH auf der Grundlage von AWS)

Die **Abbildung 2** zeigt alle verwendeten Services auf einen Blick. Die Anwendungsinstanzen, die RDS-Datenbanken sowie der Load Balancer sind hochverfügbar und ausfallsicher über verschiedene Availability Zones verteilt. Rechts sind zudem weitere Services aufgeführt, die Deployment, Monitoring, Mailversand und -empfang sowie Backup und Sicherheit garantieren. Zudem ist die Architektur und das Zusammenspiel von EC2, ELB und RDS sowie die VPN-Anbindung in ein lokales Rechenzentrum schematisch dargestellt. Exemplarisch ist hier eine Data-Center-Installation von Confluence mit separatem Synchrony (Synchrony ist die Lösung für die kollaborative Bearbeitung in Confluence) ausgewählt. User können ausschließlich über den Elastic Load Balancer auf die Anwendung zugreifen. Bei einer Single-Server-Installation dient der Load Balancer als Reverse Proxy. In beiden Fällen wird Traffic in das ansonsten abgeschottete private Subnetz weitergeleitet. Der gleiche Load Balancer wird auch verwendet, um Requests an Synchrony weiterzuleiten.

Auch die RDS-Datenbank liegt im privaten Subnetz und kann nur von den Anwendungsinstanzen aus erreicht werden. Alle diese Ressourcen existieren mindestens zweimal in verschiedenen Availability Zones um größtmögliche Ausfallsicherheit zu gewährleisten. Bei der Datenbank ist dies direkt in der Konfiguration von RDS auszuwählen ("Multi-AZ"), die verschiedenen EC2-Instanzen werden separat provisioniert. Eine weitere Instanz dient zudem als zentraler NFS-Server für Daten, die zwischen den Anwendungsinstanzen geteilt werden müssen. Auch das AWS Elastic File System (EFS) ist eine Option, bei großen Installationen führt die fehlende Snapshot-Möglichkeit jedoch zu Komplikationen bei Backup- und Testsystemgenerierung, da ein Kopieren der gesamten Installation zu viel Zeit in Anspruch nehmen kann. Wird die Snapshot-Funktion für EBS-Volumes und RDS-Datenbanken benutzt, können Zero-Downtime-Backups schnell und unkompliziert erstellt werden. Das Wiederherstellen des vollständigen Systems als Grundlage für ein Testsystem ist hierdurch, auch bei sehr großen Installationen mit mehreren hundert Gigabyte, problemlos in unter 20 Minuten möglich und gut automatisierbar.

Bei ausreichender Automatisierung, beispielsweise durch Ansible und CodeDeploy, kann durch dieses Design auch eine Auto-Scaling-Umgebung geschaffen werden, die durch AWS-interne Mechanismen eine automatische Hinzu- und Abschaltung von neuen EC2-Instanzen bei hoher beziehungsweise geringer Last ermöglicht. Die Grenzen, innerhalb derer sich diese Skalierung bewegt, sind individuell konfigurierbar.

Amazon WorkMail und SES werden für Mail-Empfang und -versand benötigt, via SNS können Alarme von CloudWatch beispielsweise direkt als Mail versendet werden. Die konsequente Verwendung von IAM und ein umsichtiger Umgang mit der Vergabe von Rechten an einzelne Personen garantieren höchstmögliche Sicherheit. Der Key Management Service erleichtert die strikte Verschlüsselung von Daten an allen Stellen und Lambda-Funktionen dienen dazu, regelmäßige Backups der Festplatten zu erstellen. Um die weltweiten Zugriffszeiten zu reduzieren, kann CloudFront als CDN genutzt werden. Je nach Anwendungsfall kann es jedoch sinnvoller sein, separate Installationen in unterschiedlichen Regionen zu pflegen und eine anwendungsinterne Synchronisation zu verwenden.

9. Monitoring, Alerting, Capacity Planning

AWS bietet mit CloudWatch einen zentralen Dienst an, mit dem sowohl Infrastruktur-, System- und Applikationsmetriken als auch Logdateien auf Betriebssystem- und Anwendungsebene gesammelt werden können.

Die Metriken von AWS-Diensten werden automatisch zur Verfügung gestellt. Bei EC2-Instanzen werden auch die Daten automatisch aufgezeichnet, die für den Hypervisor (auch als Virtual Machine Monitor bezeichnet, ist der Kern der meisten Produkte für die Servervirtualisierung) sichtbar sind. Feingranulare Informationen auf Systemebene, sowie Daten der Anwendung müssen über Custom-Metriken an CloudWatch übertragen werden. Dazu bieten sich neben den Java-Prozessdaten besonders auch JMX Beans an. Gerade letztere Metriken sind unersetzlich, um einen Einblick in den Anwendungszustand zu bekommen, früh auf eventuelle Engpässe und Probleme zu reagieren und Gegenmaßnahmen einleiten zu können.

