# AWS Well-Architected Framework

Juli 2019

In diesem Dokument geht es um das AWS Well-Architected Framework. Dieses ermöglicht Ihnen, Ihre Cloud-basierten Architekturen zu überprüfen und zu verbessern und die geschäftlichen Auswirkungen Ihrer Designentscheidungen besser nachzuvollziehen. Wir gehen dabei auf allgemeine konzeptionelle Grundsätze sowie auf bewährte Methoden ein und geben Anleitungen zu fünf konzeptionellen Bereichen, die wir als die *Säulen* des AWS Well-Architected Framework bezeichnen.

## Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen Produktangebote und Verfahren von AWS wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

# Einführung

Das AWS Well-Architected Framework unterstützt Sie dabei, die Vor- und Nachteile der Entscheidungen nachzuvollziehen, die Sie beim Aufbau von Systemen in AWS treffen. Das Framework hilft Ihnen, architektonische Best Practices für die Entwicklung und den Betrieb zuverlässiger, sicherer, effizienter und kosteneffektiver Systeme in der Cloud zu ermitteln. Es bietet Ihnen die Möglichkeit, Ihre Architekturen konsistent auf die Einhaltung bewährter Methoden zu prüfen und Verbesserungspotenzial zu identifizieren. Die Überprüfung einer Architektur ist kein Audit. Vielmehr ist es eine konstruktive Konversation, in der es um architektonische Entscheidungen geht. Wir sind davon überzeugt, dass architektonisch gute Systeme die Wahrscheinlichkeit des geschäftlichen Erfolgs signifikant beeinflussen.

AWS Solutions Architects entwerfen seit vielen Jahren Architekturen für unterschiedlichste Branchen und Anwendungsfälle. Wir waren am Design und der Überprüfung Tausender Kundenarchitekturen auf AWS beteiligt. Daher kennen wir die bewährten Methoden und Kernstrategien für erfolgreiche Systemarchitekturen in der Cloud.

Das AWS Well-Architected Framework dokumentiert grundlegende Fragen, mit denen Sie klären, ob eine Architektur einwandfrei mit bewährten Methoden für die Cloud vereinbar ist. Über das Framework erhalten Sie eine einheitliche Herangehensweise zur Bewertung der Eigenschaften, die Sie von modernen Cloud-basierten Systemen erwarten, sowie Vorschläge zur Realisierung dieser Eigenschaften. AWS entwickelt sich ständig weiter, und auch wir lernen durch die Arbeit mit unseren Kunden ständig dazu. Und so wie unser Wissen anwächst, können wir immer wieder noch genauer definieren, wodurch sich eine gute architektonische Struktur auszeichnet.

Dieses Framework richtet sich an Technologiefachleute, z. B. Chief Technology Officers (CTO), Architekten, Entwickler und Operations-Mitarbeiter. Die darin enthaltenen bewährten Methoden und Strategien für AWS kommen beim Design und der Nutzung von Cloud Workloads zum Einsatz. Die Links verweisen auf weitere Implementierungdetails und Architekturmodelle. Weitere Informationen finden Sie auf der Homepage von AWS Well-Architected Homepage.

AWS bietet auch an, Ihre Workloads kostenfrei zu überprüfen. Das AWS Well-Architected Tool (AWS WA Tool) ist ein Service in der Cloud, der einen einheitlichen Prozess zum Überprüfen und Messen Ihrer Architektur mit AWS Well-Architected Framework bietet. Vom AWS WA Tool erhalten Sie Empfehlungen, wie Sie Ihre Workloads zuverlässiger, sicherer, effizienter und kostengünstiger machen.

Um Ihnen das Arbeiten nach bewährten Methoden zu erleichtern, haben wir AWS Well-Architected Labsentwickelt. Der Code und die Dokumentation von Labs erlauben Ihnen, eigene Erfahrungen mit der Implementierung bewährter Methoden zu sammeln. Außerdem haben wir ausgewählte Partner aus dem AWS Partner Network (APN)

in das AWS Well-Architected-Partnerprogrammaufgenommen. Diese APN-Partner sind bestens mit AWS vertraut und können Sie beim Überprüfen und Verbessern Ihrer Workloads unterstützen.

# Definitionen

Die Experten von AWS unterstützen mit bewährten Cloud-Methoden tagtäglich Kunden beim Entwerfen von Systemarchitekturen. Während wir zusammen mit Ihnen die Architektur entwerfen, wägen wir die Anforderungen ab und treffen die richtigen Kompromisse. Wenn Sie die Systeme dann in Live-Umgebungen bereitstellen, beobachten wir, wie gut diese Systeme laufen und welche Auswirkungen die Kompromisse haben.

Unsere bisherigen Erkenntnisse sind die Grundlage von AWS Well-Architected Framework. Das Framework enthält einheitlich zusammengestellte bewährte Methoden, mit denen Kunden und Partner Architekturen bewerten. Anhand verschiedener Fragen können sie beurteilen, wie gut eine Architektur auf die bewährten Methoden von AWS ausgerichtet ist.

Das AWS Well-Architected Framework basiert auf fünf Säulen: betriebliche Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz und Kostenoptimierung.

### Tabelle 1. Die Säulen des AWS Well-Architected Framework

| Name | Beschreibung |
|---|---|
| **Betriebliche Exzellenz** | Die Fähigkeit, Systeme auszuführen und zu überwachen, einen geschäftlichen Nutzen zu erbringen und unterstützende Prozesse und Verfahren kontinuierlich zu verbessern |
| **Sicherheit** | Die Fähigkeit, Informationen, Systeme und Ressourcen mithilfe von Risikobewertungen und Migrationsstrategien zu schützen und gleichzeitig einen Mehrwert für das Geschäft zu liefern |
| **Zuverlässigkeit** | Hierbei geht es um die Fähigkeit eines Systems, sich von Infrastruktur- oder Service-Unterbrechungen zu erholen, Computing-Ressourcen dynamisch zur Erfüllung des Bedarfs anzufordern und Unterbrechungen zu minimieren, die beispielsweise aus Fehlkonfigurationen oder vorübergehenden Netzwerkproblemen resultieren. |
| **Leistungseffizienz** | Die Fähigkeit, Rechenressourcen effizient entsprechend den Systemanforderungen zu nutzen und diese Effizienz aufrechtzuerhalten, während sich die Nachfrage ändert und die Technologie weiterentwickelt. |

| Name | Beschreibung |
| --- | --- |
| **Kostenoptimierung** | Hierbei geht es um die Fähigkeit, Systeme so auszuführen, dass der Geschäftswert bei den geringstmöglichen Kosten bereitgestellt wird. |

In Zusammenhang mit dem AWS Well-Architected Framework verwenden wir dies Bezeichnungen

- Eine **Komponente** besteht aus dem Code, der Konfiguration und den AWS-Ressourcen, die für eine Anforderung bereitgestellt werden. Eine Komponente ist häufig die Einheit technischen Eigentums und von anderen Komponenten losgelöst.
- Mit **Workload** bezeichnen wir zusammengehörige Komponenten, die geschäftlichen Mehrwert darstellen. Der Workload ist in vielen Fällen der Detaillierungsgrad, von dem Führungskräfte aus Wirtschaft und Technik häufig sprechen.
- **Meilensteine** kennzeichnen wichtige Änderungen in Ihrer Architektur, die nötig sind, um sie an den Produktzyklus (Design, Tests, Go-Live und Produktionsbetrieb) anzupassen.
- Wir betrachten **Architektur** als das Zusammenwirken von Komponenten in einem Workload. Wie Komponenten kommunizieren und interagieren, ist häufig der Schwerpunkt von Architekturdiagrammen.
- Innerhalb einer Organisation ist das **Technologieportfolio** die für den Geschäftsbetrieb erforderliche Sammlung an Workloads.

Beim Entwerfen von Workloads stellen Sie eine Kosten-Nutzen-Abwägung zwischen Säulen abhängig von Ihrem Geschäftskontext an. Diese Geschäftsentscheidungen können Ihre technischen Prioritäten beeinflussen. Sie können optimieren, um Kosten zulasten der Zuverlässigkeit in Entwicklungsumgebungen zu senken, oder Sie können bei unternehmenskritischen Lösungen die Zuverlässigkeit mit höheren Kosten optimieren. Bei E-Commerce-Lösungen kann sich die Leistung auf die Einnahmen und die Kauflust der Kunden auswirken. Sicherheit und betriebliche Exzellenz haben in der Regel keine Wechselwirkung mit den anderen Säulen.

# Architektur-Überlegungen

In On-Premise-Umgebungen setzen Kunden oft ein Zentralteam für Technologiearchitektur ein. Dieses ist anderen Produkt- oder Feature-Teams vorgeschaltet, damit diese nach bewährten Methoden arbeiten. Technologiearchitektur-Teams setzen sich oft aus Fachleuten mit unterschiedlichen Aufgabengebieten zusammen [z. B. Technical Architect (Infrastruktur), Solutions Architect (Software), Data Architect, Networking Architect und Security Architect]. Diese Teams arbeiten oft nach dem TOGAF-Modell oder dem Zachman Framework – als Teil eines Kompetenzbereichs für Enterprise-Architektur.

AWS verteilt Fähigkeiten lieber auf einzelne Teams, anstatt die Kompetenz in einem Zentralteam zu konzentrieren. Wenn die Entscheidungsbefugnis auf mehrere Teams verteilt wird, geht das mit Risiken einher. So muss beispielsweise sichergestellt sein, dass die Teams internen Standards gerecht werden. Um diese Risiken aufzufangen, verwenden wir zwei Methoden. Zum einen arbeiten wir mit *Praktiken* [1] , die darauf abzielen, jedes Team mit dieser Fähigkeit auszustatten. Dafür setzen wir Experten ein, die dafür sorgen, dass die Teams die vorgegebenen Standards übertreffen. Zweitens implementieren wir *Mechanismen* [2] , die automatisch kontrollieren, ob Standards eingehalten werden. Hinter diesem breit aufgestellten Ansatz stehen die Führungsprinzipien von Amazon. Diese stellen sicher, dass in allen Aufgabenbereichen eine Kultur verankert wird, die *vom Kunden aus denkt* [3] . Kundenfixierte Teams richten die Produktentwicklung auf Kundenwünsche aus.

In Zusammenhang mit Architekturen bedeutet das: Wir erwarten von jedem Team, dass es Architekturen erstellen und nach bewährten Methoden arbeiten kann. Um neuen Teams zu diesen Fähigkeiten zu verhelfen bzw. um bestehende Teams leistungsfähiger zu machen, nehmen wir sie in eine virtuelle Community auf, in der Principal Engineers ihre Entwürfe begutachten und sie an die bewährten AWS-Methoden heranführen. Die Community der Principal Engineers hat die Aufgabe, bewährte Methoden sichtbar und verständlich zu machen. Dies geschieht beispielsweise durch Mittagsvorträge, in denen es um die Anwendung bewährter Methoden an praktischen Beispielen geht. Die Vorträge werden aufgezeichnet und können für das Onboarding neuer Teammitglieder eingesetzt werden.

Wir haben bislang mehrere Tausende Internet-ähnliche Systeme eingerichtet und dabei einen Erfahrungsschatz aufgebaut, aus dem sich die bewährten AWS-Methoden herauskristallisiert haben. Wir bevorzugen, bewährte Methoden mit Hilfe von Daten zu definieren. Wir setzen dafür aber auch Fachexperten (z. B. Principal Engineers) ein. Principal Engineers sind direkt dabei, wenn sich neue bewährte Methoden abzeichnen. Als Community können sie sicherstellen, dass die Teams danach arbeiten. Im Laufe der Zeit werden diese bewährten Methoden formalisiert in unsere internen Prüfprozesse sowie in Compliance-Mechanismen aufgenommen. Well-Architected ist die kundenseitige Implementierung unseres internen Prüfprozesses. Darin ist die Denkweise der Principal Engineers für Zuständigkeitsbereiche vor Ort (z. B. Solutions Architecture, interne Engineering-Teams) festgeschrieben. Well-Architected ist ein skalierbarer Mechanismus, mit dem Sie von diesen Erkenntnissen profitieren können.

Wenn so vorgegangen wird wie in einer Community aus Principal Engineers (mit verteilten Architekturzuständigkeiten), kann unserer Ansicht nach eine Well-Architected

[1] Vorgehensweisen, nach denen Dinge, Prozesse, Standards und gemeinhin anerkannte Normen gehandhabt werden.
[2] „Gut gemeinte Absichten funktionieren nicht. Wer etwas erreichen will, braucht gute Mechanismen.“ Jeff Bezos. Das bedeutet konkret, dass wir das Bestmögliche, das Menschen leisten können, durch (automatisierte) Mechanismen ersetzen, die kontrollieren, ob Regeln oder Prozesse eingehalten werden.
[3] Vom Kunden aus denken ist ein grundlegender Bestandteil unseres Innovationsprozesses. Unsere Arbeit richtet sich ganz nach dem Kunden und dessen Wünschen.

Enterprise-Architektur zustande kommen, die auf die Kundenwünsche ausgerichtet ist. Technologievordenker (z. B. CTO oder Entwicklungsleiter), die all Ihre Workloads nach den Prinzipien des Well-Architected-Ansatzes prüfen, können die Risiken Ihres Technologieportfolios aufzeigen. Sie identifizieren teamübergreifende Themen, die Ihre Organisation mit Hilfe von Mechanismen, Trainings oder Mittagsvorträgen angehen könnte. Allesamt Gelegenheiten für Ihre Principal Engineers, ihr Wissen zu bestimmten Themen an mehrere Teams weiterzugeben.

# Allgemeine konzeptionelle Grundsätze

Das Well-Architected Framework fasst allgemeine konzeptionelle Grundsätze zusammen, die gutes Design in der Cloud fördern:

- **Keine Ungewissheit mehr über die Kapazität**: Ungewissheit mehr beim Bestimmen der Anforderungen an die Infrastrukturkapazität muss nicht sein. Wenn Sie vor der Bereitstellung eines Systems eine Entscheidung zur Kapazität treffen, sitzen Sie anschließend möglicherweise auf nicht genutzten Ressourcen oder haben zu wenig Kapazität und müssen sich mit mangelnder Performance herumschlagen. Beim Cloud Computing gibt es diese Probleme nicht. Sie arbeiten mit so viel oder so wenig Kapazität wie nötig. Das System wird automatisch hoch- oder herunterskaliert.
- **Systeme auf Produktionsbetrieb testen**: Sie können in der Cloud bei Bedarf eine Testumgebung in Produktionsgröße einrichten, Ihre Tests abschließen und die Ressourcen dann wieder stilllegen. Weil Sie für die Testumgebung nur dann zahlen, wenn sie genutzt wird, können Sie Ihre Live-Umgebung zu einem Bruchteil der Kosten testen, die Sie an einem lokalen Standort hätten.
- **Automatisierung vereinfacht Architekturexperimente**: Wenn Sie automatisieren, können Sie Ihre Systeme kostengünstig erstellen und replizieren und vermeiden manuellen Aufwand. Sie können an der Automatisierungen vorgenommene Änderungen nachverfolgen, die Auswirkungen nachprüfen und ggf. auf die vorherigen Parameter zurücksetzen.
- **Voraussetzungen für evolutionäre Architekturen schaffen**: Schaffen Sie Voraussetzungen für evolutionäre Architekturen. In herkömmlichen Umgebungen sind architekturrelevante Entscheidungen oft als statische, einmalig auftretende Ereignisse implementiert. Dementsprechend gibt es während der Lebensdauer des Systems einige wenige große Versionen. Geschäftsvoraussetzungen und ihr Kontext unterliegen einem ständigen Wandel. Diese anfangs getroffenen Entscheidungen könnten die Fähigkeit des Systems beeinträchtigen, sich auf neue Geschäftsvoraussetzungen einzustellen. In der Cloud können Sie jederzeit automatisieren und testen. Dadurch wird weniger wahrscheinlich, dass sich Änderungen am Design negativ auswirken. Dieses System kann sich im Laufe der Zeit weiterentwickeln. Unternehmen können dann wie selbstverständlich Innovationen für sich nutzen.
- **Mit Daten Architekturen weiterentwickeln**: Sie können in der Cloud Daten zu der Frage sammeln, wie Ihre architekturrelevanten Entscheidungen auf das Verhalten Ihres Workloads durchschlagen. Sie können also mit faktenbasierten Entscheidungen Ihren Workload verbessern. Ihre Cloud-Infrastruktur ist Code. Das bedeutet, dass Sie diese Daten im Laufe der Zeit in architekturrelevante Entscheidungen und Verbesserungsmaßnahmen einfließen lassen können.

- **Verbesserung mit Hilfe von Ernstfallübungen**: Stellen Sie fest, wie Ihre Architektur und Ihre Prozesse performen. In regelmäßigen Ernstfallübungen (Gamedays) simulieren Sie Ereignisse aus dem Produktionsbetrieb. So können Sie nachvollziehen, wo nachgebessert werden kann. Zudem üben Sie dabei ein, wie Ihre Organisation mit Ereignissen umgeht.

# Die fünf Säulen des Framework

Wenn Sie ein Softwaresystem bauen, gehen Sie ähnlich vor wie beim Hausbau. Wenn das Fundament nicht trägt, können Risse auftreten und das Gebäude unbrauchbar machen. Wenn Sie die Architektur einer Technologielösung planen und die fünf Säulen Operative Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz und Kostenoptimierung vernachlässigen, kann es schwer werden, ein System zu schaffen, das Ihre Erwartungen und Anforderungen erfüllt. Berücksichtigen Sie aber diese Säulen in Ihrer Architektur, steht am Ende ein stabiles, effizientes System. Und das gibt Ihnen Freiraum, um sich auf andere Designaspekte (z. B. funktionale Anforderungen) zu konzentrieren.

## Betriebliche Exzellenz

Die (Säule) Säule beinhaltet (Beschreibung)

Die Säule für die betriebliche Exzellenz gibt einen Überblick über konzeptionelle Grundsätze, Best Practices und Fragen. Obligatorische Anleitungen zur Implementierung finden Sie im Whitepaper zur Säule für die betriebliche Exzellenz.

### Konzeptionelle Grundsätze

Es gibt in der Cloud (Anzahl) konzeptionelle Grundsätze für (untere Säule):

- **Betriebliche Vorgänge als Code ausführen ("Operations-as-Code")**: In der Cloud können Sie die gleichen technischen Vorgehensweisen wie bei Anwendungscode in Ihrer gesamten Umgebung anwenden. Sie können sämtliche Workloads (Anwendungen, Infrastruktur) als Code definieren und mit Code aktualisieren. Sie können Ihre betrieblichen Verfahren als Code implementieren und deren Ausführung automatisieren, indem Sie sie von Ereignissen auslösen lassen. Indem der Betrieb als Code ausgeführt wird, werden menschliche Fehler ausgeräumt und einheitliche Reaktionen auf Ereignisse möglich gemacht.
- **Dokumente kommentieren**: In einer lokalen Umgebung werden Dokumente manuell erstellt und von Anwendern genutzt. Im Falle von Änderungen ist es aber schwierig, die Dokumentation auf dem Laufenden zu halten. In der Cloud dagegen können Sie nach jedem Build-Vorgang kommentierende Dokumente automatisch erstellen (oder manuell erstellte Dokumente automatisch kommentieren) lassen. Kommentierende Dokumente können von Anwendern und Systemen genutzt werden. Verwenden Sie Anmerkungen als Eingaben für Ihren Betriebscode.
- **Kleine, häufige und umkehrbare Änderungen vornehmen**: Legen Sie Workloads so aus, dass es möglich ist, Komponenten regelmäßig zu aktualisieren. Nehmen Sie Änderungen in kleinen Schritten vor, die wieder zurückgenommen werden können (ohne dass Kunden dadurch beeinträchtigt werden, sofern möglich).

- **Betriebliche Verfahren regelmäßig nachbessern**: Suchen Sie beim Einsatz betrieblicher Verfahren nach Möglichkeiten, diese zu verbessern. Entwickeln Sie beim Ausbau Ihrer Workloads auch Ihre Verfahren entsprechend weiter. Legen Sie regelmäßige Termine fest, an denen überprüft wird, ob alle Verfahren effektiv und alle Teams mit den Verfahren vertraut sind.
- **Fehlern vorbeugen**: Führen Sie vorbeugende Übungen durch, um potenzielle Fehlerquellen zu identifizieren, damit diese behoben oder umgangen werden können. Testen Sie Ihre Ausfallszenarien und stellen Sie sicher, dass Sie deren Auswirkungen kennen. Testen Sie Ihre Reaktionsverfahren, um sicherzustellen, dass diese wirksam sind und dass Ihre Teams mit deren Ausführung vertraut sind. Legen Sie regelmäßige Termine fest, an denen getestet wird, wie Workloads und Teams auf simulierte Ereignisse reagieren.
- **Aus allen betrieblichen Ausfällen lernen**: Ziehen Sie aus allen betrieblichen Zwischenfällen und Ausfällen entsprechende Lehren und treiben Sie geeignete Verbesserungen voran. Geben Sie Ihre Erkenntnisse an alle Teams in Ihrer gesamten Organisation weiter.

# Definition

Es gibt in der Cloud (Anzahl) Bereiche, in denen bewährte Methoden für (untere Säule) zur Anwendung kommen:

- **Vorbereitung**
- **Betrieb**
- **Verbesserung**

Operations-Teams müssen ihr Handwerk beherrschen und wissen, was der Kunde benötigt, um das Unternehmen effektiv und effizient unterstützen zu können. Das Operations-Team stellt Verfahren für die Reaktion auf betriebliche Ereignisse auf, wendet diese an und prüft deren Wirksamkeit anhand geschäftlicher Anforderungen nach. Das Operations-Team sammelt Metriken, mit denen die Fortschritte bestimmter geschäftlicher Ziele nachgemessen wird. Ständig ändert sich alles – Ihr geschäftliches Umfeld, Ihre geschäftlichen Prioritäten, die Anforderungen Ihrer Kunden usw. Daher ist es wichtig, den Betrieb so zu konzeptionieren, dass ständige Weiterentwicklungen möglich sind und neue Erkenntnisse im laufenden Betrieb implementiert werden können.

# Bewährte Methoden

## *Vorbereitung*

Für die betriebliche Effizienz ist eine wirkungsvolle Vorbereitung unerlässlich. Der geschäftliche Erfolg basiert auf gemeinsamen Zielen und der Kommunikation zwischen den Geschäfts-, Entwicklungs- und Operations-Teams. Gängige Standards vereinfachen das Design und die Verwaltung von Workloads und ermöglichen so den betrieblichen Erfolg. Statten Sie Workloads mit Mechanismen aus, um Anwendungs-, Plattform- und Infrastrukturkomponenten zu überwachen und Einblick in Kundenerfahrung und -verhalten zu erhalten.

Erstellen Sie Mechanismen, die nachprüfen, ob Workloads – oder Änderungen – für den Einsatz in der Produktionsumgebung bereit sind und vom Betrieb auch unterstützt werden. Die betriebliche Bereitschaft wird über Checklisten überprüft, um sicherzustellen, dass ein Workload vorab festgelegte Standards erfüllt und erforderliche Verfahrensweisen in Runbooks und Playbooks niedergeschrieben sind. Überprüfen Sie, dass gut geschultes Personal für den Workload vorhanden ist. Testen Sie vor der Übergabe die Reaktionen auf betriebliche Ereignisse und Fehler. Üben Sie die Reaktionen in unterstützten Umgebungen mittels Fehlersimulationen und Übungsveranstaltungen.

AWS ermöglicht Operations-as-Code in der Cloud und bietet die Möglichkeit, sicher zu experimentieren, betriebliche Verfahren zu entwickeln und Ausfälle zu üben. Durch den Einsatz von AWS CloudFormation verfügen Sie über konsistente, auf Vorlagen basierende und in einer Sandbox befindliche Entwicklungs-, Test- und Produktionsumgebungen mit steigenden Leveln von operativer Kontrolle. Mittels verschiedener Protokollierungs- und Überwachungsfunktionen gibt Ihnen AWS auf allen Ebenen Einblick in Ihre Workloads. Über Amazon CloudWatch, AWS CloudTrail und VPC Flow Logs können Daten über die Verwendung von Ressourcen, APIs (Application Programming Interfaces, Anwendungsschnittstellen) und Protokolle über den Netzwerkdatenverkehr gesammelt werden. Mit dem collectd-Plug-in oder dem CloudWatch Logs-Agenten können Sie Informationen über das Betriebssystem in CloudWatch zusammenfassen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule). (Eine Liste mit Fragen und bewährten Methoden zu (untere Säule) finden Sie im Anhang.).

**OPS 1: Wie können Sie Ihre Prioritäten bestimmen?**

Alle Beteiligten müssen verstehen, welchen Anteil sie am geschäftlichen Erfolg haben. Setzen Sie sich gemeinsame Ziele, damit Sie die Prioritäten für Ressourcen festlegen können. Dadurch erzielen Ihre Bemühungen den größtmöglichen Nutzen.

**OPS 2: Wie können Sie Ihren Workload so konzipieren, dass ihr jeweiliger Zustand klar ersichtlich ist?**

Gestalten Sie Ihren Workload so, dass sie die Informationen liefert, die Sie benötigen, um ihren internen Zustand über alle Komponenten hinweg zu verstehen (z. B. mithilfe von Metriken, Protokollen und Traces). Auf diese Weise können Sie im Bedarfsfall effektiv reagieren.

**OPS 3: Wie können Sie Fehler reduzieren, die Fehlerbehebung erleichtern und den Ablauf bis zur Produktion verbessern?**

Verwenden Sie Strategien, die die Übertragung von Änderungen auf die Produktionsumgebung verbessern und Refactoring, schnelles Feedback zur Qualität sowie eine schnelle Fehlerbehebung ermöglichen. Dadurch fließen nützliche Änderungen schneller in die Produktion ein und es treten bei der Bereitstellung weniger Probleme auf. Zudem können Probleme, die durch Bereitstellungsaktivitäten verursacht werden, schnell aufgespürt und gelöst werden.

**OPS 4: Wie können Sie Bereitstellungsrisiken eindämmen?**

Verwenden Sie Ansätze, die ein schnelles Feedback zur Qualität liefern und eine umgehende Wiederherstellung des vorherigen Zustands nach Änderungen ermöglichen, die nicht zu den gewünschten Ergebnissen führen. Mit diesen Verfahren können Sie die Auswirkung von Problemen eindämmen, die durch die Bereitstellung von Änderungen entstehen.

**OPS 5: Wie bringen Sie in Erfahrung, ob Sie für die Unterstützung eines Workloads bereit sind?**

Bewerten Sie die betriebliche Bereitschaft Ihres Workloads, Prozesse und Verfahren sowie Ihrer Mitarbeiter, damit Sie die betrieblichen Risiken im Zusammenhang mit Ihrer Workload genau kennen.

Implementieren Sie für Ihre Workloads so wenige Architektur-Standards wie möglich. Wenn Sie für einen Workload einen Standard implementieren, vergleichen Sie die Kosten mit dem Nutzen, den dieser Standard bietet, sowie die damit verbundenen Betriebslasten. Reduzieren Sie die Anzahl unterstützter Standards, um das Risiko zu minimieren, dass unzulängliche Standards versehentlich angewendet werden. Mitglieder des Operations-Team sind meist voll ausgelastet.

Investieren Sie in die Implementierung betrieblicher Aktivitäten als Code, um die Produktivität von Operations-Mitarbeitern zu maximieren, Fehlerraten zu minimieren und automatisierte Reaktionen zu ermöglichen. Übernehmen Sie Bereitstellungsmethoden, die die Elastizität der Cloud ausnutzen, um die Vorabbereitstellung von Systemen und damit schnellere Implementierungen zu ermöglichen.

## *Betrieb*

Der erfolgreiche Betrieb eines Workloads wird daran gemessen, ob geschäftliche Resultate erreicht und Kundenanforderungen erfüllt werden. Definieren Sie zu erwartende Resultate, legen Sie fest, wie der Erfolg gemessen wird und geben Sie an, welche Workload-Metriken und betrieblichen Metriken in Berechnungen verwendet werden sollen, mit denen festgestellt wird, ob der Betrieb erfolgreich ist. Beachten Sie, dass der betriebliche Status sowohl den Status des Workloads als auch den Status und Erfolg der betrieblichen Vorgänge beinhaltet, die an dem Workload beteiligt sind (z. B. Bereitstellung und Vorfallreaktion). Legen Sie Ausgangswerte fest, von denen aus die Verbesserung oder Verschlechterung betrieblicher Vorgänge gemessen wird. Sammeln und analysieren Sie Ihre Metriken und prüfen Sie dann nach, wie weit diese mit ihrem Verständnis von betrieblichen Erfolgen übereinstimmen und welche Änderungen es im zeitlichen Verlauf gibt. Finden Sie anhand gesammelter Metriken heraus, ob kundenseitige und geschäftliche Anforderungen erfüllt werden, und stellen Sie fest, wo noch etwas verbessert werden kann.

Um betriebliche Exzellenz zu erreichen, ist eine effiziente und effektive Verwaltung betrieblicher Ereignisse erforderlich. Dies gilt sowohl für geplante als auch für ungeplante betriebliche Ereignisse. Greifen Sie bei bekannten Ereignissen auf vorab aufgestellte Runbooks zurück. Lassen Sie sich bei der Behebung anderer Ereignisse von Playbooks helfen. Priorisieren Sie Ihre Reaktionen auf Ereignisse anhand der Beeinträchtigungen, die das jeweilige Ereignis für den Geschäftsbetrieb und die Kunden mit sich bringt. Stellen Sie sicher, dass für einen Alarm, der bei einem bestimmten Ereignis ausgelöst werden soll, auch ein auszuführendes Verfahren inklusive einem zuständigen Besitzer festgelegt sind. Legen Sie vorab fest, welche Mitarbeiter für die Behebung eines Ereignisses zuständig sein sollen. Dazu gehören auch Auslöser für einen Eskalationsprozess, über den im Notfall weitere Mitarbeiter herangezogen werden sollen (d.h. ab einer bestimmten Zeitdauer, Schweregrad oder Umfang eines Vorfalls). Für den Fall, dass eine nicht vorab festgelegte Vorfallreaktion erforderlich ist, die möglicherweise den geschäftlichen Betrieb beeinträchtigen kann, legen Sie Personen fest, die über die nötige Autorität für Entscheidungen verfügen.

Geben Sie Informationen zum betrieblichen Status von Workloads über Dashboards und Mitteilungen weiter, die für die Zielgruppe (z. B. Kunde, Unternehmen, Entwickler, Operations-Team) zugeschnitten sind, damit diese Leute geeignete Maßnahmen durchführen können und wissen, wann der normale Betrieb wieder weitergeht.

Stellen Sie die Ursache von ungeplanten Ereignissen und unerwarteten Beeinträchtigungen geplanter Ereignisse fest. Diese Informationen werden verwendet, um Ihre Verfahren entsprechend zu aktualisieren, damit sich so etwas zukünftig nicht wiederholt. Teilen Sie gefundene Ursachen anderen Betroffenen mit.

In AWS können Sie Dashboard-Ansichten Ihrer Metriken generieren, die aus Workloads erfasst wurden oder systemeigenen aus AWS stammen. Sie können CloudWatch oder Anwendungen von Drittanbietern verwenden, um Ansichten von betrieb-

lichen Aktivitäten auf geschäftlicher, Workload-bezogener und betrieblicher Ebene zusammenzustellen und anzuzeigen. AWS stellt über seine Protokollierungsfähigkeiten (wie AWS X-Ray, CloudWatch, CloudTrail und VPC Flow Logs) Einblicke in Workloads bereit. So können Workload-Probleme identifiziert werden, was bei der Ursachensuche, Analyse und Behebung von Fehlern hilft.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**OPS 6: Wie können Sie den Zustand Ihres Workloads beurteilen?**

Definieren, erfassen und analysieren Sie Workload-Metriken, um einen Einblick in Workload-Ereignisse zu erhalten. Dies ist wichtig, damit Sie bei Bedarf entsprechende Maßnahmen ergreifen können.

**OPS 7: Wie können Sie den Zustand Ihrer Operationen beurteilen?**

Definieren, erfassen und analysieren Sie Metriken für Operationen, um einen Einblick in Ereignisse rund um Ihre operativen Abläufe zu erhalten. Dies ist wichtig, damit Sie bei Bedarf entsprechende Maßnahmen ergreifen können.

**OPS 8: Wie bewältigen Sie Workload- und operationsspezifische Ereignisse?**

Erarbeiten und prüfen Sie Verfahren für die Reaktion auf Ereignisse, um Beeinträchtigungen für Ihren Workload zu minimieren.

Routinemäßige Vorgänge sowie Reaktionen auf ungeplante Ereignisse sollten automatisiert werden. Manuelle Prozesse für Bereitstellungen, Verwaltung von Freigaben, Änderungen und Rollbacks sollten vermieden werden. Freigaben sollten nicht als große Batches erfolgen, die sporadisch erfolgen. Rollbacks sind bei großen Änderungen viel schwieriger. Wenn kein Rollback-Plan vorliegt oder wenn die Auswirkungen von Ausfällen nicht abgemildert werden können, besteht die Gefahr, dass die Kontinuität des Geschäftsbetriebs nicht aufrecht erhalten werden kann. Richten Sie Metriken so an geschäftlichen Anforderungen aus, dass bei Reaktionen die geschäftliche Kontinuität beibehalten wird. Wenn einmalige, dezentrale Metriken ein manuelles Eingreifen benötigen, führt dies bei ungeplanten Ereignissen zu einer größeren Unterbrechung des Betriebs.

## *Verbesserung*

Die Verbesserung betrieblicher Vorgänge ist unerlässlich, um die betriebliche Exzellenz dauerhaft aufrecht zu erhalten. Planen Sie Arbeitszyklen ein, um kontinuierlich kleinere Verbesserungen vorzunehmen. Beurteilen und priorisieren Sie in regelmäßigen Abständen Möglichkeiten für Verbesserungen (z. B. Anfragen nach Features, Behebung von Problemen, Compliance-Anforderungen), inklusive Workload- und Betriebsverfahren. Nehmen Sie Feedback-Schleifen in Ihre Verfahren auf, um Verbesserungsmöglichkeiten schnell zu erfahren und Rückmeldungen aus dem Praxisbetrieb zu dokumentieren.

Geben Sie die Dinge, die Sie erfahren, an andere Teams weiter, damit alle davon profitieren. Untersuchen Sie, ob Ihre neuen Erkenntnisse vielleicht Trends aufzeigen, und

führen Sie nachträglich teamübergreifende Analysen von operativen Metriken durch, um Verbesserungsmöglichkeiten und -methoden festzustellen. Implementieren Sie Änderungen, die zu Verbesserungen führen sollen, und beurteilen Sie deren Ergebnisse.

Mit den AWS Developer Tools können Sie kontinuierliche Build-, Test- und Bereitstellungsaktivitäten implementieren, die mit den verschiedensten Quellcode-, Build-, Test- und Bereitstellungs-Tools von AWS und Drittanbietern funktionieren. Die Ergebnisse von Bereitstellungsaktivitäten können genutzt werden, um Verbesserungsmöglichkeiten sowohl im Bereitstellungs- als auch im Entwicklungsbereich zu aufzuspüren. Sie können an Ihren Metrikdaten Analysen durchführen und Daten aus Betriebs- und Bereitstellungsaktivitäten integrieren, um festzustellen, wie sich diese Aktivitäten auf geschäftliche und kundenseitige Ziele auswirken. Diese Daten können in teamübergreifenden nachträglichen Analysen dazu genutzt werden, um Verbesserungsmöglichkeiten und -methoden zu ermitteln.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

| **OPS 9: Wie können Sie Operationen weiterentwickeln?** |
| --- |
| Kalkulieren Sie Zeit und Ressourcen für kontinuierliche schrittweise Verbesserungen ein, damit sich die Effektivität und Effizienz Ihrer Operationen ständig weiterentwickeln. |

Das Fundament für eine erfolgreiche Weiterentwicklung des Betriebs sind ständige kleinere Verbesserungen, das Bereitstellen sicherer Umgebungen und Zeitrahmen zum Experimentieren, Entwickeln und Testen von Verbesserungen sowie das Schaffen eines Umfeldes, in dem alle ermutigt werden, aus Fehlern zu lernen. Die operative Unterstützung für Sandbox-, Entwicklungs-, Test- und Produktionsumgebungen, mit steigenden Leveln von operativer Kontrolle, erleichtert die Entwicklung und steigert die Kalkulierbarkeit, dass Änderungen zu erfolgreichen Ergebnissen führen.

# Wichtige AWS-Services

Das für (Säule) maßgebliche (Angebot) ist (Service-Name), (Service-Beschreibung) Die folgenden Services und Funktionen unterstützen die (Anzahl) Bereiche in (untere Säule):

- **Vorbereitung**: AWS Config- und AWS Config-Regeln können verwendet werden, um Standards für Workloads zu erstellen und um festzustellen, ob Umgebungen mit diesen Standards kompatibel sind, bevor sie in den Produktionsbetrieb geschaltet werden.
- **Betrieb**: Amazon CloudWatch erlaubt es Ihnen, den betrieblichen Status eines Workloads zu überwachen.
- **Verbesserung**: Amazon Elasticsearch Service (Amazon ES) erlaubt Ihnen das Analysieren Ihrer Protokolldaten, um schnell und sicher umsetzbare Einblicke zu erhalten.

## Ressourcen

Werfen Sie einen Blick auf die folgenden Ressourcen, um mehr über unsere bewährten Methoden für (Säule) zu erfahren.

**Dokumentation**

- DevOps and AWS

**Whitepaper**

- Operational Excellence Pillar

**Video**

- DevOps at Amazon

# Sicherheit

Die (Säule) Säule beinhaltet (Beschreibung)

Die Säule für Sicherheit bietet einen Überblick über konzeptionelle Grundsätze, Best Practices und Fragen. Verbindliche Leitlinien zur Implementierung finden Sie im Whitepaper der Säule für Sicherheit.

## Konzeptionelle Grundsätze

Es gibt in der Cloud (Anzahl) konzeptionelle Grundsätze für (untere Säule):

- **Implementieren einer starken Identitätsgrundlage**: Implementieren Sie das Prinzip der geringsten Rechte, und erzwingen Sie die Trennung von Pflichten durch eine entsprechende Autorisierung für jede Interaktion mit Ihren AWS-Ressourcen. Zentralisieren Sie die Rechteverwaltung, und reduzieren oder eliminieren Sie langfristig geltende Anmeldeinformationen.
- **Nachverfolgbarkeit**: Überwachen, melden und prüfen Sie Aktionen und Änderungen in Ihrer Umgebung in Echtzeit. Integrieren Sie Protokolle und Kennzahlen in Systeme, um automatisch reagieren und Maßnahmen ergreifen zu können.
- **Sicherheit auf allen Ebenen**: Verwenden Sie eine tiefgreifende Abwehrstrategie unter Einbindung anderer Sicherheitskontrollen, anstatt sich nur auf den Schutz einer einzelnen äußeren Schicht zu konzentrieren. Schützen Sie alle Ebenen (Edge-Netzwerk, VPC, Subnetz, Load Balancer, alle Instances, Betriebssystem, Anwendungen usw.).
- **Automatisieren bewährter Sicherheitsverfahren**: Mithilfe automatisierter softwarebasierter Sicherheitsmechanismen können Sie Ihr System sicher, schnell und

kosteneffektiv skalieren. Erstellen Sie sichere Architekturen, einschließlich implementierter Kontrollen, die als Code in versionsgesteuerten Vorlagen definiert und verwaltet werden.

- **Schutz von Daten während der Übertragung und im Ruhezustand**: Klassifizieren Sie Daten nach Sensibilität und Nutzungsmechanismen wie Verschlüsselung, Tokenisierung und Zugriff, sofern zutreffend.
- **Trennen von Benutzern und Daten**: Erstellen Sie Mechanismen und Tools, um den direkten Zugriff oder die manuelle Verarbeitung von Daten zu reduzieren oder gänzlich zu eliminieren. Sie reduzieren dadurch das Risiko, dass sensible Daten verloren gehen, geändert werden oder anderweitigen Benutzerfehlern unterliegen.
- **Vorbereitung auf Sicherheitsereignisse**: Seien Sie auf Vorfälle vorbereitet. Richten Sie entsprechend Ihren organisatorischen Anforderungen ein Verfahren zur Vorfallverwaltung ein. Simulieren Sie Vorfallreaktionen und nutzen Sie automatisierbare Tools, um die Erkennung, Untersuchung und Wiederherstellung zu beschleunigen.

# Definition

Es gibt in der Cloud (Anzahl) Bereiche, in denen bewährte Methoden für (untere Säule) zur Anwendung kommen:

- **Identity and Access Management**
- **Aufdeckende Kontrollen**
- **Schutz der Infrastruktur**
- **Datenschutz**
- **Vorfallreaktion**

Vor der Entwicklung eines Systems ist es wichtig, geeignete Sicherheitsverfahren festzulegen. Sie müssen die einzelnen Prozesse steuern können. Wichtig ist auch, dass Sie Sicherheitsvorfälle erkennen, Ihre Systeme und Services schützen und die Vertraulichkeit und Integrität von Daten durch entsprechende Schutzmaßnahmen wahren können. Richten Sie ein gut definiertes und geübtes Verfahren ein, das es Ihnen ermöglicht, auf Sicherheitsvorfälle zu reagieren. Derartige Tools und Techniken sind unabdinglich, um Ihr Unternehmen vor finanziellen Verlusten zu schützen und gesetzliche Vorgaben zu erfüllen.

Das AWS-Modell der gemeinsamen Verantwortlichkeit ermöglicht Unternehmen, durch die Migration zur Cloud ihre Sicherheits- und Compliance-Ziele zu erfüllen. Dadurch, dass sich AWS um den physischen Schutz der Infrastruktur unserer Cloud-Services kümmert, können Sie sich als AWS-Kunden darauf fokussieren, mithilfe unserer Services Ihre Ziele zu erreichen. Sie haben in der AWS Cloud auch einen verbesser-

ten Zugriff auf Sicherheitsdaten und können automatisch auf Sicherheitsereignisse reagieren.

# Bewährte Methoden

## *Identity and Access Management*

Das Identity and Access Management ist ein wichtiger Bestandteil eines Informationssicherheitsprogramms. Es stellt sicher, dass nur autorisierte und authentifizierte Benutzer und nur in dem von Ihnen gewünschten Umfang auf Ihre Ressourcen zugreifen können. Definieren Sie beispielsweise Prinzipien (d. h. Benutzer, Gruppen, Services und Rollen, die Aktionen in Ihrem Konto durchführen), erstellen Sie entsprechende Richtlinien, und implementieren Sie eine strenge Verwaltung von Anmeldeinformationen. Diese Elemente der Rechteverwaltung bilden die Grundlage der Authentifizierung und Autorisierung.

In AWS erfolgt die Rechteverwaltung primär durch AWS Identity and Access Management (IAM)-Service. Damit können Sie sowohl den Benutzerzugriff als auch den programmgesteuerten Zugriff auf AWS-Services und -Ressourcen steuern. Wenden Sie detaillierte Richtlinien an, um Benutzern, Gruppen, Rollen oder Ressourcen Berechtigungen zuzuweisen. Darüber hinaus können Sie die Verwendung starker Kennwörter erzwingen. Sie können deren Komplexität vorgeben, Wiederverwendungen vermeiden und Multi-Factor Authentication (MFA) nutzen. Sie haben die Möglichkeit, die Rechteverwaltung mit Ihrem Verzeichnisdienst zu verbinden. Wenn Sie Workloads haben, die Zugriff auf AWS erfordern, ermöglicht IAM diesen sicher durch Rollen, Instance-Profile, Identitätsverbund und temporäre Anmeldeinformationen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule). (Eine Liste mit Fragen und bewährten Methoden zu (untere Säule) finden Sie im Anhang.).

**SEC 1: Wie verwalten Sie Anmeldeinformationen und die Authentifizierung?**

Anmeldeinformationen und Authentifizierungsmechanismen umfassen Passwörter, Tokens und Schlüssel, die entweder direkt oder indirekt Zugriff in Ihren Workload gewähren. Schützen Sie Anmeldeinformationen durch entsprechende Mechanismen, um das Risiko einer unbeabsichtigten oder böswillligen Verwendung zu reduzieren.

**SEC 2: Wie kontrollieren Sie den Zugriff durch Personen?**

Kontrollieren Sie den Zugriff durch Personen, indem Sie Mechanismen implementieren, die sich an definierten Geschäftsanforderungen orientieren. Dadurch reduzieren Sie das Risiko und die Auswirkung eines nicht autorisierten Zugriffs. Dies gilt für berechtigte Benutzer und Administratoren Ihres AWS-Kontos sowie für Endbenutzer Ihrer Anwendung.

**SEC 3: Wie kontrollieren Sie den programmgesteuerten Zugriff?**

Kontrollieren Sie den programmgesteuerten oder automatischen Zugriff mit entsprechend definiertem, eingeschränktem und getrenntem Zugriff, um das Risiko eines nicht autorisierten Zugriffs zu verringern. Der programmgesteuerte Zugriff umfasst den internen Zugriff auf Ihren Workload sowie den Zugriff auf AWS-Ressourcen.

Anmeldeinformationen dürfen nicht zwischen Benutzern oder Systemen weitergegeben werden. Der Benutzerzugriff sollten nach dem Prinzip der geringsten Rechte erfolgen, passwortgeschützt sein und nur mittels MFA möglich sein. Der programmgesteuerte Zugriff etwa durch API-Aufrufe von AWS-Services sollte mit eingeschränkten Berechtigungen und temporären Anmeldeinformationen erfolgen, die beispielsweise durch den AWS Security Token Service ausgegeben werden.