Für die Fehlerdiagnose sind neben den Metriken auch Logfiles aller Applikationen unverzichtbar. Diese können mit Hilfe des CloudWatch Agents übertragen werden und stehen somit unmittelbar und für definierte Zeiträume zur Verfügung auch ohne, dass ein direkter Zugriff auf die jeweilige Instanz nötig ist.

Basierend auf den gesammelten CloudWatch-Metriken können bestimmte Aktionen veranlasst werden. Durch Events kann beispielsweise eine Benachrichtigung verschickt werden, aber auch Atlassian Data-Center-Installationen können so in eine Auto-Scaling-Umgebung implementiert werden.

Die langfristige Aufzeichnung von CPU-, RAM- und Speicherplatzbedarf ist die Basis, um ein optimales Verhältnis zwischen der nötigen Performance und dem Kostenaufwand für den individuellen Einsatzzweck zu erhalten.

10. Sicherheit & Datenschutz

Doch wie ist das Thema Datenschutz für einen Betrieb der Atlassian-Produkte auf AWS zu bewerten? In Europa spielt das Thema Datenschutz (GDPR/EU-DSGVO) seit dem 25.05.2018, aber auch schon davor eine sehr wichtige Rolle. Unternehmen nehmen die Regelungen in der Zwischenzeit sehr ernst und prüfen die Richtigkeit der Umsetzung kontinuierlich. Eine Toolchain auf der Basis der Atlassian-Produkte ist aus verschiedenen Gründen datenschutzrelevant. Auf der Plattform werden persönliche Daten von Mitarbeitern und externen Partnern gespeichert. AWS bietet hierfür ein sehr umfangreiches Paket an Services rund um das Thema GDPR/EU-DSGVO an und kann nachweisen, dass alle Dienste von AWS datenschutzkonform sind. Viele Kunden der Scandio nutzen hierzu die Sicherheit eines europäischen AWS-Rechenzentrums, insbesondere die Standorte Deutschland und Irland.

Noch wichtiger als die formelle Bestätigung der Datenschutzkonformität ist die tatsächliche technische Umsetzung der Datensicherheit und der darauf basierende Zugriffsschutz. Der Amazon Web Service bietet hierzu tief integrierte Funktionen zu den Themen Verschlüsselung, Überwachung, Protokollierung und Zugriffssteuerung an, die weit über den Standard in einem mittelständischen Unternehmen hinausgehen. Ebenso einfach lässt sich der partielle Zugriff auf Applikationen aus dem Internet steuern und auch die Multi-Factor-Authentifizierung kann mit einfachen Mitteln implementiert werden.

11. Kostenoptimierung durch Entlastung der Infrastruktur und Kapazitäten

Herkömmliche OnPremise-Lösungen erfordern für ihren Betrieb eine Hardware-Infrastruktur mit Servern, Speicher und Netzwerken. Alle Geräte müssen in sicheren und meist teuren Rechenzentren untergebracht werden. Darüber hinaus muss die gesamte Hardware gewartet, aktualisiert und regelmäßig ausgetauscht werden, sobald sie veraltet ist. Diese Aufgaben benötigen ein gewisses Maß an Fachkompetenz und stellen hohe - oft schlecht kalkulierbare - Einstiegskosten dar, bevor effektiv damit gearbeitet werden kann.

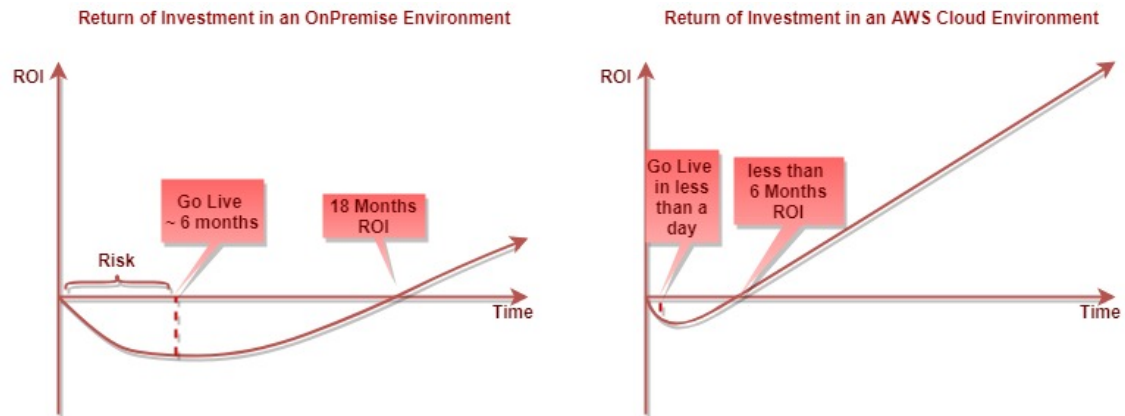


Abbildung 3 Vergleich des Return on Investments in einer On-Premise Installation und einer in der AWS Cloud installierten Variante.