AWS bietet Ressourcen, die Ihnen das Identity and Access Management erleichtern. Mehr zu den Best Practices erfahren Sie in unseren praktischen Übungen zu den Themen Verwaltung von Anmeldeinformationen und Authentifizierung, Steuerung des Benutzerzugriffssowie Steuerung des programmgesteuerten Zugriffs.

## *Aufdeckende Kontrollen*

Aufdeckende Kontrollen bieten Ihnen die Möglichkeit, potenzielle Sicherheitsbedrohungen oder -vorfälle zu erkennen. Die Kontrollmechanismen sind ein wesentlicher Bestandteil von Governance-Frameworks. Sie können zur Unterstützung von Qualitätssicherungsverfahren, zur Einhaltung gesetzlicher Vorgaben und Pflichten sowie zur Erkennung und Abwehr von Bedrohungen genutzt werden. Es gibt unterschiedliche Arten aufdeckender Kontrollen. Eine Bestandserfassung der Ressourcen und ihrer detaillierten Attribute trägt beispielsweise zu einer effektiveren Entscheidungsfindung (und Lebenszyklussteuerung) bei, wenn es darum geht, operative Ausgangswerte festzulegen. Sie können auch durch eine interne Prüfung der mit Informationssystemen verbundenen Steuerelemente sicherstellen, dass Ihre Verfahren den Richtlinien und Anforderungen entsprechen. Basierend auf definierten Bedingungen sind passende automatisierte Benachrichtigungen möglich. Diese Steuerelemente sind wichtige reaktive Faktoren, die es Ihrem Unternehmen ermöglichen, den Umfang anomaler Aktivitäten zu ermitteln und zu verstehen.

In AWS können Sie aufdeckende Kontrollen durch Verarbeitungsprotokolle, Ereignisse und Überwachungsfunktionen implementieren, die eine Prüfung, automatisierte Analyse und Benachrichtigung ermöglichen. Mit CloudTrail-Protokollen, AWS API-Aufrufen und CloudWatch können Sie Kennzahlen überwachen und Benachrichtigungen senden. Der Konfigurationsverlauf ist mit AWS Config einsehbar. Amazon GuardDuty ist ein verwalteter Service zur Bedrohungserkennung, der Ihre AWS-Konten und -Workloads zu deren Schutz fortlaufend auf böswillige oder unbefugte Verhaltensweisen überwacht. Mit Serviceprotokollen etwa von Amazon Simple Storage Service (Amazon S3) können Sie Zugriffsanfragen protokollieren.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

| |
|---|
| **SEC 4: Wie erkennen und untersuchen Sie Sicherheitsereignisse?** |
| Erfassen und analysieren Sie Ereignisse mithilfe von Protokollen und Kennzahlen, um Einblick zu erhalten. Ergreifen Sie Maßnahmen bei Sicherheitsereignissen und potenziellen Bedrohungen, um Ihren Workload zu schützen. |
| **SEC 5: Wie wehren Sie sich gegen neue Sicherheitsbedrohungen?** |
| Bleiben Sie bei den AWS Best Practices und Best Practices der Branche sowie bei Informationen zu Bedrohungen auf dem Laufenden, um sich über neue Risiken im Klaren zu sein. Dadurch haben Sie die Möglichkeit, ein Gefahrenmodell zu erstellen, um entsprechende Kontrollen zum Schutz Ihres Workloads zu ermitteln, zu priorisieren und zu implementieren. |

Die Protokollverwaltung ist für ein architektonisch gutes Design wichtig, um so vielfältige Bereiche wie Sicherheit, Forensik sowie die Einhaltung gesetzlicher Vorgaben abzudecken. Um potenzielle Sicherheitsvorfälle ermitteln zu können, müssen diese Protokolle analysiert und bei Bedarf entsprechende Maßnahmen ergriffen werden. AWS bietet Funktionen, die die Protokollverwaltung erleichtern. Sie können damit einen Lebenszyklus für die Datenaufbewahrung festlegen oder angeben, wo Daten gespeichert, archiviert oder schließlich gelöscht werden. Dies vereinfacht die vorhersehbare und zuverlässige Datenverarbeitung und senkt die Kosten.

## *Schutz der Infrastruktur*

Zum Schutz der Infrastruktur sind Steuermethoden wie etwa eine tiefgreifende Abwehr erforderlich, um Best Practices sowie organisatorische und gesetzliche Verpflichtungen zu erfüllen. Die Nutzung dieser Methoden ist für erfolgreiche, kontinuierliche Betriebsabläufe sowohl in der Cloud als auch lokal ausschlaggebend.

AWS ermöglicht die Überprüfung zustandsbehafteter und zustandsloser Pakete. Sie können dafür wahlweise AWS-native Technologien oder im AWS Marketplace angebotene Partnerprodukte und -services nutzen. Amazon Virtual Private Cloud (Amazon VPC) wird empfohlen, um eine private, sichere und skalierbare Umgebung zu erstellen, in der Sie Ihre Topologie, einschließlich Gateways, Routing-Tabellen sowie öffentlichen und privaten Subnetzen definieren können.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**SEC 6: Wie schützen Sie Ihre Netzwerke?**

Öffentliche und private Netzwerke erfordern mehrere Ebenen der Abwehr, um Schutz vor externen und internen netzwerkbasierten Bedrohungen zu bieten.

**SEC 7: Wie schützen Sie Ihre Datenverarbeitungsressourcen?**

Datenverarbeitungsressourcen in Ihrem Workload erfordern mehrere Ebenen der Abwehr zum Schutz vor externen und internen Bedrohungen. Zu den Datenverarbeitungsressourcen zählen EC2-Instances, Container, AWS Lambda-Funktionen, Datenbankservices, IoT-Geräte und mehr.

Ungeachtet der Umgebung sollten mehrere Abwehrebenen vorhanden sein. Was den Schutz der Infrastruktur anbelangt, gelten viele der Konzepte und Methoden für Cloud- und lokale Modelle gleichermaßen. Das Erzwingen des Grenzschutzes, die Überwachung von Ein- und Ausgangspunkten sowie die umfassende Protokollierung, Überwachung und Benachrichtigung sind für einen effektiven Informationssicherheitsplan wichtig.

AWS-Kunden können die Konfiguration der Amazon Elastic Compute Cloud (Amazon EC2) sowie von Amazon EC2 Container Service-Containern (Amazon ECS) und AWS Elastic Beanstalk-Instances anpassen oder härten und in einem unveränderlichen Amazon Machine Image (AMI) speichern. Dadurch erhalten alle neuen virtuellen Server (Instances), die mit diesem AMI gestartet werden, diese gehärtete Konfiguration. Dabei spielt es keine Rolle, ob sie durch Auto Scaling oder manuell ausgelöst wurden.

## *Datenschutz*

Vor der Entwicklung eines Systems sollten grundlegende Sicherheitspraktiken implementiert werden. Mittels Datenklassifizierung lassen sich beispielsweise organisatorische Daten nach Sensitivität kategorisieren. Die Verschlüsselung macht sie zudem für unbefugte Benutzer unleserlich. Derartige Tools und Techniken sind unabdinglich, um Ihr Unternehmen vor finanziellen Verlusten zu schützen und gesetzliche Vorgaben zu erfüllen.

In AWS können Sie Daten mit folgenden Maßnahmen schützen:

- Als AWS-Kunden behalten Sie die vollständige Kontrolle über Ihre Daten.
- AWS erleichtert Ihnen die Datenverschlüsselung und die Schlüsselverwaltung, einschließlich einer regulären Schlüsselrotation. Sie können diese auf einfache Weise selbst verwalten oder von AWS automatisieren lassen.
- Sie haben Zugriff auf detaillierte Protokolle mit wichtigen Angaben etwa zu Dateizugriffen und -änderungen.

- Die Speichersysteme von AWS zeichnen sich durch eine exzeptionelle Ausfallsicherheit aus. Amazon S3 Standard, S3 Standard-IA, S3 One Zone-IA und Amazon Glacier bieten beispielsweise eine einjährige Objektlanglebigkeit von 99,999999999 %. Dies entspricht einem jährlichen erwarteten Verlust von 0,000000001 % der Objekte.
- Die Versionierung, die in ein umfassenderes Verfahren zur Datenlebenszyklusverwaltung eingebunden sein kann, bietet Schutz vor versehentlichen Überschreibungen, Löschungen und ähnlichen Gefahren.
- AWS veranlasst niemals eine Verschiebung von Daten zwischen Regionen. Die in einer Region platzierten Inhalte bleiben in dieser Region, sofern Sie dies nicht ausdrücklich mithilfe einer Funktion oder eines Services veranlassen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**SEC 8: Wie klassifizieren Sie Ihre Daten?**

Die Klassifizierung stellt eine Methode dar, um Daten anhand von Vertraulichkeitsstufen zu kategorisieren. Ziel dabei ist, geeignete Schutz- und Aufbewahrungskontrollen zu bestimmen.

**SEC 9: Wie schützen Sie Ihre ruhenden Daten?**

Um den Schutz von ruhenden Daten zu gewährleisten, müssen Anforderungen definiert und Kontrollmechanismen, einschließlich einer Verschlüsselung, implementiert werden. Dadurch lässt sich das Risiko eines nicht autorisierten Zugriffs oder eines Datenverlusts reduzieren.

**SEC 10: Wie schützen Sie Ihre Daten bei der Übertragung?**

Um den Schutz von Daten bei der Übertragung zu gewährleisten, müssen Anforderungen definiert und Kontrollmechanismen, einschließlich einer Verschlüsselung, implementiert werden. Dadurch lässt sich das Risiko eines unberechtigten Zugriffs auf Daten oder einer Offenlegung von Daten reduzieren.

AWS bietet mehrere Möglichkeiten zur Verschlüsselung von Daten im Ruhezustand und während der Übertragung. Unsere Services enthalten Funktionen, die die Verschlüsselung Ihrer Daten erleichtern. Wir haben beispielsweise in Amazon S3 eine serverseitige Verschlüsselung (Server-Side Encryption, SSE) implementiert, die die Speicherung Ihrer Daten in verschlüsselter Form vereinfacht. Sie können auch das komplette Ver- und -Entschlüsselungsverfahren mit HTTPS (generell als SSL-Terminierung bekannt) mit Elastic Load Balancing (ELB) arrangieren.

## *Vorfallreaktion*

Obwohl die präventiven und aufdeckenden Kontrollen mittlerweile extrem ausgereift sind, sollte Ihr Unternehmen dennoch Verfahren etablieren, um auf Sicherheitsvorfälle reagieren und mögliche Auswirkungen mindern zu können. Wie effektiv Ihre Teams bei einem Vorfall reagieren können, um Systeme zu isolieren oder zu bergen

und Betriebsabläufe in einem bekanntermaßen funktionierenden Zustand wiederherzustellen, hängt stark von der Architektur des Workloads ab. Indem Sie sich mit entsprechenden Tools und Zugriffsmöglichkeiten auf Sicherheitsvorfälle vorbereiten und die Vorfallreaktion regelmäßig im Rahmen von Gamedays üben, stellen Sie eine zeitnahe Untersuchung und Wiederherstellung sicher.

In AWS ermöglichen die folgenden Praktiken eine effektive Vorfallreaktion:

- Eine detaillierte Protokollierung wichtiger Informationen etwa zu Dateizugriffen und -änderungen.
- Ereignisse können automatisch verarbeitet werden und Tools auslösen, die Reaktionen über AWS APIs automatisieren.
- Sie können vorab mit AWS CloudFormation entsprechende Tools und einen "Reinraum" bereitstellen. Sie erhalten dadurch eine sichere, isolierte Umgebung für forensische Untersuchungen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**SEC 11: Wie reagieren Sie auf einen Vorfall?**

Auf Sicherheitsvorfälle vorbereitet zu sein, ist entscheidend, um diese rasch untersuchen und darauf entsprechend reagieren zu können. Dadurch sind Sie in der Lage, mögliche Unterbrechungen der Geschäftsabläufe zu minimieren.

Wichtig ist, dass Sie eine Möglichkeit haben, Ihrem Informationssicherheitsteam für forensische Zwecke schnell Zugriff gewähren zu können. Automatisieren Sie sowohl die Isolation von Instances als auch die Erfassung von Daten und Zuständen.

# Wichtige AWS-Services

Das für (Säule) maßgebliche (Angebot) ist (Service-Name), (Service-Beschreibung) Die folgenden Services und Funktionen unterstützen die (Anzahl) Bereiche in (untere Säule):

- **Identity and Access Management**: Mit IAM können Sie den Zugriff auf AWS-Services und -Ressourcen sicher steuern. MFA erweitert den Benutzerzugriff um eine zusätzliche Schutzebene. In AWS Organizations können Sie Richtlinien für mehrere AWS-Konten zentral verwalten und erzwingen.
- **Aufdeckende Kontrollen**: AWS CloudTrail zeichnet AWS API-Aufrufe auf, während AWS Config eine detaillierte Bestandsaufnahme Ihrer AWS-Ressourcen und -Konfiguration bietet. Amazon GuardDuty ist ein verwalteter Service zur Bedrohungserkennung, der Vorgänge fortlaufend auf böswillige oder unbefugte Verhaltensweisen überwacht. Amazon CloudWatch ist ein Überwachungsservice für AWS-Ressour-

cen, der CloudWatch Events auslösen kann, um Sicherheitsmaßnahmen zu automatisieren.

- **Schutz der Infrastruktur**: In der Amazon Virtual Private Cloud (Amazon VPC) können Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten. Amazon CloudFront ist ein globales Netzwerk zur Inhaltsbereitstellung, das Ihren Benutzern Daten, Videos, Anwendungen und APIs sicher liefert. Zum Schutz vor DDoS kann der Service in AWS Shield integriert werden. AWS WAF ist eine Web Application Firewall, die in Amazon CloudFront oder Application Load Balancer bereitgestellt wird. Sie schützt Ihre Webanwendungen vor gängigen Webbedrohungen.
- **Datenschutz**: Services wie ELB, Amazon Elastic Block Store (Amazon EBS), Amazon S3 und Amazon Relational Database Service (Amazon RDS) bieten Verschlüsselungsfunktionen, um Ihre Daten während der Übertragung und im Ruhezustand zu schützen Amazon Macie erkennt, klassifiziert und schützt sensible Daten automatisch. AWS Key Management Service (AWS KMS) erleichtert Ihnen das Erstellen und Steuern von Verschlüsselungsschlüsseln.
- **Vorfallreaktion**: Gewähren Sie Notfallteams und Reaktionstools mit IAM entsprechende Autorisierungen. Mit AWS CloudFormation kann zu Untersuchungszwecken eine vertrauenswürdige Umgebung oder ein Reinraum geschaffen werden. Amazon CloudWatch Events ermöglichen Ihnen, Regeln zu erstellen, die automatisierte Reaktionen, einschließlich AWS Lambda-Funktionen auslösen.

# Ressourcen

Werfen Sie einen Blick auf die folgenden Ressourcen, um mehr über unsere bewährten Methoden für (Säule) zu erfahren.

**Dokumentation**

- AWS Cloud Security
- AWS Compliance
- AWS Security Blog

**Whitepaper**

- Security Pillar
- AWS Security Overview
- AWS Security Best Practices
- AWS Risk and Compliance

**Video**

- AWS Security State of the Union
- Shared Responsibility Overview

# Zuverlässigkeit

Die (Säule) Säule beinhaltet (Beschreibung)

Die Säule für Zuverlässigkeit bietet einen Überblick über konzeptionelle Grundsätze, bewährte Methoden und Fragen. Obligatorische Anleitungen zur Implementierung finden Sie im Whitepaper der Säule für Zuverlässigkeit.

## Konzeptionelle Grundsätze

Es gibt in der Cloud (Anzahl) konzeptionelle Grundsätze für (untere Säule):

- **Wiederherstellungsverfahren testen**: In einer lokalen Umgebung werden Tests häufig durchführt, um nachzuweisen, dass ein System in einem bestimmten Szenario funktioniert. Das Testen wird in der Regel nicht auf das Validieren von Wiederherstellungsstrategien angewandt. In der Cloud können Sie testen, in welchen Situationen Ihr System Fehler produziert, und Sie können Ihre Wiederherstellungsverfahren validieren. Mit Automatisierung können Sie verschiedene Fehler simulieren oder Szenarios reproduzieren, die zuvor zu Fehlern geführt haben. Auf diese Weise können Sie Fehlerpfade offenbaren, die Sie testen und korrigieren können, bevor ein tatsächliches Fehlerszenario auftritt, und damit das Risiko reduzieren, dass Komponenten ausfallen, die zuvor nicht getestet wurden.
- **Automatische Wiederherstellung nach einem Fehler**: Durch die Überwachung wichtiger Leistungskennzahlen (KPIs) eines Systems können Sie die Automatisierung auslösen, sobald ein Schwellenwert überschritten wurde. Dies ermöglicht eine automatische Benachrichtigung bei und Verfolgung von Fehlern und die Einleitung einer automatisierten Wiederherstellung, die eine Fehlerumgehung bietet oder den Fehler behebt. Bei einer ausgepfeilteren Automatisierung ist es möglich, Fehler vor ihrem eigentlichen Auftreten zu antizipieren und zu beheben.
- **Horizontale Skalierung zur Erhöhung der aggregierten Systemverfügbarkeit durchführen**: Ersetzen Sie eine große Ressource durch mehrere kleine Ressourcen, um die Auswirkung eines einzelnen Fehlers auf das Gesamtsystem zu reduzieren. Verteilen Sie Anfragen auf mehrere kleinere Ressourcen, um sicherzustellen, dass sie auf keinen gemeinsamen Fehlerpunkt zugreifen.
- **Sorgen in Bezug auf die verfügbare Kapazität beiseite schieben**: Eine häufige Fehlerursache in lokalen Systemen ist die Ressourcensättigung. Ein solches Szenario liegt vor, wenn die Nachfrage auf einem System die Kapazität dieses System überschreitet (ein häufiges Ziel von Denial-of-Service-Angriffen). In der Cloud können

Sie die Nachfrage und die Systemnutzung überwachen und das Hinzufügen oder Entfernen von Ressourcen automatisieren, um einen optimale Grad zur Erfüllung des Bedarfs ohne Über- oder Unterbereitstellung aufrechtzuerhalten.

- **Änderungen an der Automatisierung verwalten**: Änderungen an Ihrer Infrastruktur sollten über Automatisierung vorgenommen werden. Bei den zu verwaltenden Änderungen handelt sich um Änderungen an der Automatisierung.

# Definition

Es gibt in der Cloud (Anzahl) Bereiche, in denen bewährte Methoden für (untere Säule) zur Anwendung kommen:

- **Grundlagen**
- **Änderungsmanagement**
- **Fehlerverwaltung**

Zur Sicherstellung der Zuverlässigkeit muss ein System eine gut strukturierte Grundlage und Überwachung auf Basis von Verfahren zum Behandeln von bedarfs- oder anforderungsbasierten Änderungen aufweisen. Das System sollte so konzipiert sein, dass Fehler erkannt und automatisch im Rahmen einer Selbstheilung behoben werden.

# Bewährte Methoden

## *Grundlagen*

Vor dem Aufbau der Architektur eines System sollten grundlegende Anforderungen, die sich auf die Zuverlässigkeit auswirken, implementiert werden. So müssen Sie beispielsweise Ihre Rechenzentren mit einer ausreichenden Netzwerkbandbreite versorgen. Diese Anforderungen werden gelegentlich vernachlässigt (da sie nicht Teil eines Einzelprojekts sind). Diese Vernachlässigung kann sich stark auf die Bereitstellbarkeit eines zuverlässigen Systems auswirken. In einer lokalen Umgebung können diese Anforderungen aufgrund von Abhängigkeiten lange Durchlaufzeiten zur Folge haben, daher sollten sie schon in der ersten Planungsphase berücksichtigt werden.

In AWS sind die meisten dieser grundlegenden Anforderungen bereits berücksichtigt oder können nach Bedarf adressiert werden. Die Cloud ist grundsätzlich grenzenlos ausgelegt, es liegt also im Zuständigkeitsbereich von AWS, die Anforderungen an eine ausreichende Netzwerkleistung und Computing-Kapazität zu erfüllen, während Sie die Größe und die Zuweisung von Ressourcen, z. B. die Größe von Speichergeräten, bedarfsabhängig frei ändern können.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule). (Eine Liste mit Fragen und bewährten Methoden zu (untere Säule) finden Sie im Anhang.).

| **REL 1: Wie verwalte ich Service Limits?** |
| --- |
| Standardmäßig vorhandene Service Limits verhindern, dass Sie versehentlich mehr Ressourcen bereitstellen, als Sie benötigen. Auch die Anzahl der Aufrufe von API-Vorgängen ist begrenzt, um Services vor Missbrauch zu schützen. Wenn Sie AWS Direct Connect verwenden, ist der Umfang der über jede Verbindung übertragbaren Datenmenge begrenzt. Bei Nutzung von AWS Marketplace-Anwendungen ist wichtig, deren Einschränkungen zu kennen. Auch bei Webservices oder Software-as-a-Service von Drittanbietern ist wichtig, dass Sie deren Limits kennen. |
| **REL 2: Wie verwalte ich meine Netzwerktopologie?** |
| Anwendungen können in einer oder mehreren Umgebungen vorhanden sein: in Ihrer bestehenden Rechenzentrumsinfrastruktur sowie in öffentlichen Cloud-Infrastrukturen, die wahlweise öffentlich oder privat zugänglich sind. Wichtig für die Ressourcennutzung in der Cloud sind Netzwerküberlegungen wie die Konnektivität innerhalb und zwischen Systemen, die Verwaltung öffentlicher und privater IP-Adressen, sowie die Namensauflösung. |

AWS legt die Service Limits fest (also einen Höchstwert in Bezug auf die Anzahl der jeweiligen Ressourcen, die Ihr Team anfordern kann), um Sie vor einer versehentlichen Überbereitstellung von Ressourcen zu bewahren. Sie müssen Governance und Prozesse definieren, um diese Limits zu überwachen und zu ändern, um damit Ihre Geschäftsanforderungen zu erfüllen. Bei der Einführung der Cloud müssen Sie ggf. die Integration mit vorhandenen lokalen Ressourcen planen (bezeichnet als Hybrid-Ansatz). Mit einem Hybrid-Modell können Sie den allmählichen Übergang zu einem vollständigen Cloud-Ansatz durchführen. Daher ist es wichtig, ein Konzept zu entwickeln, wie Ihre AWS- und lokalen Ressourcen als Netzwerktopologie interagieren sollen.

## *Änderungsmanagement*

Mit dem Wissen, wie sich Änderungen auf ein System auswirken, können Sie proaktiv planen. Mit der Überwachung können Sie im Handumdrehen Trends identifizieren, die Kapazitätsprobleme oder SLA-Verstöße zur Folge haben könnten. In herkömmlichen Umgebungen erfolgen Prozesse zur Änderungskontrolle häufig manuell und müssen unter Aufsicht sorgfältig koordiniert werden, um wirksam kontrollieren und steuern zu können, wer wann welche Änderungen vornimmt.

Mit AWS können Sie das Verhalten eines Systems überwachen und die Reaktion auf KPIs automatisieren, z. B. durch das Hinzufügen zusätzlicher Server, wenn ein System Benutzer hinzugewinnt. Sie können kontrollieren und steuern, welche Benutzer berechtigt sind, Änderungen am System vorzunehmen, und die Historie dieser Änderungen überwachen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

| |
|---|
| **REL 3: Wie gut ist Ihr System bei Bedarfsänderungen anpassbar?** |
| Ein skalierbares System bietet die Elastizität, Ressourcen automatisch entsprechend dem aktuellen Bedarf hinzuzufügen oder zu entfernen. |
| **REL 4: So überwachen Sie Ihre Ressourcen** |
| Protokolle und Kennzahlen sind wertvolle Tools, um einen Einblick in den Zustand Ihrer Workloads zu gewinnen. Sie können Ihren Workload so konfigurieren, dass Protokolle und Kennzahlen überwacht und bei Über- oder Unterschreiten von Schwellenwerten oder signifikanten Ereignissen Benachrichtigungen gesendet werden. Im Idealfall sollte sich der Workload bei einem Fehler oder einem unterschrittenen Leistungsschwellenwert automatisch selbst reparieren oder entsprechend skalieren. |
| **REL 5: So implementieren Sie Änderungen** |
| Unkontrollierte Änderungen in Ihrer Umgebung machen es schwierig, die Auswirkung einer Änderung vorherzusagen. Kontrollierte Änderungen an bereitgestellten Ressourcen und Workloads sind erforderlich, um sicherzustellen, dass die Workloads und die Betriebsumgebung bekannte Software ausführen und auf vorhersagbare Weise durch Patches aktualisiert oder ersetzt werden können. |

Wenn Sie die Architektur eines Systems so aufbauen, dass es Ressourcen als Reaktion auf Bedarfsänderungen automatisch hinzufügt und entfernt, führt dies nicht nur zu einer Erhöhung der Zuverlässigkeit, sondern dieser Ansatz stellt darüber hinaus sicher, dass sich das Erreichen von geschäftlichem Erfolg nicht zu einer Belastung entwickelt. Wenn Überwachung implementiert ist, wird Ihr Team automatisch benachrichtigt, wenn KPIs von erwarteten Normen abweichen. Mit dem automatischen Protokollieren von Änderungen an Ihrer Umgebung können Sie auf Aktionen prüfen, die sich möglicherweise auf die Zuverlässigkeit ausgewirkt haben, und diese schnell identifizieren. Mit der Kontrolle und Steuerung des Änderungsmanagements können Sie sicherstellen, dass Sie die Regeln durchsetzen, die die geforderte Zuverlässigkeit bereitstellen.

## *Fehlerverwaltung*

In jedem System mit großer Komplexität ist es wahrscheinlich, dass Fehler auftreten. In der Regel ist es interessant, diese Fehler zu kennen, auf sie zu reagieren und dafür zu sorgen, dass sie nicht erneut auftreten.

Mit AWS können Sie mit Automatisierung auf die Überwachung von Daten reagieren. Wenn eine bestimmte Kennzahl beispielsweise einen Schwellenwert überschreitet, können Sie eine automatische Maßnahme zur Behebung dieses Problems auslösen. Statt also zu versuchen, eine fehlerhafte Ressource, die Teil Ihrer Produktionsumgebung ist, zu diagnostizieren und zu reparieren, können Sie sie durch eine neue Ressource ersetzen und die Analyse der fehlerhaften Ressource extern vornehmen. Da Sie in der Cloud temporäre Versionen eines gesamten Systems zu geringen Kosten auf-

stellen können, können Sie automatisiertes Testen verwenden, um vollständige Wiederherstellungsprozesse zu überprüfen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

| |
|---|
| **REL 6: So sichern Sie Ihre Daten** |
| Sichern Sie Daten, Anwendungen und Betriebsumgebungen (Betriebssysteme samt der darin ausgeführten Anwendungen), um Anforderungen hinsichtlich der mittleren Reparaturdauer (Mean Time to Repair, MTTR) sowie des Wiederherstellungszeitpunkts (Recovery Point Objective, RPO) zu erfüllen. |
| **REL 7: Wie stellen Sie die Systemverfügbarkeit bei Komponentenfehlern sicher?** |
| Wenn Ihre Workloads implizit oder explizit eine hohe Verfügbarkeit sowie eine kurze mittlere Reparaturzeit (Mean Time to Recovery, MTTR) erfordern, ist es wichtig, dass sie ausfallsicher sind und verteilt ausgeführt werden. |
| **REL 8: So testen Sie die Ausfallsicherheit** |
| Ermitteln Sie anhand von Tests der Ausfallsicherheit Ihres Workloads latente Bugs, die erst während der Produktion auftreten. Führen Sie diese Tests regelmäßig durch. |
| **REL 9: So planen Sie die Notfallwiederherstellung** |
| Die Notfallwiederherstellung ist wichtig, um gesicherte Daten bei Bedarf wiederherzustellen. Ihre Definition der Ziele, Ressourcen, Standorte und Funktionen der Daten sowie deren Ausführung müssen den Vorgaben für die Wiederherstellungsdauer (RTO) und den Wiederherstellungszeitpunkt (RPO) entsprechen. |

Sichern Sie Ihre Daten regelmäßig, und testen Sie Ihre Sicherungsdateien, um sicherzustellen, dass Sie Wiederherstellungen nach logischen und physischen Fehlern durchführen können. Ein Schlüssel zur Verwaltung von Fehlern ist das regelmäßige und automatisierte Testen von Systemen, die Fehler verursachen, und das anschließende Beobachten des Wiederherstellungsverhaltens. Führen Sie diese Schritte regelmäßig aus, und stellen Sie sicher, dass solche Tests auch nach signifikanten Systemänderungen durchgeführt werden. Verfolgen Sie KPIs aktiv, wie z. B. das zeitliche Ziel für die Wiederherstellung (RTO) und das Ziel für den Wiederherstellungspunkt (RPO), um die Ausfallsicherheit eines Systems (insbesondere unter Fehlertestszenarios) zu bewerten. Die Verfolgung von KPIs unterstützt Sie bei der Identifizierung und Milderung einzelner Fehlerpunkte. Dieser Ansatz zielt darauf ab, Ihre Systemwiederherstellungsprozesse gründlich zu testen, sodass Sie darauf vertrauen können, dass Sie all Ihre Daten wiederherstellen und Ihre Kunden unterbrechungsfrei bedienen können, und war selbst dann, wenn persistente Probleme auftreten. Sie sollten sich mit Ihren Wiederherstellungsprozessen genauso vertraut machen wie mit Ihren normalen Produktionsprozessen.

# Wichtige AWS-Services

Das für (Säule) maßgebliche (Angebot) ist (Service-Name), (Service-Beschreibung) Die folgenden Services und Funktionen unterstützen die (Anzahl) Bereiche in (untere Säule):

- **Grundlagen**: Mit AWS IAM können Sie den Zugriff auf AWS-Services und -Ressourcen sicher steuern. Mit Amazon VPC können Sie einen privaten, isolierten Abschnitt der AWS Cloud bereitstellen, in dem Sie AWS-Ressourcen in einem virtuellen Netzwerk starten können. AWS Trusted Advisor bietet Einblicke in die Service Limits. AWS Shield ist ein verwalteter Distributed Denial of Service (DDoS)-Schutz-Service, der Web-Anwendungen schützt, die auf AWS ausgeführt werden.
- **Änderungsmanagement**: AWS CloudTrail zeichnet Aufrufe von AWS-APIs für Ihr Konto auf und stellt Ihnen Protokolldateien bereit. AWS Config bietet eine detaillierte Bestandsauflistung Ihrer AWS-Ressourcen und der Konfiguration und erfasst laufend Änderungen an der Konfiguration. Amazon Auto Scaling ist ein Service für eine automatisierte Bedarfsverwaltung für einen bereitgestellten Workload. Amazon CloudWatch bietet die Möglichkeit, Warnungen zu Kennzahlen zu verwenden, darunter auch zu benutzerdefinierten Kennzahlen. Amazon CloudWatch ist außerdem mit einer Funktion ausgestattet, die Sie zum Aggregieren von Protokolldateien aus Ihren Ressourcen verwenden können.
- **Fehlerverwaltung**: AWS CloudFormation enthält Vorlagen für die Erstellung von AWS-Ressourcen und die Bereitstellung dieser auf geordnete und vorhersagbare Weise. Amazon S3 bietet einen Service mit hoher Beständigkeit für die Aufbewahrung Ihrer Sicherungen. Amazon Glacier bietet Archive mit hoher Beständigkeit. AWS KMS bietet ein zuverlässiges Schlüsselverwaltungssystem, das mit vielen AWS-Services integriert werden kann.

# Ressourcen

Werfen Sie einen Blick auf die folgenden Ressourcen, um mehr über unsere bewährten Methoden für (Säule) zu erfahren.

**Dokumentation**

- Service Limits
- Service Limits Reports Blog
- Amazon Virtual Private Cloud
- AWS Shield
- Amazon CloudWatch
- Amazon S3
- AWS KMS

**Whitepaper**

- Reliability Pillar

- Backup Archive and Restore Approach Using AWS
- Managing your AWS Infrastructure at Scale
- AWS Disaster Recovery
- AWS Amazon VPC Connectivity Options

**Video**

- How do I manage my AWS service limits?
- Embracing Failure: Fault-Injection and Service Reliability

**Produkt**

- AWS Premium Support
- Trusted Advisor

# Leistungseffizienz

Die (Säule) Säule beinhaltet (Beschreibung)

Die Säule für Leistungseffizienz bietet einen Überblick über konzeptionelle Grundsätze, bewährte Methoden und Fragen. Verbindliche Leitlinien zur Implementierung finden Sie im Whitepaper zur Säule der Leistungseffizienz.

## Konzeptionelle Grundsätze

Es gibt in der Cloud (Anzahl) konzeptionelle Grundsätze für (untere Säule):

- **Demokratisierung fortschrittlicher Technologien**: Die Nutzung schwierig zu implementierender Technologien lässt sich vereinfachen, indem Sie die komplexe Verwaltung an den Cloud-Anbieter übertragen. Anstatt Ihre IT-Mitarbeiter hinsichtlich des Hostings und der Ausführung neuer Technologien zu schulen, können diese die Technologien einfach als Service nutzen. Es gibt Technologien, wie etwa die NoSQL-Datenbanken, das Transcodieren von Medien sowie Machine Learning, die spezielles Fachwissen erfordern, das nicht zum allgemeinen Grundwissen der IT-Community zählt. In der Cloud kann Ihr Team diese Technologien als Service nutzen und sich auf die Produktentwicklung fokussieren, ohne sich Gedanken um die Bereitstellung und Verwaltung von Ressourcen kümmern zu müssen.
- **Globale Verteilung in wenigen Minuten**: Nehmen Sie Ihr System mit nur wenigen Mausklicks weltweit in verschiedenen Regionen in Betrieb. Dies ermöglicht es Ihnen, mit minimalem Kostenaufwand das Kundenerlebnis zu verbessern und die Latenz zu reduzieren.

- **Nutzung von Serverless Architekturen**: Aufgrund der in der Cloud verwendeten Serverless Architekturen brauchen Sie zur Durchführung herkömmlicher Rechenaktivitäten keine Server mehr auszuführen und zu verwalten. Speicherservices können beispielsweise als statische Websites genutzt werden, wodurch sich Webserver erübrigen. Ihren Code können Sie von Ereignisservices hosten lassen. Auf diese Weise entfällt nicht nur die Verwaltung dieser Server, sondern auch die Transaktionskosten sinken, da die verwalteten Services in der Cloud-Umgebung ausgeführt werden.
- **Vermehrtes Experimentieren**: Mit virtuellen und automatisierbaren Ressourcen können Sie schnell unterschiedliche Konfigurationen, Instance- oder Speichertypen miteinander vergleichen.
- **Mechanische Präferenz**: Nutzen Sie den für Ihre Anforderungen optimalen Technologieansatz. Berücksichtigen Sie bei der Auswahl des passenden Datenbank- oder Speicherkonzepts beispielsweise Ihre Datenzugriffsmuster.

# Definition

Es gibt in der Cloud (Anzahl) Bereiche, in denen bewährte Methoden für (untere Säule) zur Anwendung kommen:

- **Auswahl**
- **Prüfung**
- **Überwachung**
- **Kompromisse**

Um eine leistungsstarke Architektur sicherzustellen, empfiehlt sich für deren Entwicklung ein datenbasierter Ansatz. Sammeln Sie zu allen Aspekten der Architektur Daten, angefangen vom allgemeinen Design bis hin zur Auswahl und Konfiguration der Ressourcentypen. Indem Sie Ihre Auswahl regelmäßig prüfen, stellen Sie die bestmögliche Nutzung der sich fortlaufend weiterentwickelnde AWS Cloud sicher. Durch eine kontinuierliche Überwachung erkennen Sie Abweichungen von der erwarteten Leistung zeitnah und können entsprechende Maßnahmen ergreifen. Schließlich können Sie zur Leistungssteigerung der Architektur Kompromisse eingehen, beispielsweise durch Komprimierung oder Caching oder indem Sie hinsichtlich der Konsistenz mehr Toleranz einräumen.

# Bewährte Methoden

## *Auswahl*

Welche Lösung für das jeweilige System optimal ist, hängt von der Art des Workloads ab. Dabei empfiehlt sich häufig, mehrere Ansätze zu kombinieren. Architektonisch

gute Systeme umfassen mehrere Lösungen und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung.

In AWS werden Ressourcen visualisiert und auf unterschiedliche Weise in unterschiedlichen Konfigurationen bereitgestellt. Dies macht es einfach, den für Ihre Anforderungen passenden Ansatz zu ermitteln. Zudem profitieren Sie mitunter von Optionen, die sich in einer lokalen Infrastruktur nicht ohne Weiteres umsetzen ließen. Nehmen wir beispielsweise den verwalteten Service Amazon DynamoDB. Dieser bietet eine vollständig verwaltete NoSQL-Datenbank mit einer Latenz im einstelligen Millisekundenbereich ungeachtet des Volumens.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule). (Eine Liste mit Fragen und bewährten Methoden zu (untere Säule) finden Sie im Anhang.).

**PERF 1: Was ist bei der Wahl einer leistungsfähigen Architektur zu beachten?**

Oft sind mehrere Ansätze erforderlich, um eine optimale Leistung für einen Workload zu erzielen. Architektonisch gute Systeme umfassen mehrere Lösungen und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung.

Nutzen Sie bei der Auswahl der Muster und der Implementierung Ihrer Architektur einen datenbasierten Ansatz, um die optimale Lösung zu ermitteln. AWS Solutions Architects, AWS Reference Architectures und AWS Partner Network-Partner (APN) können Sie aufgrund unserer umfassenden Erfahrungen bei der Auswahl der Architektur unterstützen. Für ihre Optimierung sind jedoch anhand von Benchmarking oder Belastungstests erfasste Daten erforderlich.

Ihre Architektur wird vermutlich auf einer Reihe unterschiedlicher Ansätze basieren (z. B. ereignisgesteuert, ETL oder Pipeline). Implementiert wird sie mit den AWS-Services, die zur Optimierung ihrer Leistung beitragen. In den folgenden Abschnitten erörtern wir die vier Hauptressourcen, die Sie berücksichtigen sollten: Datenverarbeitung, Speicher, Datenbank und Netzwerk.

## Datenverarbeitung

Die optimale Rechenlösung für ein spezielles System kann vom Anwendungsdesign sowie von Nutzungsmustern und Konfigurationseinstellungen abhängig sein. Architekturen können unterschiedliche Rechenlösungen für verschiedene Komponenten verwenden und unterschiedliche Funktionen zur Leistungsverbesserung unterstützen. Das Auswählen der falschen Rechenlösung für eine Architektur kann die Leistungseffizienz schmälern.

In AWS gibt es drei Arten der Datenverarbeitung: Instances, Container und Funktionen:

- **Instances** Hierbei handelt es sich um virtualisierte Server, deren Funktionen Sie per Mausklick oder mit einem API-Befehl ändern können. Da sich in der Cloud Ressour-

cenentscheidungen jederzeit ändern lassen, können Sie mit verschiedenen Servertypen experimentieren. AWS bietet diese virtuellen Server-Instances in unterschiedlichen Varianten und Größen mit einer umfassenden Auswahl an Optionen, einschließlich Solid-State-Laufwerken (SSDs) und Grafikprozessoren (GPUs).

- **Container** Sie dienen zur Virtualisierung des Betriebssystems. Sie können damit eine Anwendung und deren Abhängigkeiten in von der Ressource isolierten Prozessen ausführen.
- **Funktionen** Damit wird die Ausführungsumgebung vom auszuführenden Code abstrahiert. Mit AWS Lambda können Sie beispielsweise Code ohne eine Instance ausführen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**PERF 2: Was ist bei der Wahl der Computing-Lösung zu beachten?**

Die optimale Computing-Lösung für ein System ist vom Anwendungsdesign sowie von Nutzungsmustern und Konfigurationseinstellungen abhängig. Architekturen verwenden mitunter unterschiedliche Computing-Lösungen für verschiedene Komponenten und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung. Die Wahl der falschen Computing-Lösung für eine Architektur kann die Leistungseffizienz schmälern.

Machen Sie sich bei der Datenverarbeitung die verfügbaren Elastizitätsmechanismen zunutze, um eine ausreichende Kapazität sicherzustellen und die Leistung bei sich ändernden Anforderungen aufrechtzuerhalten.

## Speicher

Die optimale Speicherlösung für ein spezielles System richtet sich nach der Zugriffsmethode (Block, Datei oder Objekt), den Zugriffsmustern (Zufallsprinzip oder sequenziell), dem erforderlichen Durchsatz, der Zugriffshäufigkeit (online, offline, Archiv), der Aktualisierungshäufigkeit (WORM, dynamisch) sowie den Einschränkungen hinsichtlich der Verfügbarkeit und Langlebigkeit. Architektonisch gute Systeme umfassen mehrere Speicherlösungen und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung.

Der Speicher in AWS ist virtualisiert. Sie können aus unterschiedlichen Speichertypen wählen. Dies erleichtert die Auswahl der passenden Speichermethoden. Außerdem profitieren Sie von Speicheroptionen, die sich in der lokalen Infrastruktur nicht ohne Weiteres umsetzen ließen. Amazon S3 ist beispielsweise für eine Langlebigkeit mit 11 Neunen (99,999999999 %) konzipiert. Darüber hinaus können Sie von magnetischen Festplattenlaufwerken (HDDs) zu Solid-State-Laufwerken (SSDs) wechseln. Virtuelle Laufwerke lassen sich innerhalb von Sekunden zwischen Instances verschieben.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**PERF 3: Was ist bei der Wahl der Speicherlösung zu beachten?**

Die optimale Speicherlösung für ein System richtet sich nach der Zugriffsmethode (Block, Datei oder Objekt), den Zugriffsmustern (Zufallsprinzip oder sequenziell), dem erforderlichen Durchsatz, der Zugriffshäufigkeit (online, offline, Archiv), der Aktualisierungshäufigkeit (WORM, dynamisch) sowie den Einschränkungen hinsichtlich Verfügbarkeit und Langlebigkeit. Architektonisch gute Systeme nutzen mehrere Speicherlösungen und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung und effizienten Ressourcennutzung.

Bei der Auswahl einer Speicherlösung ist wichtig, dass diese Ihren Zugriffsmustern entspricht, um die gewünschte Leistung zu erzielen.

## Datenbank

Welche Datenbanklösung sich am besten für ein spezielles System eignet, hängt von der erforderlichen Verfügbarkeit, Konsistenz, Partitionstoleranz, Latenz, Langlebigkeit, Skalierbarkeit und Abfragefähigkeit ab. Viele Systeme nutzen für verschiedene Untersysteme unterschiedliche Datenbanklösungen und unterstützen unterschiedliche Funktionen zur Leistungsoptimierung. Die Auswahl der falschen Datenbanklösung und -funktionen kann die Leistungseffizienz eines Systems schmälern.

Amazon RDS bietet eine vollständig verwaltete relationale Datenbank. Sie können damit die Rechen- und Speicherressourcen Ihrer Datenbank mitunter ohne Ausfallzeiten skalieren. Amazon DynamoDB ist eine vollständig verwaltete NoSQL-Datenbank, deren Latenz ungeachtet des Volumens im einstelligen Millisekundenbereich liegt. Amazon Redshift ist ein verwaltetes Data Warehouse im Petabyte-Bereich. Damit können Sie die Anzahl oder den Typ der Knoten dynamisch an Ihren jeweiligen Leistungs- oder Kapazitätsbedarf anpassen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**PERF 4: Was ist bei der Wahl der Datenbanklösung zu beachten?**

Welche Datenbanklösung sich am besten für ein System eignet, hängt von der erforderlichen Verfügbarkeit, Konsistenz, Partitionstoleranz, Latenz, Langlebigkeit, Skalierbarkeit und Abfragefähigkeit ab. Viele Systeme nutzen für verschiedene Untersysteme unterschiedliche Datenbanklösungen und bieten verschiedene Möglichkeiten zur Leistungsoptimierung. Die Wahl der falschen Datenbanklösung und -funktionen kann die Leistungseffizienz eines Systems schmälern.

Obwohl sich das für einen Workload verwendete Datenbankkonzept (RDBMS, NoSQL) erheblich auf die Leistungseffizienz auswirkt, werden bei der Auswahl oft nicht die erforderlichen Unternehmensdaten berücksichtigt. Ebenso wie beim Speicher sollten

auch hier unbedingt die Zugriffsmuster des Workloads berücksichtigt werden. Auch gilt zu prüfen, ob andere nicht datenbankgestützte Lösungen möglicherweise effizienter wären (z. B. eine Suchmaschine oder ein Data Warehouse).

### Netzwerk

Welche Netzwerklösung für ein spezielles System optimal ist, hängt von der Latenz, dem erforderlichen Durchsatz usw. ab. Physische Einschränkungen wie Benutzer- oder Hardwareressourcen können durch Edge-Techniken oder Ressourcenplatzierungen behoben werden.

In AWS wird das Netzwerk visualisiert und auf unterschiedliche Weise in unterschiedlichen Konfigurationen bereitgestellt. Dies ermöglicht es Ihnen, Ihre Netzwerkmethoden besser an Ihre Anforderungen anzupassen. AWS bietet zur Optimierung des Netzwerkdatenverkehrs Produktfunktionen wie Enhanced Networking, für Amazon EBS optimierte Instances, Amazon S3 Transfer Acceleration sowie den dynamischen Amazon CloudFront-Service. Zur Verbesserung der Latenz und der Stabilität des Netzwerks finden Sie in AWS Netzwerkfunktionen wie die latenzbasierte Weiterleitung mit Amazon Route 53, Amazon VPC-Endpunkte sowie AWS Direct Connect.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**PERF 5: Was ist beim Konfigurieren der Netzwerklösung zu beachten?**

Welche Netzwerklösung für ein System optimal ist, richtet sich unter anderem nach der Latenz und dem erforderlichen Durchsatz. Physische Einschränkungen wie Benutzer- oder Hardwareressourcen können durch Edge-Techniken oder Ressourcenplatzierungen behoben werden.