(Quelle: Scandio GmbH)

Im Gegensatz dazu werden bei Software-as-a-Service alle oben genannten Überlegungen vom Anbieter übernommen und verwaltet. Kunden müssen hierbei weder Hardware kaufen noch in Hochverfügbarkeits- oder Sicherheitslösungen investieren. Alle Infrastruktur- und Leistungsanforderungen werden in Service Level Agreements (SLAs) mit dem AWS-Infrastrukturanbieter definiert, dessen Geschäfts- und Kernkompetenz die Bereitstellung von Software-Services ist.

Die Kosten der AWS-Dienste lassen sich mit dem AWS Calculator im Voraus gut bestimmen. Somit werden Vorabkosten eliminiert und ein komfortables Pay-as-you-go-Modell etabliert, das auf tatsächlichen Ausgaben und nicht auf Kapitalinvestitionen basiert. Durch die Nutzung von AWS kaufen Unternehmen keine Hardware oder virtuelle Server, sondern mieten Rechenzeit. Diese Betrachtung ist enorm wichtig, denn RAM, Anzahl der CPU-Kerne und Storage-Größen können jederzeit angepasst werden. Somit haben Unternehmen die Chance, nur die tatsächlich verwendete Kapazität zu buchen und zu bezahlen. Mittels mehrerer Optimierungsmaßnahmen lassen sich die Kosten der Infrastruktur während des Betriebs weiter senken. Diese sind:

- **Reserved Instances** - Mittels fester Buchungen bei einer Dauer von 12 Monaten oder 36 Monaten können die Kosten je nach Service um bis zu 60 % gesenkt werden.
- **Spot Instances** - Hierbei können die Kosten für den EC2-Dienst um bis zu 90 % reduziert werden. Der einzige Unterschied zwischen On-Demand-Instances und Spot-Instances liegt darin, dass Spot-Instances mit zwei Minuten Benachrichtigungsvorlauf durch EC2 unterbrochen werden können, wenn EC2 die Kapazität benötigt.
- **Continuous Monitoring** - Prüfen Unternehmen kontinuierlich den tatsächlichen Bedarf an Rechenleistung und Storage-Kapazitäten, werden Überkapazitäten dauerhaft abgebaut, die im lokalen Rechenzentrum mit mindestens 50 % angenommen werden.
- **Auto Scaling** - Nutzt man die Data-Center-Option von Atlassian, können möglichst kleine Server-Knoten verwendet werden. Nur bei tatsächlichem Bedarf werden weitere Knoten zugeschaltet. Geht man beispielsweise von zwei Peak-Phasen à zwei Stunden pro Tag aus, können hier die Kosten, je nach Zeitzonen-Nutzung, ebenfalls signifikant gesenkt werden.

Im Allgemeinen kann man davon ausgehen, dass bei dieser detaillierten Gegenüberstellung die Kosten der AWS-Dienste im Vergleich zum lokalen Rechenzentrum keine wesentliche Teuerung darstellen, aber sehr wohl eine Flexibilitätssteigerung. Zusätzlich werden bisher belegte Kapazitäten im Unternehmen frei, die sich fortan auf die Kernkompetenz des Unternehmens konzentrieren und sich somit gewinnbringend für das Unternehmen einbringen können.

12. Zeitersparnis und Effizienzsteigerung

Nicht nur die oben beschriebenen monetären Einsparungen sollten betrachtet werden, sondern auch die eingesparte Zeit, wenn die Applikationen in der AWS Cloud installiert werden. Aus eigener Erfahrung hat sich gezeigt, dass hierbei ein Live-Gang schneller realisiert werden kann als bei On-Premise-Lösungen, da die Abstimmung mit der internen Infrastruktur entfällt und nun völlig dem Cloud-Anbieter obliegt.