Bei der Auswahl der Netzwerklösung sollte unbedingt der Standort berücksichtigt werden. AWS bietet Ihnen zur Reduzierung der Latenz die Möglichkeit, Ressourcen in der Nähe ihres Verwendungsorts zu platzieren. Mit den entsprechenden Regionen, Platzierungsgruppen und Edge-Standorte können Sie die Leistung erheblich steigern.

## *Prüfung*

Die Auswahlmöglichkeiten bei den Architekturlösungen sind begrenzt. Im Lauf der Zeit werden jedoch immer wieder neue Technologien und Ansätze zur Leistungsoptimierung der Architektur entwickelt.

Mit AWS profitieren Sie von unseren fortlaufenden Innovationen, die wir aufgrund von Kundenanforderungen erstellen. Wir stellen regelmäßig neue Regionen, Edge-Standorte, Services und Funktionen zur Verfügung. Diese können zur Steigerung der Leistungseffizienz Ihrer Architektur beitragen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**PERF 6: Wie profitiert Ihren Workload von neuen Releases?**

Bei der Architektur von Workloads sind die Wahlmöglichkeiten begrenzt. Im Laufe der Zeit werden jedoch immer wieder neue Technologien und Ansätze zur Leistungsoptimierung des Workloads entwickelt.

Wenn Sie die Leistungsengpässe Ihrer Architektur kennen, können Sie auf Veröffentlichungen achten, mit denen sich diese beheben lassen.

## *Überwachung*

Nachdem Sie die Architektur implementiert haben, sollten Sie unbedingt ihre Leistung überwachen, um Probleme zu beheben, bevor sich diese auf Ihre Kunden auswirken. Lassen Sie sich mithilfe von Überwachungskennzahlen benachrichtigen, wenn Schwellenwerte überschritten werden. Dabei können automatisierte Aktionen ausgelöst werden, um fehlerhafte Komponenten zu umgehen.

Amazon CloudWatch bietet entsprechende Überwachungs- und Benachrichtigungsfunktionen. Automatisieren Sie die Umgehung von Leistungsproblemen durch über Amazon Kinesis, Amazon Simple Queue Service (Amazon SQS) und AWS Lambda ausgelöste Aktionen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**PERF 7: Wie lassen sich Ressourcen überwachen, um sicherzustellen, dass sie die erwartete Leistung liefern?**

Die Systemleistung kann sich mit der Zeit verschlechtern. Überwachen Sie die Systemleistung, um eine solche Verschlechterung frühzeitig zu erkennen und ihr entgegenzuwirken, etwa indem Sie interne oder externe Faktoren wie das Betriebssystem oder die Anwendungslast korrigieren.

Eine effektive Überwachungslösung zeichnet sich dadurch aus, dass Sie möglichst wenige Falschmeldungen erhalten und nicht mit Daten überflutet werden. Automatisierte Trigger eliminieren Benutzerfehler und können die Fehlerbehebung beschleunigen. Planen Sie Experimentiertage ein, an denen Sie Ihre Benachrichtigungslösung mithilfe von Simulationen in der Produktionsumgebung testen, um sicherzustellen, dass Probleme richtig erkannt werden.

## *Kompromisse*

Bei der Entwicklung von Lösungen können Kompromisse helfen, den optimalen Ansatz zu wählen. Je nach Situation können Sie beispielsweise die Latenz reduzieren,

indem Sie bedingte Abstriche bei der Konsistenz, der Langlebigkeit und dem Speicherplatz machen.

AWS ermöglicht Ihnen, globale Veröffentlichungen innerhalb weniger Minuten vorzunehmen. Sie können damit Ressourcen weltweit an verschiedenen Standorten bereitstellen, um die Entfernung zu Endbenutzern und damit die Latenz zu reduzieren. Des Weiteren haben Sie die Möglichkeit, in Informationsspeichern wie etwa Datenbanksystemen Lesereplikate bereitzustellen, um die Last der primären Datenbank zu reduzieren. AWS bietet außerdem Caching-Lösungen wie Amazon ElastiCache mit einem In-Memory-Datenspeicher oder -Cache sowie Amazon CloudFront, um Kopien Ihrer statischen Inhalte näher bei Endbenutzern zwischenzuspeichern. Mit Amazon DynamoDB Accelerator (DAX) erhalten Sie eine Amazon DynamoDB vorgelagerte verteilte Read-Through/Write-Through-Caching-Ebene. Diese unterstützt dieselbe API, bietet bei Entitäten im Cache jedoch eine Latenz im Mikrosekundenbereich.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**PERF 8: Wie lässt sich Leistung durch Kompromisse verbessern?**

Durch aktives Einbeziehen von Kompromissen beim Gestalten von Lösungen lässt sich der optimale Ansatz einfacher bestimmen. Leistung lässt sich oft durch Zugeständnisse in anderen Bereichen verbessern, etwa bei Konsistenz, Beständigkeit, Zeit und Latenz.

Durch Kompromisse kann sich die Komplexität der Architektur erhöhen. Prüfen Sie in diesem Fall mithilfe von Lasttests, ob ein messbarer Nutzen entsteht.

# Wichtige AWS-Services

Das für (Säule) maßgebliche (Angebot) ist (Service-Name), (Service-Beschreibung) Die folgenden Services und Funktionen unterstützen die (Anzahl) Bereiche in (untere Säule):

- **Auswahl**
  - **Datenverarbeitung**: Auto Scaling ist wichtig, um sicherzustellen, dass Sie über ausreichend Instances verfügen, damit Sie den Bedarf dynamisch decken können.
  - **Speicher**: Amazon EBS bietet eine Vielzahl von Speicheroptionen, wie etwa SSDs und bereitgestellte I/O-Operationen pro Sekunde (Provisioned Input/Output Operations per Second, PIOPS). Damit können Sie Optimierungen für Ihren Anwendungsfall erzielen. Amazon S3 ermöglicht eine Serverless Inhaltsbereitstellung, während sich Dateien mit Amazon S3 Transfer Acceleration schnell, einfach und sicher über große Entfernungen übertragen lassen.
  - **Datenbank**: Amazon RDS bietet eine Vielzahl von Datenbankfunktionen wie PIOPS und Lesereplikate zur Optimierung Ihres Anwendungsfalls. Mit Amazon

DynamoDB profitieren Sie ungeachtet des Volumens von einer Latenz im Millisekundenbereich.

  - **Netzwerk**: Amazon Route 53 bietet eine latenzbasierte Weiterleitung. Mit Amazon VPC-Endpunkte und AWS Direct Connect können Sie die Latenz und Stabilität Ihres Netzwerks verbessern.

- **Prüfung**: Über den AWS-Blog und den Abschnitt "Neuigkeiten" auf der AWS-Website können Sie stets bezüglich neu eingeführter Funktionen und Services auf dem Laufenden bleiben.
- **Überwachung**: Amazon CloudWatch bietet Kennzahlen, Alarme und Benachrichtigungen, die Sie in Ihre bestehende Überwachungslösung integrieren und anschließend zusammen mit AWS Lambda nutzen können, um Aktionen auszulösen.
- **Kompromisse**: Mit den Services Amazon ElastiCache, Amazon CloudFront und AWS Snowball können Sie die Leistung steigern. Durch Lesereplikate lassen sich in Amazon RDS leseintensive Workloads skalieren.

## Ressourcen

Werfen Sie einen Blick auf die folgenden Ressourcen, um mehr über unsere bewährten Methoden für (Säule) zu erfahren.

**Dokumentation**

- Amazon S3 Performance Optimization
- Amazon EBS Volume Performance

**Whitepaper**

- Performance Efficiency Pillar

**Video**

- AWS re:Invent 2016: Scaling Up to Your First 10 Million Users (ARC201)
- AWS re:Invent 2017: Deep Dive on Amazon EC2 Instances

# Kostenoptimierung

Die (Säule) Säule beinhaltet (Beschreibung)

Die Säule für Kostenoptimierung bietet einen Überblick über konzeptionelle Grundsätze, bewährte Methoden und Fragen. Obligatorische Anleitungen zur Implementierung finden Sie im Whitepaper der Säule für Kostenoptimierung.

# Konzeptionelle Grundsätze

Es gibt in der Cloud (Anzahl) konzeptionelle Grundsätze für (untere Säule):

- **Verbrauchsmodell einführen**: Zahlen Sie nur für die benötigten Computing-Ressourcen, und erhöhen oder verringern Sie die Nutzung auf Basis Ihrer Geschäftsanforderungen und nicht durch aufwändige Prognosen. Entwicklungs- und Testumgebungen werden in einer normalen Arbeitswoche beispielsweise nur acht Stunden pro Tag benötigt. Sie können diese Ressourcen anhalten, wenn sie nicht verwendet werden und damit potenzielle Einsparungen von 75 % (40 Stunden vs. 168 Stunden) erzielen.
- **Gesamteffizienz messen**: Messen Sie die geschäftliche Leistung des Workloads und die mit der Bereitstellung verknüpften Kosten. Verwenden Sie diese Kennzahlen, um die Gewinne zu ermitteln, die Sie aus der Erhöhung der Leistung und der Reduzierung der Kosten erzielen.
- **Ausgaben für Rechenzentrumsabläufe stoppen**: AWS übernimmt Aufgaben wie das Aufstellen, Instandhalten und Betreiben von Servern, sodass Sie sich voll auf Ihre Kunden und Unternehmensprojekte statt auf die IT-Infrastruktur konzentrieren können.
- **Ausgaben analysieren und zuordnen**: Mit der Cloud ist es einfacher, die Nutzung und die Kosten von Systemen genau zu ermitteln und auf Basis dieser Daten eine transparente Zuordnung der IT-Kosten auf einzelne Workload-Eigentümer durchzuführen. Auf diese Weise erhalten Sie Unterstützung bei der Messung der Umsatzrendite (ROI), und Workload-Eigentümer erhalten die Möglichkeit, ihre Ressourcen zu optimieren und die Kosten zu reduzieren.
- **Verwaltete Services und Services auf Anwendungsebene zur Reduzierung der Gesamtbetriebskosten verwenden**: In der Cloud eliminieren verwaltete Services und Services auf Anwendungsebene die betrieblichen Hürden bei der Bereithaltung von Servern für Aufgaben wie das Senden von E-Mails oder das Verwalten von Datenbanken. Da verwaltete Services in der großen Cloud-Umgebung ausgeführt werden, profitieren Sie hier von geringeren Kosten pro Transaktion oder Service.

# Definition

Es gibt in der Cloud (Anzahl) Bereiche, in denen bewährte Methoden für (untere Säule) zur Anwendung kommen:

- **Ausgabenbewusstsein**
- **Kostengünstige Ressourcen**
- **Abstimmen von Angebot und Bedarf**

- **Schrittweises Optimieren**

Wie bei anderen Säulen müssen auch hier Kompromisse akzeptiert werden. So müssen Sie z. B. entscheiden, ob Sie die Markteinführungsgeschwindigkeit oder die Kosten priorisieren möchten. In manchen Fällen ist es sinnvoll, die Priorität auf Geschwindigkeit zu legen, z. B. verbunden mit einer raschen Markteinführung, der Bereitstellung neuer Funktionen oder einer simplen Fristerfüllung, statt im Vorfeld in Kostenoptimierung zu investieren. Konzeptionelle Entscheidungen werden gelegentlich durch Eile statt auf Basis empirischer Daten getroffen, und man ist immer der Versuchung ausgesetzt, einem potenziellen Szenario zu viel Bedeutung beizumessen, statt Zeit in die Bestimmung des kostengünstigsten Workloads für einen bestimmten Zeitraum zu investieren. Dies führt häufig zu überversorgten und mangelhaft optimierten Bereitstellungen, die über ihren gesamten Lebenszyklus hinweg statisch bleiben. In den folgenden Abschnitten stellen wir Techniken und eine strategische Anleitung für die anfängliche und laufende Kostenoptimierung Ihrer Bereitstellung bereit.

# Bewährte Methoden

## *Ausgabenbewusstsein*

Die erhöhte Flexibilität und Agilität der Cloud fördert Innovationen und rasche Entwicklungen und Bereitstellungen. Diese Merkmale eliminieren die manuellen Prozesse und den Zeitaufwand für die Bereitstellung einer lokalen Infrastruktur, einschließlich der Identifizierung von Hardware-Spezifikationen, dem Verhandeln von Preisen, der Verwaltung von Bestellungen, der Planung von Lieferungen und schließlich der Bereitstellung der Ressourcen. Die einfache Nutzung und die nahezu unbegrenzte On-Demand-Verfügbarkeit macht neue Wege erforderlich, über Ausgaben nachzudenken.

Viele Unternehmen bestehen aus einer Vielzahl von Systemen, die von unterschiedlichen Teams betrieben werden. Die Möglichkeit, die Ressourcenkosten der jeweiligen Organisation oder den jeweiligen Produkteigentümer zuzuordnen, fördert ein effizientes Nutzungsverhalten und hilft, Verschwendung von Ressourcen einzudämmen. Mit einer präzisen Kostenzuordnung wissen Sie, welche Produkte wirklich profitabel sind, und Sie können fundierte Entscheidungen in Bezug auf die Aufteilung des Budgets treffen.

In AWS können Sie Cost Explorer verwenden, um Ihre Ausgaben zu verfolgen und Einblicke dazu zu gewinnen, wo die Ausgaben anfallen. Mit AWS Budgets können Sie Benachrichtigungen versenden, wenn Ihre Nutzung oder Kosten Ihre Prognosen überschreiten. Sie können Ressourcen-Tagging verwenden, um Geschäfts- und Unternehmensinformationen auf Ihre Nutzung und Kosten anzuwenden. Damit erhalten Sie zusätzliche Einblicke in die Optimierung aus einer unternehmerischen Perspektive.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule). (Eine Liste mit Fragen und bewährten Methoden zu (untere Säule) finden Sie im Anhang.).

**COST 1: Wie können Sie die Nutzung steuern?**

Definieren Sie Richtlinien und Verfahren, um sicherzustellen, dass sich die Kosten auf dem Weg zur Erreichung Ihrer Ziele in einem angemessenen Rahmen bewegen. Durch den Einsatz eines Kontrollsystems können Sie Innovationen vorantreiben, ohne das Budget zu überschreiten.

**COST 2: Wie können Sie die Nutzung und Kosten überwachen?**

Definieren Sie Richtlinien und Verfahren, um Ihre Kosten überwachen und richtig zuordnen zu können. Dadurch können Sie die Kosteneffizienz des Workloads bewerten und verbessern.

**COST 3: Wie können Sie Ressourcen außer Betrieb nehmen?**

Implementieren Sie vom Beginn bis zum Abschluss eines Projekts eine Änderungskontrolle und Ressourcenverwaltung. Auf diese Weise können Sie ungenutzte Ressourcen herunterfahren oder beenden, um Verschwendungen zu minimieren.

Sie können die Tags für die Kostenzuordnung verwenden, um Ihre Nutzung und Kosten in AWS zu kategorisieren und zu verfolgen. Wenn Sie Tags auf Ihre AWS-Ressourcen anwenden (z. B. EC2-Instances oder S3 Buckets), generiert AWS einen Kosten- und Nutzungsbericht mit Ihrer Nutzung und Ihren Tags. Sie können Tags anwenden, die für Unternehmenskategorien stehen (z. B. Kostenstellen, Workload-Namen oder Eigentümer), um Ihre Kosten verschiedenen Services zuzuordnen.

Durch das Kombinieren von gekennzeichneten Ressourcen mit einer Entitätslebenszyklus-Verfolgung (Mitarbeiter, Projekte) können Sie verwaiste Ressourcen oder Projekte identifizieren, die für das Unternehmen keine Werte mehr generieren und außer Betrieb gesetzt werden sollten. Sie können Gebührenlimit-Warnungen einrichten, damit Sie bei prognostizierten Budgetüberschreitungen informiert werden; mit dem AWS Einfacher Monatsrechner können Sie Ihre Kosten für Datenübertragungen berechnen.

## *Kostengünstige Ressourcen*

Die Verwendung der entsprechenden Instances und Ressourcen für Ihren Workload ist für Kosteneinsparungen von entscheidender Bedeutung. Die Ausführung eines Berichtsprozesses kann auf kleineren Servern beispielsweise bis zu fünf Stunden dauern, auf einem doppelt so teuren großen Server jedoch lediglich eine Stunde. Auf beiden Servern erhalten Sie dasselbe Ergebnis, der kleinere Server generiert über den Ausführungszeitraum jedoch höhere Kosten.

Architektonisch gute Workloads verwenden die kostengünstigsten Ressourcen; dieses Verhalten kann eine signifikante und positive wirtschaftliche Auswirkung haben. Sie haben außerdem die Möglichkeit, verwaltete Services für die Kostenreduzierung zu

verwenden. So können Sie für die E-Mail-Zustellung beispielsweise einen Service nutzen, bei dem die Kosten nach der Anzahl der versendeten Nachrichten berechnet werden, statt Server für diese Aufgabe bereithalten zu müssen.

AWS bietet eine große Vielfalt an flexiblen und kostengünstigen Preisoptionen für den Kauf von EC2- und anderen Instances auf eine Art und Weise, die sich für Ihre Anforderungen optimal eignet. *Mit On-Demand-Instances* können Sie die genutzte Rechenkapazität auf Stundenbasis und ohne Mindestverpflichtungen bezahlen. *Mit Reserved Instances* können Sie Kapazitäten reservieren und von Einsparungen von bis zu 75 % im Vergleich zum On-Demand-Preis profitieren. Mit Spot-Instances können Sie nicht genutzte Amazon EC2-Kapazität nutzen und von Einsparungen von bis zu 90 % im Vergleich zum On-Demand-Preis profitieren. *Spot-Instances* eignen sich, wenn das System eine Flotte von Servern toleriert, bei der einzelne Server dynamisch aktiviert und deaktiviert werden können, wie z. B. bei zustandslosen Web-Servern, bei der Stapelverarbeitung oder bei der Nutzung von HPC und Big Data.

Auch mit der Auswahl geeigneter Services ist es möglich, Nutzung und Kosten zu reduzieren. So können Sie beispielsweise CloudFront nutzen, um das Datenübertragungsvolumen zu reduzieren, oder Sie können Kosten vollständig eliminieren, z. B. mit Amazon Aurora on RDS, mit dem Sie kostspielige Datenbanklizensierungskosten vermeiden können.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**COST 4: Wie können Sie die Kosten bei der Auswahl von Services einschätzen?**

Bei Amazon EC2, Amazon EBS und Amazon S3 handelt es sich um AWS-Services, die als einzelne Bausteine angeboten werden. Verwaltete Services, etwa Amazon RDS und Amazon DynamoDB, sind AWS-Services auf einer höheren Ebene oder Anwendungsebene. Wenn Sie sich für die richtigen Bausteine und verwalteten Services entscheiden, können Sie die Kosten dieses Workloads optimieren. Durch die Nutzung von verwalteten Services können Sie einen Großteil Ihres administrativen und betrieblichen Overheads reduzieren oder beseitigen und damit Kapazitäten für anwendungs- und geschäftsbezogene Aktivitäten gewinnen.

**COST 5: Wie können Sie bei der Auswahl des Ressourcentyps und -umfangs Kostenziele erfüllen?**

Stellen Sie sicher, dass Sie den richtigen Ressourcenumfang für die jeweilige Aufgabe wählen. Durch die Auswahl des kostengünstigsten Typs und Umfangs minimieren Sie Verschwendungen.

**COST 6: Wie können Sie Kosten mithilfe von Preismodellen senken?**

Verwenden Sie das Preismodell, das sich für Ihre Ressourcen am besten eignet. So halten Sie die Ausgaben möglichst niedrig.

**COST 7: Wie können Sie die Kosten für Datenübertragungen planen?**

Damit Sie architekturbezogene Entscheidungen zur Kostenminimierung treffen können, müssen Sie unbedingt die Datenübertragungskosten einplanen und überwachen. Eine geringfügige, aber effektive Änderung an der Architektur kann Ihre Betriebskosten über einen längeren Zeitraum hinweg erheblich senken.

Durch das Faktorisieren der Kosten während der Service-Auswahl und die Verwendung von Werkzeugen wie Cost Explorer und AWS Trusted Advisor für die regelmäßige Überprüfung Ihrer AWS-Nutzung können Sie Ihre Nutzung aktiv überwachen und Ihre Bereitstellungen entsprechend anpassen.

## *Abstimmen von Angebot und Bedarf*

Eine optimale Abstimmung von Angebot und Bedarf ermöglicht die geringstmöglichen Kosten für einen Workload, es muss jedoch auch ein ausreichendes Mehrangebot für die Bereitstellungszeit und für einzelne Ressourcenfehler vorhanden sein. Der Bedarf kann fest oder variabel sein und Kennzahlen und Automatisierung erfordern, um sicherzustellen, dass durch die Verwaltung keine signifikanten Kosten generiert werden.

In AWS können Sie Ressourcen automatisch bereitstellen, um den Bedarf zu erfüllen. Auf Basis von Auto Scaling- und Bedarfs-, Puffer- und zeitbasierten Ansätzen können Sie Ressourcen nach Bedarf hinzufügen und entfernen. Wenn Sie in der Lage sind, Bedarfsänderungen zu antizipieren, können Sie mehr Geld sparen und gleichzeitig sicherstellen, dass Ihre Ressourcen Ihren Workload-Anforderungen entsprechen.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**COST 8: Wie können Sie das Ressourcenangebot auf den Bedarf abstimmen?**

Stellen Sie bei einem Workload mit ausgewogenen Ausgaben und Leistungen sicher, dass alles, wofür Sie bezahlen, genutzt wird, und vermeiden Sie eine erhebliche Unterauslastung der Instances. Eine verschobene Auslastungsmetrik in einer der Richtungen wirkt sich nachteilig auf Ihr Unternehmen aus, entweder im Hinblick auf die Betriebskosten (verschlechterte Leistung aufgrund von Überbelegung) oder auf die verschwendeten AWS-Ausgaben (aufgrund von Überversorgung).

Bei der Konzeption der Abstimmung von Angebot und Bedarf sollten Sie aktiv über die Nutzungsmodelle und den Zeitbedarf nachdenken, die für die Bereitstellung neuer Ressourcen erforderlich sind.

## *Schrittweises Optimieren*

Im Zuge der Veröffentlichung neuer Services und Funktionen durch AWS empfiehlt es sich, dass Sie Ihre bestehenden Entscheidungen zur Architektur überprüfen, um sicherzustellen, dass diese weiterhin so kostengünstig wie möglich sind. Wenn sich Ihre Anforderungen ändern, setzen Sie Ressourcen, ganze Services und Systeme, die Sie nicht mehr benötigen, aktiv außer Betrieb.

Mit verwalteten Services von AWS können Sie den Workload nachhaltig optimieren, es ist also wichtig, dass Sie in Bezug auf die Verfügbarkeit neuer verwalteter Services und Funktionen auf dem Laufenden bleiben. Das Ausführen einer Amazon RDS-Datenbank kann beispielsweise günstiger sein als das Ausführen Ihrer eigenen Datenbank in Amazon EC2.

In den folgenden Fragen geht es um diese Überlegungen zu (untere Säule).

**COST 9: Wie können Sie neue Services bewerten?**

Im Zuge der Veröffentlichung neuer Services und Funktionen durch AWS empfiehlt es sich, dass Sie Ihre bestehenden Entscheidungen zur Architektur überdenken, um sicherzustellen, dass diese weiterhin so kostengünstig wie möglich sind.

Wenn Sie Ihre Bereitstellungen regelmäßig überprüfen, sollten Sie auch bewerten, wie Sie mit neueren Services möglicherweise Geld sparen können. Mit Amazon Aurora on RDS können Sie beispielsweise die Kosten für relationale Datenbanken reduzieren.

# Wichtige AWS-Services

Das für (Säule) maßgebliche (Angebot) ist (Service-Name), (Service-Beschreibung) Die folgenden Services und Funktionen unterstützen die (Anzahl) Bereiche in (untere Säule):

- **Ausgabenbewusstsein**: Mit AWS Cost Explorer können Sie Ihre Nutzung im Detail anzeigen und verfolgen. Sie werden von AWS Budgets benachrichtigt, wenn Ihre Nutzung oder die Ausgaben die tatsächlichen oder prognostizierten Budgetbeträge überschreiten.
- **Kostengünstige Ressourcen**: Sie können Cost Explorer für Reserved Instance-Empfehlungen verwenden, um Modelle zu finden, anhand derer Sie Ihre Ausgaben für AWS-Ressourcen im Laufe der Zeit ermitteln können. Mit Amazon CloudWatch und Trusted Advisor können Sie Ihre Ressourcen richtig dimensionieren. Mit Amazon Aurora on RDS können Sie Ihre Datenbanklizensierungskosten entfernen. Mit AWS Direct Connect und Amazon CloudFront können Sie die Datenübertragung optimieren.
- **Abstimmen von Angebot und Bedarf**: Mit Auto Scaling können Sie Ressourcen hinzufügen oder entfernen, um den Bedarf ohne Budgetüberschreitungen zu erfüllen.
- **Schrittweises Optimieren**: Der AWS-Blog mit Neuigkeiten und der Abschnitt "Neuigkeiten" auf der AWS-Website sind die Ressourcen, denen Sie neu eingeführte Funktionen und Services entnehmen können. AWS Trusted Advisor prüft Ihre AWS-Umgebung und identifiziert Möglichkeiten für Einsparungen, indem nicht genutzte oder im Leerlauf befindliche Ressourcen eliminiert werden oder Reserved Instance-Kapazität erhalten wird.

# Ressourcen

Werfen Sie einen Blick auf die folgenden Ressourcen, um mehr über unsere bewährten Methoden für (Säule) zu erfahren.

**Dokumentation**

- Analyzing Your Costs with Cost Explorer
- AWS Cloud Economics Center
- AWS Detailed Billing Reports

**Whitepaper**

- Cost Optimization Pillar

**Video**

- Cost Optimization on AWS

**Tool**

- AWS Total Cost of Ownership (TCO) Calculators
- AWS Simple Monthly Calculator

# Die Überprüfung

Architekturen müssen nach einheitlichen Gesichtspunkten überprüft werden. Wenn dabei niemand an den Pranger gestellt wird, ist eine Voraussetzung für tief schürfende Analysen gegeben. Der Prozess sollte nicht schwerfällig sein (Stunden, nicht Tage) und als Konversation angelegt sein, nicht als Audit. Architekturen werden überprüft, um festzustellen, ob kritische Mängel vorliegen, gegen die etwas unternommen werden muss – oder um festzustellen, ob bestimmte Bereiche nachgebessert werden können. Am Ende der Überprüfung stehen Maßnahmen, die dem Kunden, der mit dem Workload arbeitet, ein angenehmeres Erlebnis ermöglichen.

Wie bereits im Abschnitt "Architektur-Überlegungen" angesprochen, ist es in Ihrem Interesse, dass jedes Teammitglied Verantwortung für die Qualität der Architektur übernimmt. Wir empfehlen, dass die Teammitglieder, die die Architektur entwerfen, mit Hilfe des Well-Architected Framework ihre Architektur fortlaufend überprüfen, anstatt eine formelle Überprüfungsbesprechung anzusetzen. Findet die Überprüfung fortlaufend statt, können Ihre Teammitglieder parallel mit der Entwicklung der Architektur Antworten aktualisieren und mit jeder neuen Funktion die Architektur verbessern.

AWS Well-Architected ist ähnlich aufgebaut wie der interne AWS-Prozess zur Überprüfung von Systemen und Services. Der architektonische Ansatz wird beeinflusst von konzeptionellen Grundsätzen und Fragen, die sicherstellen, dass Bereiche nicht vernachlässigt werden, die häufig in der Ursachenanalyse auftauchen. Tritt an einem internen System, AWS-Service oder bei einem Kunden ein schwerwiegendes Problem auf, untersuchen wir die Ursachenanalyse auf Verbesserungsmöglichkeiten für unsere Überprüfungsprozesse.

Die Überprüfungen müssen an wichtigen Meilensteinen des Produktzyklus erfolgen – früh in der Entwurfsphase, um *einseitige Türen* [1] zu vermeiden, an denen schwer nachzubessern ist. Und zuletzt schließlich kurz vor dem Go-Live. Nach dem Go-Live verändert sich Ihr Workload weiter, da neue Funktionen hinzukommen und Sie Technologieimplementierungen anpassen. Die Architektur eines Workloads verändert sich mit der Zeit. Treffen Sie durchdachte Hygienemaßnahmen, um zu verhindern, dass die Qualität seiner architektonischen Merkmale im Zuge der Weiterentwicklung nachlässt. Wenn Sie an der Architektur signifikante Änderungen vornehmen, müssen Sie bestimmte Hygieneprozesse befolgen, z. B. eine Überprüfung nach dem Well-Architected-Prinzip.

Wenn die Überprüfung als einmalige Momentaufnahme oder unabhängige Messung vorgesehen ist, müssen alle wichtigen Beteiligten in die Konversation eingebunden

[1] Viele Entscheidungen sind umkehrbar (zweiseitig öffnende Türen). Für diese Entscheidungen reicht ein schlanker Prozess. Einseitige Türen sind nur schwerlich oder gar nicht umkehrbar und müssen vor dem Einsetzen genauer inspiziert werden.

sein. Häufig ist die Überprüfung der Punkt, an dem einem Team das erste Mal richtig klar wird, was es implementiert hat. Wird der Workload eines anderen Teams überprüft, ist es sinnvoll, mehrere informelle Konversationen über seine Architektur einzuplanen. In diesen Gesprächen erhalten Sie Antworten auf die meisten Fragen. Im Anschluss daran können Sie in ein oder zwei Besprechungen Punkte abklären und ausführlich auf Unklarheiten oder eventuelle Risiken eingehen.

Damit Ihre Besprechungen erfolgreich verlaufen, empfehlen wir folgende Ausstattung:

- Besprechungszimmer mit Whiteboards
- Diagramme und Entwurfsnotizen ausgedruckt auf Papier
- Liste der Fragen, die sich nicht mit herkömmlichen Mitteln beantworten lassen (z. B. „Werden die Daten verschlüsselt?“)

Nach der Überprüfung sollten Sie eine Liste mit Problemen vorliegen haben. Welche Sie priorisieren, hängt vom geschäftlichen Kontext ab. Berücksichtigen Sie auch, wie sich diese Probleme auf die tägliche Arbeit Ihres Teams auswirken. Wenn Sie die Probleme frühzeitig anpacken, gewinnen Sie vielleicht Zeit. Zeit, in der Sie geschäftlichen Mehrwert schaffen können, anstatt sich um wiederkehrende Probleme zu kümmern. Während Sie die Probleme aus der Welt schaffen, können Sie Ihre Überprüfung aktualisieren und so verfolgen, wie sich die Architektur verbessert.

Wie hilfreich eine Überprüfung war, zeigt sich erst danach. Neue Teams widersetzen sich möglicherweise zuerst. Sie können Einwänden der Teams entgegnen, indem Sie sie über die Vorteile einer Überprüfung aufklären:

- „Wir sind zu beschäftigt!“ (Häufig im Vorfeld großer Produktstarts zu hören.)
  - Wenn ihr euch auf einen großen Launch vorbereitet, sollte der möglichst glatt über die Bühne gehen. Die Überprüfung deckt Schwachstellen auf, die ihr vielleicht übersehen habt.
  - Wir empfehlen, dass ihr früh im Produktzyklus Überprüfungen einbaut, um Risiken aufzudecken und einen Auffangplan auszuarbeiten, der auf die Roadmap für die Feature-Bereitstellung abgestimmt ist.
- „Wir haben nicht die Zeit, um mit den Ergebnissen etwas anzufangen!“ (Oft zu hören, wenn ein unverrückbares Ereignis näher rückt (z. B. eine große Sportveranstaltung), auf das alles ausgerichtet ist.)
  - Diese Ereignisse lassen sich nicht verschieben. Wollt ihr da wirklich reingehen, ohne die Risiken eurer Architektur zu kennen? Selbst wenn ihr nicht alle Probleme wegbekommt, könnt ihr euch immer noch mit Playbooks helfen, wenn sie tatsächlich eintreten.

- „Wir möchten nicht, dass andere die Geheimnisse unserer Lösungsimplementierung kennenlernen!“
    - Wenn Sie die Aufmerksamkeit des Teams auf die Fragen im Well-Architected Framework richten, erkennen sie, dass keine der Fragen kommerziell oder technisch sensible Informationen herauszieht.

Wenn Sie mit Teams aus Ihrer Organisation mehrere Überprüfungen durchführen, identifizieren Sie möglicherweise thematische Fragen. So könnte sich beispielsweise herausstellen, dass mehrere Teams in einer bestimmten Säule oder einem bestimmten Themengebiet mehrere zusammenhängende Probleme haben. Werfen Sie einen ganzheitlichen Blick auf all Ihre Überprüfungen und identifizieren Sie Mechanismen, Trainings oder Principal-Engineer-Vorträge, mit deren Hilfe sich diese thematischen Fragen angehen lassen.

# Fazit

Das AWS Well-Architected Framework liefert über alle fünf Säulen hinweg bewährte architektonische Methoden für die Entwicklung und den Betrieb zuverlässiger, sicherer, effizienter und kosteneffektiver Systeme in der Cloud. Die Fragen aus dem Framework erlauben Ihnen, bestehende und geplante Architekturen zu überprüfen. Außerdem sind darin bewährte AWS-Methoden für die fünf Säulen enthalten. Als fester Bestandteil Ihres Architekturdesigns fördert das Framework stabile und effiziente Systeme. Anschließend können Sie sich auf Ihre funktionalen Anforderungen konzentrieren.

# Mitwirkende

Dieses Dokument ist unter der Mitarbeit folgender Personen und Organisationen entstanden:

- "Fitz" Philip Fitzsimons: Sr. Manager Well-Architected, Amazon Web Services
- Brian Carlson: Operations Lead Well-Architected, Amazon Web Services
- Ben Potter: Security Lead Well-Architected, Amazon Web Services
- Rodney Lester: Reliability Lead Well-Architected, Amazon Web Services
- John Ewart: Performance Lead Well-Architected, Amazon Web Services
- Nathan Besh: Cost Lead Well-Architected, Amazon Web Services
- Jon Steele: Sr. Technical Account Manager, Amazon Web Services
- Ryan King: Technical Program Manager, Amazon Web Services
- Erin Rifkin: Senior Product Manager, Amazon Web Services
- Max Ramsay: Principal Security Solutions Architect, Amazon Web Services
- Scott Paddock: Security Solutions Architect, Amazon Web Services
- Callum Hughes: Solutions Architect, Amazon Web Services

# Weitere Informationen

*AWS Well-Architected Partner program*

*AWS Well-Architected Tool*

*AWS Well-Architected homepage*

*Cost Optimization Pillar whitepaper*

*Operational Excellence Pillar whitepaper*

*Performance Efficiency Pillar whitepaper*

*Reliability Pillar whitepaper*

*Security Pillar whitepaper*

# Dokumentversionen

## Tabelle 2.

## Wichtige Überarbeitungen:

| Datum | Beschreibung |
|---|---|
| **Juli 2019** | Aufnahme von AWS Well-Architected Tool, Link zu AWS Well-Architected Labs, und AWS Well-Architected-Partner, kleinere Fehlerbehebungen, um mehrere Framework-Sprachversionen zu ermöglichen. |
| **November 2018** | Die meisten Fragen und Antworten wurden noch einmal durchgelesen und umgeschrieben, damit die Fragen jeweils nur ein Thema behandeln. Dabei wurden einige Fragen in mehrere Einzelfragen aufgeteilt. Häufig verwendete Begriffe (Workload, Komponente usw.) wurden definiert. Darstellung der Fragen im Textkorpus wurde bearbeitet, um Platz zu schaffen für Erläuterungen. |
| **Juni 2018** | Fragentext ist nach mehreren Updates einfacher formuliert, Antworten sind standardisiert, und die Lesbarkeit wurde verbessert. |
| **November 2017** | "Betriebliche Exzellenz" wurde vor die anderen Säulen gesetzt und umgeschrieben. Umfasst jetzt die anderen Säulen. Die anderen Säulen wurden aktualisiert, um der Weiterentwicklung von AWS Rechnung zu tragen. |
| **November 2016** | Aktualisierung des Framework. Dieses enthält jetzt die Säule "Betriebliche Exzellenz". Die anderen Säulen wurden überarbeitet und aktualisiert. Dabei wurden Doppelnennungen ausgeräumt und Erkenntnisse aus Überprüfungen bei mehreren Tausend Kunden aufgenommen. |
| **November 2015** | Aktualisierung des Anhangs mit neuen Informationen zu Amazon CloudWatch Logs. |
| **Oktober 2015** | Erstveröffentlichung. |

# Anhang: Fragen und bewährte Methoden

## Betriebliche Exzellenz

### OPS 1 Wie können Sie Ihre Prioritäten bestimmen?

Alle Beteiligten müssen verstehen, welchen Anteil sie am geschäftlichen Erfolg haben. Setzen Sie sich gemeinsame Ziele, damit Sie die Prioritäten für Ressourcen festlegen können. Dadurch erzielen Ihre Bemühungen den größtmöglichen Nutzen.

Bewährte Methoden:

- **Bewerten der Bedürfnisse externer Kunden**: Binden Sie alle wichtigen Beteiligten ein, einschließlich der Teams aus den Bereichen Betriebswirtschaft, Entwicklung und Operationen, um festzustellen, an welchen Stellen die Aufgaben im operativen Geschäft an den Bedürfnissen externer Kunden ausgerichtet werden müssen. Dadurch wird sichergestellt, dass Sie die Unterstützung der Operationen, die für die Erzielung der gewünschten geschäftlichen Ergebnisse erforderlich ist, genau kennen und verstehen.
- **Bewerten der Bedürfnisse interner Kunden**: Binden Sie alle wichtigen Beteiligten ein, einschließlich der Teams aus den Bereichen Betriebswirtschaft, Entwicklung und Operationen, wenn Sie ermitteln, an welchen Stellen die Aufgaben im operativen Geschäft an den Bedürfnissen interner Kunden ausgerichtet werden müssen. Dadurch wird sichergestellt, dass Sie die Unterstützung der Operationen, die für die Erzielung der gewünschten geschäftlichen Ergebnisse erforderlich ist, genau kennen und verstehen.
- **Bewerten der Compliance-Anforderungen**: Bewerten Sie externe Faktoren, wie z. B. gesetzliche Compliance-Anforderungen und Branchenstandards, um sicherzustellen, dass Sie sich der Richtlinien oder Verpflichtungen bewusst sind, die einen bestimmten Fokus erfordern oder verstärken können. Wenn keine Compliance-Anforderungen festgestellt werden, stellen Sie sicher, dass Sie bei dieser Ermittlung die erforderliche Sorgfalt walten lassen.
- **Bewerten der Bedrohungsszenarien**: Bewerten Sie Bedrohungen für das Unternehmen (z. B. Konkurrenz, Geschäftsrisiken und -verpflichtungen, operative Risiken und Bedrohungen der Informationssicherheit), damit Sie deren Auswirkungen bei der Entscheidung berücksichtigen können, worauf sich die operativen Anstrengungen konzentrieren sollen.
- **Bewerten von Kompromissen**: Bewerten Sie die Auswirkungen von Kompromissen bei konkurrierenden Interessen, um fundierte Entscheidungen zu treffen, wenn es darum geht, auf welche Bereiche die operativen Anstrengungen konzentriert werden sollen. So kann beispielsweise die Beschleunigung der Markteinführung neuer Features einen höheren Stellenwert haben als die Kostenoptimierung.
- **Abwägen von Vorteilen und Risiken**: Wägen Sie die Vorteile und Risiken ab, um fundierte Entscheidungen zu treffen, wenn es darum geht, auf welche Bereiche die operativen Anstrengungen konzentriert werden sollen. So kann es beispielsweise sinnvoll sein, ein System mit noch offenen Problemen bereitzustellen, um den Kunden wichtige neue Funktionen zur Verfügung zu stellen.

### OPS 2 Wie können Sie Ihren Workload so konzipieren, dass ihr jeweiliger Zustand klar ersichtlich ist?

Gestalten Sie Ihren Workload so, dass sie die Informationen liefert, die Sie benötigen, um ihren internen Zustand über alle Komponenten hinweg zu verstehen (z. B. mithilfe von Metriken, Protokollen und Traces). Auf diese Weise können Sie im Bedarfsfall effektiv reagieren.

Bewährte Methoden:

- **Implementieren einer Anwendungstelemetrie**: Nutzen Sie Ihren Anwendungscode, um Informationen über den jeweiligen internen Zustand, den Status und die Erreichung von Geschäftsergebnissen zu erhalten. Die Warteschlangenlänge, Fehlermeldungen und Reaktionszeiten können beispielsweise wichtige Indikatoren sein. Ermitteln Sie mithilfe dieser Informationen, wann ein Eingreifen erforderlich ist.
- **Implementieren und Konfigurieren der Workload-Telemetrie**: Entwickeln und konfigurieren Sie Ihren Workload so, dass Sie Informationen zu ihrem internen Zustand und zum aktuellen Status erhalten. Die Menge an API-Aufrufen, HTTP-Statuscodes und Skalierungsereignisse können beispielsweise Aufschluss über den Zustand geben. Ermitteln Sie mithilfe dieser Informationen, wann ein Eingreifen erforderlich ist.
- **Implementieren einer Telemetrie für Benutzeraktivität**: Nutzen Sie Ihren Anwendungscode, um Informationen über die Benutzeraktivität zu erhalten. Hier können zum Beispiel Click-Streams oder gestartete, abgebrochene und abgeschlossenen Transaktionen aufschlussreich sein. Verwenden Sie diese Informationen, um zu verstehen, wie die Anwendung verwendet wird oder welche Nutzungsmuster sie aufweist, und um festzustellen, wann ein Eingreifen erforderlich ist.
- **Implementieren einer Abhängigkeitstelemetrie**: Entwickeln und konfigurieren Sie Ihren Workload so, dass Sie Informationen zum Status der Ressourcen erhalten, auf die sie angewiesen ist. Beispiele hierfür sind externe Datenbanken, DNS und Netzwerkkonnektivität. Ermitteln Sie mithilfe dieser Informationen, wann ein Eingreifen erforderlich ist.
- **Implementieren einer Nachvollziehbarkeit von Transaktionen**: Implementieren Sie Ihren Anwendungscode und konfigurieren Sie Ihre Workload-Komponenten so, dass Sie Informationen über den Transaktionsfluss im gesamten Workload erhalten. Mithilfe dieser Informationen können Sie feststellen, wann ein Eingreifen erforderlich ist. Außerdem wird dadurch die Ermittlung der eigentlichen Fehlerursachen erleichtert.

### OPS 3 Wie können Sie Fehler reduzieren, die Fehlerbehebung erleichtern und den Ablauf bis zur Produktion verbessern?

Verwenden Sie Strategien, die die Übertragung von Änderungen auf die Produktionsumgebung verbessern und Refactoring, schnelles Feedback zur Qualität sowie eine schnelle Fehlerbehebung ermöglichen. Dadurch fließen nützliche Änderungen schneller in die Produktion ein und es treten bei der Bereitstellung weniger Probleme auf. Zudem können Probleme, die durch Bereitstellungsaktivitäten verursacht werden, schnell aufgespürt und gelöst werden.

Bewährte Methoden:

- **Einsatz einer Versionskontrolle**: Ermöglichen Sie die Verfolgung von Änderungen und Releases mithilfe einer Versionskontrolle.
- **Testen und Validieren von Änderungen**: Testen und validieren Sie Änderungen, um Fehler zu reduzieren und zu erkennen. Automatisieren Sie Tests, um Fehler aufgrund von manuellen Prozessen zu reduzieren und den Testaufwand zu verringern.
- **Einsatz von Systemen zur Konfigurationsverwaltung**: Verwenden Sie Systeme zur Konfigurationsverwaltung, um Änderungen vorzunehmen und zu verfolgen. Diese Systeme reduzieren Fehler aufgrund von manuellen Prozessen und verringern den Testaufwand.
- **Einsatz von Systemen zur Build- und Bereitstellungsverwaltung**: Verwenden Sie Systeme zur Build- und Bereitstellungsverwaltung. Diese Systeme reduzieren Fehler aufgrund von manuellen Prozessen und verringern den Testaufwand.
- **Patch-Verwaltung durchführen**: Führen Sie eine Patch-Verwaltung durch, um Funktionen zu erhalten, Probleme zu beheben und die Konformität mit der Governance zu gewährleisten. Automatisieren Sie die Patch-Verwaltung, um Fehler aufgrund von manuellen Prozessen zu reduzieren und den Aufwand für die Installation von Patches zu verringern.
- **Gemeinsame Design-Standards**: Tauschen Sie teamübergreifend Best Practices aus, um das Bewusstsein zu schärfen und den Nutzen der Entwicklungsarbeit zu maximieren.
- **Implementieren von Verfahren zur Verbesserung der Codequalität**: Implementieren Sie Verfahren zur Verbesserung der Codequalität und Minimierung von Fehlern. Geeignete Maßnahmen sind zum Beispiel testbasierte Entwicklungen, Codeprüfungen und die Einführung von Standards.
- **Verwenden mehrerer Umgebungen**: Verwenden Sie mehrere Umgebungen, in denen Sie Ihren Workload ausprobieren, entwickeln und testen. Durch die Verstärkung von Versionskontrollen können Sie sich darauf verlassen, dass Ihr Workload wie beabsichtigt funktioniert.
- **Vornehmen kleiner, häufiger und umkehrbarer Änderungen**: Häufige, kleine und umkehrbare Änderungen verringern den Umfang und die Auswirkung einer Änderung. Dies erleichtert die Fehlersuche, ermöglicht eine schnellere Fehlerbehebung und bietet die Möglichkeit, eine Änderung zurückzusetzen.
- **Vollständige Automatisierung von Integration und Bereitstellung**: Automatisieren Sie den Aufbau, die Bereitstellung und die Tests des Workloads. Dadurch werden Fehler aufgrund von manuellen Prozessen reduziert und der Aufwand für die Bereitstellung von Änderungen verringert.

## OPS 4 Wie können Sie Bereitstellungsrisiken eindämmen?

Verwenden Sie Ansätze, die ein schnelles Feedback zur Qualität liefern und eine umgehende Wiederherstellung des vorherigen Zustands nach Änderungen ermöglichen, die nicht zu den gewünschten Ergebnissen führen. Mit diesen Verfahren können Sie die Auswirkung von Problemen eindämmen, die durch die Bereitstellung von Änderungen entstehen.

Bewährte Methoden:

- **Einkalkulieren nicht erfolgreicher Änderungen**: Planen Sie Maßnahmen für die Rückkehr zu einem bekanntermaßen funktionierenden Zustand oder die Korrektur in der Produktionsumgebung ein, falls eine Änderung nicht das gewünschte Ergebnis bewirkt. Dank dieser Vorbereitung verkürzt sich die Wiederherstellungszeit, da schneller reagiert werden kann.
- **Testen und Validieren von Änderungen**: Testen Sie Änderungen und validieren Sie die Ergebnisse in allen Phasen des Lebenszyklus. Auf diese Weise können Sie neue Funktionen prüfen und das Risiko und die Auswirkungen fehlgeschlagener Bereitstellungen minimieren.
- **Verwenden von Systemen zur Bereitstellungsverwaltung**: Verwenden Sie Systeme zur Bereitstellungsverwaltung, um Änderungen zu verfolgen und zu implementieren. Dadurch werden Fehler aufgrund von manuellen Prozessen reduziert und der Aufwand für die Bereitstellung von Änderungen verringert.
- **Testen mit begrenzten Bereitstellungen**: Führen Sie parallel zu den bestehenden Systemen Tests mit begrenzten Bereitstellungen durch, um vor der Gesamtbereitstellung zu prüfen, ob tatsächlich die gewünschten Ergebnisse erzielt werden. Führen Sie beispielsweise Tests mit Bereitstellungen in einer ausgewählten Gruppe oder in nur einem System durch.
- **Bereitstellung unter Verwendung paralleler Umgebungen**: Implementieren Sie Änderungen in parallelen Umgebungen und nehmen Sie dann eine Umstellung auf die neue Umgebung vor. Behalten Sie die bisherige Umgebung, bis die erfolgreiche Bereitstellung sichergestellt ist. Dadurch verkürzt sich die Wiederherstellungszeit, da Sie jederzeit zur vorherigen Umgebung zurückkehren können.
- **Bereitstellen häufiger, kleiner und umkehrbarer Änderungen**: Verringern Sie den Umfang einer Änderung durch häufige, kleine und umkehrbare Änderungen. Dies erleichtert die Fehlersuche und ermöglicht eine schnellere Korrektur, da die Möglichkeit besteht, eine Änderung zurückzusetzen.
- **Vollständige Automatisierung von Integration und Bereitstellung**: Automatisieren Sie den Aufbau, die Bereitstellung und die Tests des Workloads. Dadurch werden Fehler aufgrund von manuellen Prozessen reduziert und der Aufwand für die Bereitstellung von Änderungen verringert.
- **Automatisieren von Tests und Zurücksetzung**: Automatisieren Sie die Tests von bereitgestellten Umgebungen, um die gewünschten Ergebnisse sicherzustellen. Automatisieren Sie die Zurücksetzung auf einen zuvor bekanntermaßen funktionierenden Zustand, wenn die gewünschten Ergebnisse nicht erzielt werden. So können Sie die Wiederherstellungszeit minimieren und verringern Fehler, die durch manuelle Prozesse entstehen.

## OPS 5 Wie bringen Sie in Erfahrung, ob Sie für die Unterstützung eines Workloads bereit sind?

Bewerten Sie die betriebliche Bereitschaft Ihres Workloads, Prozesse und Verfahren sowie Ihrer Mitarbeiter, damit Sie die betrieblichen Risiken im Zusammenhang mit Ihrer Workload genau kennen.

Bewährte Methoden:

- **Sicherstellen des Know-how der Mitarbeiter**: Nutzen Sie einen Mechanismus, mit dem Sie prüfen können, ob Sie über ausreichend geschulte Mitarbeiter verfügen, die die betrieblichen Anforderungen unterstützen können. Schulen Sie Ihre Mitarbeiter und passen Sie die Mitarbeiterkapazität entsprechend an, damit Sie stets einen effektiven Support anbieten können.
- **Sicherstellen einer konsistenten Prüfung der betrieblichen Bereitschaft**: Sorgen Sie dafür, dass Ihre Bereitschaft für den Betrieb eines Workloads auf konsistente Art und Weise geprüft wird. Die Prüfung muss mindestens die betriebliche Bereitschaft der Teams und des Workloads sowie Sicherheitsaspekte umfassen. Implementieren Sie Prüfungsaktivitäten im Code und lösen Sie gegebenenfalls eine automatisierte Überprüfung als Reaktion auf Ereignisse aus, um Konsistenz und eine hohe Ausführungsgeschwindigkeit zu gewährleisten. Außerdem können Sie dadurch Fehler verringern, die durch manuelle Prozesse entstehen.
- **Verwenden von Runbooks für die Ausübung von Verfahren**: Runbooks sind dokumentierte Verfahren, die ein bestimmtes Ergebnis verfolgen. Durch die Dokumentation von Verfahren in Runbooks schaffen Sie die Voraussetzung für die einheitliche und schnelle Reaktion auf gut bekannte Ereignisse. Implementieren Sie Runbooks als Code und lösen Sie gegebenenfalls die Ausführung von Runbooks als Reaktion auf Ereignisse aus, um Konsistenz zu gewährleisten und Reaktionen zu beschleunigen. Außerdem können Sie dadurch Fehler verringern, die durch manuelle Prozesse entstehen.
- **Verwenden von Playbooks zur Ermittlung von Problemen**: Playbooks sind dokumentierte Prozesse für die Untersuchung von Problemen. Durch die Dokumentation der Untersuchungsabläufe in Playbooks schaffen Sie die Voraussetzung für eine einheitliche und schnelle Reaktion auf Fehlerszenarien. Implementieren Sie Playbooks als Code und lösen Sie gegebenenfalls die Ausführung von Playbooks als Reaktion auf Ereignisse aus, um Konsistenz zu gewährleisten und Reaktionen zu beschleunigen. Außerdem können Sie dadurch Fehler verringern, die durch manuelle Prozesse entstehen.
- **Treffen fundierter Entscheidungen für die Bereitstellung von Systemen und Änderungen**: Bewerten Sie die Fähigkeiten des Teams zur Unterstützung des Workloads und die Einhaltung der Governance durch den Workload. Wägen Sie diese Aspekte gegen die Vorteile der Bereitstellung ab, wenn Sie vor der Entscheidung stehen, ob Sie ein System umstellen oder eine Änderung in der Produktion vornehmen sollten. Beschäftigen Sie sich eingehend mit den Vorteilen und Risiken, damit Sie fundierte Entscheidungen treffen können.

# Betrieb

## OPS 6 Wie können Sie den Zustand Ihres Workloads beurteilen?

Definieren, erfassen und analysieren Sie Workload-Metriken, um einen Einblick in Workload-Ereignisse zu erhalten. Dies ist wichtig, damit Sie bei Bedarf entsprechende Maßnahmen ergreifen können.

Bewährte Methoden:

- **Ermitteln von wichtigen Leistungskennzahlen**: Ermitteln Sie auf Basis der gewünschten geschäftlichen und kundenspezifischen Ergebnisse wichtige Leistungskennzahlen (Key Performance Indicators, KPIs). Bewerten Sie zur Messung des Workload-Erfolgs KPIs.
- **Definieren von Workload-Metriken**: Definieren Sie Workload-Metriken für die Analyse der Erfüllung von KPIs. Definieren Sie Workload-Metriken für die Analyse des Workload-Zustands. Bewerten Sie Metriken, um festzustellen, ob der Workload die gewünschten Ergebnisse erzielt, und um den Zustand des Workloads zu beurteilen.
- **Erfassen und Analysieren von Workload-Metriken**: Unterziehen Sie die Metriken regelmäßigen proaktiven Überprüfungen, um Trends ermitteln und feststellen zu können, wo gegebenenfalls geeignete Maßnahmen ergriffen werden müssen.
- **Festlegen von Ausgangswerten für Workload-Metriken**: Legen Sie Ausgangswerte für Metriken fest, um erwartete Werte als Grundlage für den Vergleich und die Ermittlung von Komponenten mit unter- oder überdurchschnittlicher Leistung bereitzustellen.
- **Lernen erwarteter Aktivitätsmuster für den Workload**: Legen Sie Muster für die Workload-Aktivität fest, um festzustellen, wann das Verhalten von den erwarteten Werten abweicht, so dass Sie bei Bedarf angemessen reagieren können.
- **Alarm bei gefährdeten Workload-Ergebnissen**: Lösen Sie einen Alarm aus, wenn die Workload-Ergebnisse gefährdet sind, damit Sie bei Bedarf angemessen reagieren können.
- **Alarm bei festgestellten Workload-Anomalien**: Lösen Sie einen Alarm aus, wenn Workload-Anomalien festgestellt werden, damit Sie bei Bedarf angemessen reagieren können.
- **Prüfen der Erreichung von angestrebten Ergebnissen und der Wirksamkeit von KPIs und Metriken** : Erstellen Sie eine Ansicht Ihrer Workload-Operationen auf Geschäftsebene, mit der Sie schnell feststellen können, ob Sie die Anforderungen erfüllen, und welche Bereiche verbessert werden müssen, um die Geschäftsziele zu erreichen. Prüfen Sie die Wirksamkeit von KPIs und Metriken und überarbeiten Sie diese gegebenenfalls.

## OPS 7 Wie können Sie den Zustand Ihrer Operationen beurteilen?

Definieren, erfassen und analysieren Sie Metriken für Operationen, um einen Einblick in Ereignisse rund um Ihre operativen Abläufe zu erhalten. Dies ist wichtig, damit Sie bei Bedarf entsprechende Maßnahmen ergreifen können.

Bewährte Methoden:

- **Ermitteln von wichtigen Leistungskennzahlen**: Ermitteln Sie auf Basis der gewünschten geschäftlichen und kundenspezifischen Ergebnisse wichtige Leistungskennzahlen (Key Performance Indicators, KPIs). Bewerten Sie zur Messung des Erfolgs von Operationen KPIs.
- **Definieren von Metriken für Operationen**: Definieren Sie operationsspezifische Metriken für die Analyse der Erfüllung von KPIs. Definieren Sie operationsspezifische Metriken, um den Zustand der Operationen beurteilen zu können. Bewerten Sie Metriken, um festzustellen, ob die Operationen die gewünschten Ergebnisse erzielen, und um den Zustand der Operationen zu beurteilen.
- **Erfassen und Analysieren der operationsspezifischen Metriken**: Unterziehen Sie die Metriken regelmäßigen proaktiven Überprüfungen, um Trends ermitteln und feststellen zu können, wo gegebenenfalls geeignete Maßnahmen ergriffen werden müssen.
- **Festlegen von Ausgangswerten für operationsspezifische Metriken**: Legen Sie Ausgangswerte für Metriken fest, um erwartete Werte als Grundlage für den Vergleich und die Ermittlung von Prozessen mit unter- oder überdurchschnittlicher Leistung bereitzustellen.
- **Lernen erwarteter Aktivitätsmuster für Operationen**: Legen Sie Ausgangswerte für Metriken fest, um erwartete Werte als Vergleichsgrundlage bereitzustellen.
- **Alarm bei gefährdeten Ergebnissen von Operationen**: Lösen Sie einen Alarm aus, wenn die operationsspezifischen Ergebnisse gefährdet sind, damit Sie bei Bedarf angemessen reagieren können.
- **Alarm bei festgestellten Anomalien von Operationen**: Lösen Sie einen Alarm aus, wenn Anomalien bei Operationen festgestellt werden, damit Sie bei Bedarf angemessen reagieren können.
- **Prüfen der Erreichung von angestrebten Ergebnissen und der Wirksamkeit von KPIs und Metriken** : Erstellen Sie eine Ansicht Ihrer operationsspezifischen Aktivitäten auf Geschäftsebene, mit der Sie schnell feststellen können, ob Sie die Anforderungen erfüllen, und welche Bereiche verbessert werden müssen, um die Geschäftsziele zu erreichen. Prüfen Sie die Wirksamkeit von KPIs und Metriken und überarbeiten Sie diese gegebenenfalls.

### OPS 8 Wie bewältigen Sie Workload- und operationsspezifische Ereignisse?

Erarbeiten und prüfen Sie Verfahren für die Reaktion auf Ereignisse, um Beeinträchtigungen für Ihren Workload zu minimieren.

Bewährte Methoden:

- **Verwenden von Prozessen für die Bewältigung von Ereignissen, Vorfällen und Problemen**: Implementieren Sie Prozesse zur Behandlung von beobachteten Ereignissen, Ereignissen, die ein Eingreifen erfordern (Vorfälle) und Ereignissen, die ein Eingreifen erfordern und entweder wiederholt auftreten oder derzeit nicht beseitigt werden können (Probleme). Verwenden Sie diese Prozesse, um die Auswirkungen dieser Ereignisse auf das Unternehmen und Ihre Kunden zu minimieren, indem Sie rechtzeitige und zielgerichtete Reaktionen sicherstellen.
- **Verwenden eines Prozesses für die Ursachenanalyse**: Erarbeiten Sie ein Verfahren, um die Ursache eines Ereignisses zu ermitteln und zu dokumentieren. Damit können Sie Abhilfemaßnahmen entwickeln, um ein erneutes Auftreten einzudämmen oder gänzlich zu verhindern, und Verfahren für eine rasche und wirksame Reaktion erstellen. Kommunizieren Sie die Ursache, soweit erforderlich, auf die jeweiligen Zielgruppen zugeschnitten.
- **Implementieren eines Prozesses für jeden Alarm**: Legen Sie für jedes Ereignis, für das Sie einen Alarm auslösen, eine klar definierte Reaktion (Runbook oder Playbook) mit einem eigens dafür angegebenen Besitzer fest. Dies gewährleistet eine effektive und schnelle Reaktion auf Betriebsereignisse und verhindert, dass aktionsrelevante Ereignisse aufgrund weniger wichtiger Benachrichtigungen übersehen werden.
- **Priorisieren von betrieblichen Ereignissen auf Basis der Auswirkung auf das Unternehmen**: Stellen Sie sicher, dass bei mehreren Ereignissen, die eine Intervention erfordern, zuerst diejenigen angegangen werden, die für das Unternehmen die größte Tragweite haben. Zu den Auswirkungen können beispielsweise Todesfälle oder Verletzungen, finanzielle Verluste oder Rufschädigung bzw. Vertrauensverlust gehören.
- **Definieren von Eskalationspfaden**: Definieren Sie Eskalationspfade in Ihren Runbooks und Playbooks und legen Sie auch fest, was eine Eskalation auslöst. Erarbeiten Sie zudem Verfahren für die Eskalation. Weisen Sie jeder Aktion explizit Besitzer zu, um effektive und schnelle Reaktionen auf betriebliche Ereignisse zu gewährleisten.
- **Ermöglichen von Push-Benachrichtigungen**: Kommunizieren Sie direkt mit Ihren Benutzern (beispielsweise per E-Mail oder SMS), wenn die von ihnen genutzten Services betroffen sind oder wenn die Services wieder ordnungsgemäß funktionieren, damit die Benutzer entsprechende Maßnahmen ergreifen können.
- **Bekanntgeben des Status über Dashboards**: Stellen Sie Dashboards zur Verfügung, die auf die jeweilige Zielgruppe zugeschnitten sind (z. B. interne technische Teams, Führungskräfte und Kunden), um diese über den aktuellen Betriebsstatus des Unternehmens zu informieren und interessante Metriken bereitzustellen.
- **Automatisieren von Reaktionen auf Ereignisse**: Automatisieren Sie Reaktionen auf Ereignisse, um Fehler zu reduzieren, die durch manuelle Prozesse entstehen, und um schnelle und konsistente Reaktionen zu gewährleisten.

# Verbesserung

## OPS 9 Wie können Sie Operationen weiterentwickeln?

Kalkulieren Sie Zeit und Ressourcen für kontinuierliche schrittweise Verbesserungen ein, damit sich die Effektivität und Effizienz Ihrer Operationen ständig weiterentwickeln.

Bewährte Methoden:

- **Implementieren eines Prozesses für die kontinuierliche Verbesserung**: Bewerten und priorisieren Sie regelmäßig Verbesserungsmöglichkeiten, um die Maßnahmen dort zu intensivieren, wo sie den größten Nutzen bringen.
- **Implementieren von Feedbackschleifen**: Nehmen Sie Feedbackschleifen in Ihre Verfahren und Workloads auf, um die Ermittlung von Problemen und Bereichen mit Verbesserungspotenzial zu erleichtern.
- **Definieren von Verbesserungsfaktoren**: Ermitteln Sie Verbesserungsfaktoren, um das Potenzial besser bewerten und priorisieren zu können.
- **Prüfen von Erkenntnissen**: Überprüfen Sie Ihre Analyseergebnisse und Reaktionen mit fachbereichsübergreifenden Teams und Geschäftsverantwortlichen. Schaffen Sie mithilfe dieser Prüfungen ein allgemeines Verständnis, ermitteln Sie weitere Auswirkungen und legen Sie einen Maßnahmenkatalog fest. Passen Sie die Reaktionen bei Bedarf an.
- **Prüfungen von operationsspezifischen Metriken**: Führen Sie regelmäßig teamübergreifend mit Teilnehmern aus verschiedenen Unternehmensbereichen nachträgliche Analysen der operationsspezifischen Metriken durch. Ermitteln Sie mithilfe dieser Prüfungen Verbesserungspotenziale sowie mögliche Maßnahmen und teilen Sie diese Erkenntnisse auch anderen mit.
- **Dokumentieren und Weitergeben von Erkenntnissen**: Dokumentieren Sie die Erkenntnisse aus den betrieblichen Aktivitäten und geben Sie diese weiter, damit Sie sie sowohl intern als auch teamübergreifend nutzen können.
- **Einplanen von Zeit für Verbesserungen**: Reservieren Sie Zeit und Ressourcen innerhalb Ihrer Prozesse, um kontinuierliche, schrittweise Verbesserungen zu ermöglichen.

# Sicherheit

## Identity and Access Management

### SEC 1 Wie verwalten Sie Anmeldeinformationen und die Authentifizierung?

Anmeldeinformationen und Authentifizierungsmechanismen umfassen Passwörter, Tokens und Schlüssel, die entweder direkt oder indirekt Zugriff in Ihren Workload gewähren. Schützen Sie Anmeldeinformationen durch entsprechende Mechanismen, um das Risiko einer unbeabsichtigten oder böswillligen Verwendung zu reduzieren.

Bewährte Methoden:

- **Definieren der Anforderungen an Identity and Access Management (IAM)**: Die Identity and Access Management-Konfigurationen müssen definiert werden, um die organisatorischen, rechtlichen und Compliance-Anforderungen zu erfüllen.
- **Sicherer AWS-Stammbenutzer**: Sichern Sie den AWS-Stammbenutzer durch MFA, nicht durch Zugriffsschlüssel, und beschränken Sie die Verwendung, um Ihr AWS-Konto zu sichern.
- **Erzwingen der Verwendung der Multi-Factor Authentication**: Erzwingen Sie die Multi-Factor Authentication (MFA) mit Software- oder Hardwaremechanismen, um eine zusätzliche Zugriffssteuerung bereitzustellen.
- **Automatisches Erzwingen von Zugriffskontrollen**: Erzwingen Sie Zugriffskontrollen durch automatische Tools und durch Benachrichtigungen bei Unregelmäßigkeiten. Dadurch können Sie Ihren Anforderungen für die Verwaltung von Anmeldeinformationen entsprechen.
- **Integrieren mit einem zentralen Verbundanbieter**: Führen Sie eine Integration mit einem Partneridentitätsanbieter oder Verzeichnisservice durch, um alle Benutzer an einem zentralen Ort zu authentifizieren. Dadurch verringert sich die Anforderung für mehrere Anmeldeinformationen und der Verwaltungsaufwand.
- **Erzwingen von Passwortanforderungen**: Erzwingen Sie Richtlinien für Mindestlänge, Komplexität und Wiederverwendung von Passwörtern, um sich vor Brute-Force- und anderen Passwortangriffen zu schützen.
- **Regelmäßiges Ändern von Anmeldeinformationen**: Ändern Sie regelmäßig Anmeldeinformationen, um das Risiko einer Verwendung alter Anmeldeinformationen durch nicht autorisierte Systeme oder Benutzer zu verringern.
- **Regelmäßige Prüfung von Anmeldeinformationen**: Prüfen Sie Anmeldeinformationen, um sicherzustellen, dass die definierten Kontrollen (z. B. MFA) erzwungen und die Anmeldeinformationen regelmäßig geändert werden und dass die entsprechende Zugriffsebene vorhanden ist.

## SEC 2 Wie kontrollieren Sie den Zugriff durch Personen?

Kontrollieren Sie den Zugriff durch Personen, indem Sie Mechanismen implementieren, die sich an definierten Geschäftsanforderungen orientieren. Dadurch reduzieren Sie das Risiko und die Auswirkung eines nicht autorisierten Zugriffs. Dies gilt für berechtigte Benutzer und Administratoren Ihres AWS-Kontos sowie für Endbenutzer Ihrer Anwendung.

Bewährte Methoden:

- **Definieren von Anforderungen an den Zugriff durch Personen**: Definieren Sie klare Anforderungen für den Zugriff durch Benutzer basierend auf dem Tätigkeitsbereich, um das Risiko durch nicht benötigte Berechtigungen zu verringern.
- **Gewähren von minimal erforderlichen Berechtigungen**: Gewähren Sie Benutzern nur die von Ihnen definierten minimal erforderlichen Berechtigungen, um das Risiko eines nicht autorisierten Zugriffs zu reduzieren.
- **Zuweisen eindeutiger Anmeldeinformationen für jede Person**: Anmeldeinformationen werden nicht von mehreren Benutzern gemeinsam genutzt, um die Trennung von Benutzern und die Nachvollziehbarkeit sicherzustellen.
- **Verwalten von Anmeldeinformationen anhand des Benutzerlebenszyklus**: Integrieren Sie die Zugriffsverwaltung in den Benutzerlebenszyklus. Setzen Sie beispielsweise einen Benutzer außer Betrieb, um nicht verwendete und nicht benötigte Anmeldeinformationen zu sperren, wenn ein Benutzer das Unternehmen verlässt oder eine andere Rolle im Unternehmen übernimmt.
- **Automatisches Verwalten von Anmeldeinformationen**: Durch das automatische Verwalten von Anmeldeinformationen erzwingen Sie minimal erforderliche Berechtigungen und deaktivieren nicht verwendete Anmeldeinformationen. Automatisieren Sie die Überprüfung, Berichterstellung und Verwaltung des Lebenszyklus von Benutzern.
- **Gewähren von Zugriff durch Rollen oder Verbund**: Verwenden Sie IAM-Rollen statt IAM-Benutzer oder statische Zugriffsschlüssel. Damit ermöglichen Sie einen sicheren kontenübergreifenden Zugriff und das Einrichten von Verbundbenutzern.

## SEC 3 Wie kontrollieren Sie den programmgesteuerten Zugriff?

Kontrollieren Sie den programmgesteuerten oder automatischen Zugriff mit entsprechend definiertem, eingeschränktem und getrenntem Zugriff, um das Risiko eines nicht autorisierten Zugriffs zu verringern. Der programmgesteuerte Zugriff umfasst den internen Zugriff auf Ihren Workload sowie den Zugriff auf AWS-Ressourcen.

Bewährte Methoden:

- **Definieren der Anforderungen an den programmgesteuerten Zugriff**: Definieren Sie klare Anforderungen für den automatischen oder programmgesteuerten Zugriff, um das Risiko durch nicht benötigte Berechtigungen zu verringern.
- **Gewähren von minimal erforderlichen Berechtigungen**: Gewähren Sie dem automatischen oder programmgesteuerten Zugriff nur die von Ihnen definierten minimal erforderlichen Berechtigungen, um das Risiko eines nicht autorisierten Zugriffs zu reduzieren.
- **Automatisches Verwalten von Anmeldeinformationen**: Durch das automatische Verwalten von Anmeldeinformationen erzwingen Sie minimal erforderliche Berechtigungen und deaktivieren nicht verwendete Anmeldeinformationen. Automatisieren Sie die Überprüfung, Berichterstellung und Verwaltung der dynamischen Authentifizierung.
- **Zuweisen eindeutiger Anmeldeinformationen für jede Komponente**: Anmeldeinformationen werden nicht von mehreren Komponenten gemeinsam genutzt, um die Trennung und die Nachvollziehbarkeit sicherzustellen. Verwenden Sie beispielsweise unterschiedliche IAM-Rollen für AWS Lambda-Funktionen und EC2-Instances.
- **Gewähren von Zugriff durch Rollen oder Verbund**: Verwenden Sie IAM-Rollen oder einen Verbund statt IAM-Benutzer oder statische Zugriffsschlüssel. Damit ermöglichen Sie einen sicheren programmgesteuerten Zugriff.
- **Implementieren der dynamischen Authentifizierung**: Anmeldeinformationen werden von einem Service oder System dynamisch abgerufen und regelmäßig geändert.

# Aufdeckende Kontrollen

## SEC 4 Wie erkennen und untersuchen Sie Sicherheitsereignisse?

Erfassen und analysieren Sie Ereignisse mithilfe von Protokollen und Kennzahlen, um Einblick zu erhalten. Ergreifen Sie Maßnahmen bei Sicherheitsereignissen und potenziellen Bedrohungen, um Ihren Workload zu schützen.

Bewährte Methoden:

- **Definieren der Anforderungen an Protokolle**: Definieren Sie die Anforderungen an Aufbewahrung und Zugriffssteuerung für Protokolle, um die organisatorischen, rechtlichen und Compliance-Anforderungen zu erfüllen.
- **Definieren der Anforderungen an Kennzahlen**: Durch das Erfassen von Kennzahlen und das Definieren von Ausgangswerten können Sie Einblicke in potenzielle Sicherheitsbedrohungen erhalten.
- **Definieren der Anforderungen an Benachrichtigungen**: Definieren Sie, wer Benachrichtigungen erhalten soll und wie die betreffenden Personen mit diesen Benachrichtigungen verfahren sollen.
- **Konfigurieren der Service- und Anwendungsprotokollierung**: Konfigurieren Sie die Protokollierung im gesamten Workload, einschließlich Anwendungsprotokolle, AWS-Serviceprotokolle und Ressourcenprotokolle.
- **Zentrale Analyse von Protokollen**: Alle Protokolle sollten zentral gesammelt und automatisch analysiert werden, um Anomalien und Indikatoren von böswilligen Aktivitäten oder einer Kompromittierung zu erkennen.
- **Automatische Benachrichtigung bei Schlüsselindikatoren**: Schlüsselindikatoren, einschließlich sicherheitsrelevante Kennzahlen und Ereignisse, müssen überwacht werden und automatische Benachrichtigungen bei Erreichen bestimmter Schwellenwerte auslösen.
- **Entwickeln von Untersuchungsprozessen**: Entwickeln Sie Prozesse zur Untersuchung verschiedener Ereignistypen, einschließlich Eskalationspfade für Prozesse bei Reaktionen auf Vorfälle.

## SEC 5 Wie wehren Sie sich gegen neue Sicherheitsbedrohungen?

Bleiben Sie bei den AWS Best Practices und Best Practices der Branche sowie bei Informationen zu Bedrohungen auf dem Laufenden, um sich über neue Risiken im Klaren zu sein. Dadurch haben Sie die Möglichkeit, ein Gefahrenmodell zu erstellen, um entsprechende Kontrollen zum Schutz Ihres Workloads zu ermitteln, zu priorisieren und zu implementieren.

Bewährte Methoden:

- **Auf dem Laufenden sein bei organisatorischen, rechtlichen und Compliance-Anforderungen**: Bleiben Sie bei organisatorischen, rechtlichen und Compliance-Anforderungen auf dem Laufenden, um Ihre Sicherheitsausrichtung entsprechend anpassen zu können.
- **Auf dem Laufenden sein bei Best Practices im Bereich Sicherheit**: Bleiben Sie bei den AWS Best Practices und Best Practices der Branche im Bereich Sicherheit auf dem Laufenden, um den Schutz des Workloads weiterzuentwickeln.
- **Auf dem Laufenden sein bei Sicherheitsbedrohungen**: Entwickeln Sie ein Verständnis für Angriffsvektoren, indem Sie sich über die neuesten Sicherheitsbedrohungen auf dem Laufenden halten. Dadurch können Sie aufdeckende und vorbeugende Kontrollen implementieren.
- **Regelmäßiges Bewerten von neuen Sicherheitsservices und -funktionen**: Bewerten Sie Sicherheitsservices von AWS und APN-Partnern, einschließlich neuer Funktionen zur Einschränkung des Risikos von Bedrohungen.
- **Definieren und Priorisieren von Risiken anhand eines Gefahrenmodells**: Verwenden Sie ein Gefahrenmodell, um potenzielle Bedrohungen zu ermitteln und diese in einer aktuelle Liste zu pflegen. Priorisieren Sie Bedrohungen, die auf Ihre Situation zutreffen, und passen Sie Ihre Sicherheitsausrichtung entsprechend an, um darauf reagieren zu können.
- **Implementieren von neuen Sicherheitsservices und -funktionen**: Führen Sie Sicherheitsservices und -funktionen ein, um Kontrollen zum Schutz des Workloads zu implementieren.

# Schutz der Infrastruktur

## SEC 6 Wie schützen Sie Ihre Netzwerke?

Öffentliche und private Netzwerke erfordern mehrere Ebenen der Abwehr, um Schutz vor externen und internen netzwerkbasierten Bedrohungen zu bieten.

Bewährte Methoden:

- **Definieren der Anforderungen an den Netzwerkschutz**: Definieren Sie Kontrollen zum Schutz Ihrer Netzwerke, die Ihre organisatorischen, rechtlichen und Compliance-Anforderungen erfüllen.
- **Eingrenzen des Gefahrenpotenzials**: Grenzen Sie das Gefahrenpotenzial des Workloads im Internet und in internen Netzwerken ein, indem Sie nur den minimal erforderlichen Zugriff zulassen.
- **Automatische Konfigurationsverwaltung**: Erzwingen und validieren Sie sichere Konfigurationen automatisch. Verwenden Sie dazu einen Service oder ein Tool zur Konfigurationsverwaltung, um das menschliche Fehlerpotenzial zu verringern.
- **Automatischer Netzwerkschutz**: Automatisieren Sie Schutzmechanismen, um ein selbstverteidigendes Netzwerk bereitzustellen, das auf Threat Intelligence und Erkennung von Anomalien beruht.
- **Implementieren von Prüfung und Schutz**: Prüfen und filtern Sie den Datenverkehr auf Anwendungsebene. Verwenden Sie dazu beispielsweise eine Webanwendungsfirewall, um sich vor Bedrohungen zu schützen.
- **Kontrollieren des Datenverkehrs auf allen Ebenen**: Kontrollieren Sie den eingehenden und ausgehenden Datenverkehr und verhindern Sie Datenverlust. Amazon Virtual Private Cloud (VPC) stellt dazu Sicherheitsgruppen, Netzwerk-Zugriffskontrolllisten und Subnetze bereit. Erwägen Sie für AWS Lambda das Ausführen in Ihrer privaten VPC, um den Datenverkehr zu kontrollieren.

## SEC 7 Wie schützen Sie Ihre Datenverarbeitungsressourcen?

Datenverarbeitungsressourcen in Ihrem Workload erfordern mehrere Ebenen der Abwehr zum Schutz vor externen und internen Bedrohungen. Zu den Datenverarbeitungsressourcen zählen EC2-Instances, Container, AWS Lambda-Funktionen, Datenbankservices, IoT-Geräte und mehr.

Bewährte Methoden:

- **Definieren der Anforderungen an den Schutz der Datenverarbeitung**: Definieren Sie Kontrollen zum Schutz Ihrer Datenverarbeitungsressourcen, die Ihre organisatorischen, rechtlichen und Compliance-Anforderungen erfüllen.
- **Suchen von Schwachstellen und Anwenden von Patches**: Suchen Sie regelmäßig nach Schwachstellen in Ihrer Codebasis und Infrastruktur und wenden Sie Patches an, um sich vor neuen Bedrohungen zu schützen.
- **Automatische Konfigurationsverwaltung**: Erzwingen und validieren Sie sichere Konfigurationen automatisch. Verwenden Sie dazu einen Service oder ein Tool zur Konfigurationsverwaltung, um das menschliche Fehlerpotenzial zu verringern.
- **Automatischer Schutz der Datenverarbeitung**: Automatisieren Sie die Abwehr mit einem Eindringschutz, einschließlich eines Schutzes vor unbekannten Bedrohungen. Nutzen Sie dafür beispielsweise virtuelle Patches.
- **Verringern der Angriffsfläche**: Verringern Sie die Angriffsfläche, u. a. durch Härten von EC2-Betriebssystemen und Konfigurieren von Containern und Serverless-Ressourcen, um das Gefahrenpotenzial einzugrenzen.
- **Implementieren von verwalteten Services**: Implementieren Sie Services zum Verwalten von Ressourcen, z. B. Amazon RDS, AWS Lambda und Amazon ECS, um Sicherheitswartungsaufgaben zu reduzieren.

# Datenschutz

## SEC 8 Wie klassifizieren Sie Ihre Daten?

Die Klassifizierung stellt eine Methode dar, um Daten anhand von Vertraulichkeitsstufen zu kategorisieren. Ziel dabei ist, geeignete Schutz- und Aufbewahrungskontrollen zu bestimmen.

Bewährte Methoden:

- **Definieren der Anforderungen an die Datenklassifizierung**: Definieren Sie die Anforderungen an die Datenklassifizierung, die Ihre organisatorischen, rechtlichen und Compliance-Anforderungen erfüllen
- **Definieren von Datenschutzkontrollen**: Schützen Sie Daten entsprechend ihrer Vertraulichkeitsstufe. Sichern Sie beispielsweise öffentlich zugängliche Daten laut den Best Practices und vertrauliche Daten durch zusätzliche Kontrollen.
- **Implementieren von Datenidentifikation**: Klassifizieren Sie Daten mit leicht identifizierbaren Indikatoren. Verwenden Sie beispielsweise Tags für Amazon S3-Buckets und -Objekte, die die Daten in den Buckets klassifizieren.
- **Automatische Identifikation und Klassifizierung**: Automatisieren Sie die Identifikation und Klassifizierung von Daten, um das menschliche Fehlerpotenzial zu verringern.
- **Ermitteln von Datentypen**: Achten Sie auf die Datentypen in Ihrem Workload, damit Sie entsprechende Kontrollen implementieren können, die die organisatorischen, rechtlichen und Compliance-Anforderungen erfüllen.

### SEC 9 Wie schützen Sie Ihre ruhenden Daten?

Um den Schutz von ruhenden Daten zu gewährleisten, müssen Anforderungen definiert und Kontrollmechanismen, einschließlich einer Verschlüsselung, implementiert werden. Dadurch lässt sich das Risiko eines nicht autorisierten Zugriffs oder eines Datenverlusts reduzieren.

Bewährte Methoden:

- **Definieren der Anforderungen an die Verwaltung und den Schutz von ruhenden Daten**: Definieren Sie die Anforderungen an die Verwaltung und den Schutz von ruhenden Daten, wie Verschlüsselung und Datenaufbewahrung, um die organisatorischen, rechtlichen und Compliance-Anforderungen zu erfüllen.
- **Implementieren einer sicheren Schlüsselverwaltung**: Verschlüsselungsschlüssel müssen an einem sicheren Ort gespeichert und mit strenger Zugriffskontrolle geändert werden. Verwenden Sie dazu beispielsweise einen Schlüsselverwaltungsservice wie AWS Key Management Service. Erwägen Sie die Verwendung verschiedener Schlüssel, um unterschiedliche Datenklassifizierungsstufen voneinander zu trennen und um den Anforderungen an die Aufbewahrung zu entsprechen.
- **Erzwingen einer Verschlüsselung bei ruhenden Daten**: Erzwingen Sie die definierten Verschlüsselungsanforderungen anhand der neuesten Standards und Best Practices zum Schutz Ihrer ruhenden Daten.
- **Erzwingen einer Zugriffskontrolle**: Erzwingen Sie eine Zugriffskontrolle mit minimal erforderlichen Berechtigungen und Mechanismen, einschließlich Datensicherungen, Isolierung und Versionsverwaltung, zum Schutz Ihrer ruhenden Daten. Achten Sie dabei darauf, welche Ihrer Daten öffentlich zugänglich sind.
- **Bereitstellen von Mechanismen, die den direkten Zugriff auf Daten verhindern**: Unterbinden Sie den direkten Zugriff auf vertrauliche Daten durch Personen. Hierzu können Sie beispielsweise ein Dashboard statt eines direkten Zugriffs auf einen Datenspeicher verwenden und Tools für die indirekte Verwaltung von Daten bereitstellen.

## SEC 10 Wie schützen Sie Ihre Daten bei der Übertragung?

Um den Schutz von Daten bei der Übertragung zu gewährleisten, müssen Anforderungen definiert und Kontrollmechanismen, einschließlich einer Verschlüsselung, implementiert werden. Dadurch lässt sich das Risiko eines unberechtigten Zugriffs auf Daten oder einer Offenlegung von Daten reduzieren.

Bewährte Methoden:

- **Definieren der Anforderungen an den Schutz von Daten bei der Übertragung**: Definieren Sie die Anforderungen an den Schutz von Daten bei der Übertragung, wie Verschlüsselungsstandards, anhand der Datenklassifizierung, um die organisatorischen, rechtlichen und Compliance-Anforderungen zu erfüllen. Zu den Best Practices zählen das Verschlüsseln und Authentifizieren des gesamten Datenverkehrs sowie das Erzwingen der neuesten Standards und Verschlüsselungsverfahren.
- **Implementieren einer sicheren Schlüssel- und Zertifikatverwaltung**: Speichern Sie Verschlüsselungsschlüssel und Zertifikate an einem sicheren Ort und rotieren Sie sie unter strenger Zugriffssteuerung. Zu diesem Zweck eignet sich ein Zertifikatverwaltungsservice wie AWS Certificate Manager.
- **Erzwingen einer Verschlüsselung bei der Übertragung**: Erzwingen Sie die definierten Verschlüsselungsanforderungen anhand der neuesten Standards und Best Practices, um Ihre organisatorischen, rechtlichen und Compliance-Anforderungen zu erfüllen.
- **Automatisches Erkennen eines Datenlecks**: Setzen Sie Tools oder Erkennungsmechanismen ein, die automatisch erkennen, wenn versucht wird, Daten außerhalb festgelegter Grenzen zu verschieben. Damit lässt sich beispielsweise ein Datenbanksystem erkennen, das Daten auf einen unbekannten Host kopiert.
- **Authentifizieren der Netzwerkkommunikation**: Überprüfen Sie die Identität der Kommunikation mithilfe von Protokollen wie Transport Layer Security (TLS) oder IPsec, um das Risiko der Manipulation oder des Verlusts von Daten zu reduzieren.

# Vorfallreaktion

## SEC 11 Wie reagieren Sie auf einen Vorfall?

Auf Sicherheitsvorfälle vorbereitet zu sein, ist entscheidend, um diese rasch untersuchen und darauf entsprechend reagieren zu können. Dadurch sind Sie in der Lage, mögliche Unterbrechungen der Geschäftsabläufe zu minimieren.

Bewährte Methoden:

- **Ermitteln von wichtigen personellen und externen Ressourcen**: Ermitteln Sie interne und externe Mitarbeiter und Ressourcen, die bei Auftreten eines Vorfalls reagieren können.
- **Ermitteln von Tools**: Ermitteln Sie AWS-, Partner- und Open-Source-Tools, mit denen Ihr Unternehmen auf einen Vorfall reagieren kann.
- **Erarbeiten von Plänen für die Reaktion auf Vorfälle**: Erstellen Sie Pläne für die Reaktion auf Vorfälle. Beginnen Sie mit den wahrscheinlichsten Szenarien für Ihren Workload und Ihr Unternehmen. Diese Pläne sollten Vorgehensweisen zur internen und externen Kommunikation und Eskalation enthalten.
- **Automatische Eingrenzung**: Automatisieren Sie die Eingrenzung eines Vorfalls, um die Reaktionszeiten und Auswirkungen auf Ihr Unternehmen zu reduzieren.
- **Ermitteln forensischer Kapazitäten**: Ermitteln Sie die verfügbaren forensischen Untersuchungskapazitäten, einschließlich externer Spezialisten.
- **Zugriff vor der Bereitstellung**: Stellen Sie sicher, dass das Sicherheitspersonal über die geeigneten Zugriffsberechtigungen in AWS vor der Bereitstellung verfügt, damit bei einem Vorfall eine entsprechende Reaktion erfolgen kann.
- **Vorabbereitstellen von Tools**: Stellen Sie sicher, dass die richtigen Tools in AWS für das Sicherheitspersonal vorab bereitgestellt wurden, damit bei einem Vorfall eine entsprechende Reaktion erfolgen kann.
- **Üben des Ernstfalls**: Führen Sie regelmäßig eine Übung des Ernstfalls durch (Simulation), arbeiten Sie daraus gewonnene Erkenntnisse in die Pläne ein und verbessern Sie kontinuierlich Reaktionen und Pläne.

# Zuverlässigkeit

## Grundlagen

### REL 1 Wie verwalte ich Service Limits?

Standardmäßig vorhandene Service Limits verhindern, dass Sie versehentlich mehr Ressourcen bereitstellen, als Sie benötigen. Auch die Anzahl der Aufrufe von API-Vorgängen ist begrenzt, um Services vor Missbrauch zu schützen. Wenn Sie AWS Direct Connect verwenden, ist der Umfang der über jede Verbindung übertragbaren Datenmenge begrenzt. Bei Nutzung von AWS Marketplace-Anwendungen ist wichtig, deren Einschränkungen zu kennen. Auch bei Webservices oder Software-as-a-Service von Drittanbietern ist wichtig, dass Sie deren Limits kennen.

Bewährte Methoden:

- **Bezüglich Limits bewusst, werden aber nicht verfolgt**: Sie sind sich bezüglich vorhandener Limits bewusst, verfolgen diese derzeit aber nicht.
- **Überwachen und Verwalten von Limits**: Bewerten Sie Ihre potenzielle Nutzung, erhöhen Sie Ihre regionalen Limits entsprechend und planen Sie eine steigende Nutzung ein.
- **Automatisiertes Überwachen und Verwalten von Limits**: Implementieren Sie Tools, um vor dem Erreichen von Schwellenwerten benachrichtigt zu werden. Wichtig ist ein Verteilungsmechanismus zur Benachrichtigung einer verantwortlichen Gruppe, bis Anfragen zur Limiterhöhung automatisiert werden können.
- **Berücksichtigen fester Service Limits durch die Architektur**: Beziehen Sie unveränderliche Service Limits in die Architektur ein.
- **Sicherstellen eines ausreichenden Spielraums für einen Failover zwischen dem aktuellen Service Limit und der maximalen Nutzung**: Eine ausgefallene Ressource kann bis zu ihrer ordnungsgemäßen Beendigung weiterhin zu Limits zählen. Stellen Sie sicher, dass etwaige Überschneidungen ausgefallener Ressourcen mit deren Ersatz bis zur Beendigung der ausgefallenen Ressourcen durch die Limits abgedeckt sind. Berücksichtigen Sie bei der Berechnung des Spielraums auch den Ausfall einer Availability Zone.
- **Verwalten von Service Limits für alle relevanten Konten und Regionen**: Wenn Sie mehrere AWS-Konten oder -Regionen verwenden, ist es wichtig, dass Sie in allen Umgebungen, in denen Sie Ihre Produktions-Workloads ausführen, dieselben Limits anfordern.

## REL 2 Wie verwalte ich meine Netzwerktopologie?

Anwendungen können in einer oder mehreren Umgebungen vorhanden sein: in Ihrer bestehenden Rechenzentrumsinfrastruktur sowie in öffentlichen Cloud-Infrastrukturen, die wahlweise öffentlich oder privat zugänglich sind. Wichtig für die Ressourcennutzung in der Cloud sind Netzwerküberlegungen wie die Konnektivität innerhalb und zwischen Systemen, die Verwaltung öffentlicher und privater IP-Adressen, sowie die Namensauflösung.

Bewährte Methoden:

- **Sicherstellen einer hochverfügbaren Konnektivität zwischen privaten IP-Adressen in öffentlichen Clouds und der lokalen Umgebung**: Nutzen Sie zwischen separat bereitgestellten privaten IP-Adressbereichen mehrere AWS Direct Connect (DX)-Schaltungen und mehrere VPN-Tunnel. Verwenden Sie für eine hohe Verfügbarkeit mehrere DX-Standorte. Wenn Sie mehrere AWS-Regionen nutzen, benötigen Sie in mindestens zwei Regionen auch mehrere DX-Standorte. Erwägen Sie gegebenenfalls AWS Marketplace-Appliances zur Beendigung von VPNs. Stellen Sie bei Verwendung von AWS Marketplace-