On-Premise	AWS
Einrichtung und Wartung von Datenbank-Clustern	Verwenden Sie den Relationalen Datenbankdienst und konfigurieren Sie ihn mit wenigen Klicks im Detail.
Aufbau und Wartung eines hochverfügbaren Load Balancer	Nutzen Sie den Elastic Load Balancing Service und konfigurieren Sie mit wenigen Klicks detailliert.
Durchlaufen interner Prozesse zur Änderung virtueller Maschinen	Einfache Änderung des Instanztyps Ihrer EC2-Rechner und RDS-Instanzen
Ein bestimmter Prozentsatz Ihrer Infrastruktur muss ungenutzt sein, um im Notfall verfügbar zu sein.	Bezahlen Sie nur für das, was Sie nutzen.
Einrichtung und Wartung von Mail-Servern	Verwenden Sie den einfachen E-Mail-Service zum Senden und WorkMail zum Empfangen von E-Mails.
Koordination und Pflege von Domains und Zertifikaten	Verwenden Sie selbstverlängernde Amazon-Zertifikate zusammen mit Route53.

Tabelle 1 Vergleich ausgewählter Ressourcen in einer On-Premise Umgebung und in der AWS-Cloud

Diese Effizienzvorteile setzen sich im laufenden Betrieb fort und lassen sich auf alle Wartungs- und Upgrade-Arbeiten, die nun extern stattfinden, übertragen. Da sich die Cloud-Anwendung und die gesamte Infrastruktur außerhalb des Unternehmens befinden, sind Unternehmen nicht an Wartungen oder Upgrades beteiligt, da diese ausschließlich von den Cloud-Anbietern in ihren Rechenzentren durchgeführt werden.

Unternehmensweit können die Applikationen ohne regionale Bindung und zusätzliche Kosten angeboten werden. Da Benutzer nur eine Internetverbindung benötigen, um auf die Cloud-Anwendung zuzugreifen, wird der Standort irrelevant. Dies ist ein großer Vorteil für zunehmend mobile Mitarbeiter und mögliche Partnerfirmen.

13. Anbieterinformationen

13.1. Amazon Web Services (AWS)

Im Jahr 2006 begann [Amazon Web Services \(AWS\)](#), IT-Infrastruktur-Services für Unternehmen als Web-Dienste (heute allgemein bekannt als Cloud Computing) anzubieten. Heute bietet AWS eine hochzuverlässige, skalierbare und kostengünstige Infrastrukturplattform in der Cloud, die für den Betrieb von Hunderttausenden von Unternehmen in 190 Ländern auf der ganzen Welt genutzt wird.



Die AWS Cloud bietet eine breite Palette von Infrastruktur-diensten, wie Rechenleistung, Speicheroptionen, Netzwerke und Datenbanken, die als Dienstprogramme bereitgestellt werden: On-Demand, in Sekundenschnelle verfügbar, mit Pay-as-you-go-Preisen. Vom Data Warehousing bis hin zu Bereitstellungstools, Verzeichnissen und der Bereitstellung von Inhalten stehen über 100 AWS-Dienste zur Verfügung.

13.2. Atlassian

[Atlassian](#) wurde 2002 mit der Mission gegründet, das Potenzial in jedem Team zu entfalten. Atlassians Suite von Team Collaboration Software - Jira Software, Confluence, Bitbucket, Jira Service Desk und Portfolio for Jira - erleichtert es Teams, Arbeit zu organisieren, zu diskutieren und abzuschließen. Heute helfen die Atlassian-Produkte Teams aller Art und Größen in nahezu jeder Branche - von Software- und Technikteams bis hin zu Vertriebs- und Marketing-Teams. Damit unterstützt Atlassian seit vielen Jahren grosse Unternehmen bei der Einführung agiler Methoden.



13.3. Scandio GmbH

Die [Scandio](#) GmbH ist eine Softwareschmiede voller technikbegeisterter Consultants, Entwickler und Problemlöser. Auf Basis eines umfangreichen Know-hows und langjähriger Erfahrung entwickelt Scandio seit 15 Jahren erfolgreich maßgeschneiderte Lösungen für ihre Kunden. Sie unterstützen Unternehmen ebenso in den Bereichen Cloud-Strategie, UI/UX-Consulting und DevOps Engineering, sowie bei der Automatisierung, der Orchestrierung und im agilen Development. Seit mehr als 10 Jahren ist die Scandio Atlassian Platinum Solution Partner. 2018 wurde Scandio von Atlassian zum Partner des Jahres in der Kategorie "Enterprise" gewählt. Durch die langjährige Partnerschaft mit AWS konnten die Berater der Scandio massiv Wissen in beiden Bereichen aufbauen. Zu den Kunden der Scandio gehören unter anderem BMW, BSH, Infineon und Siemens.

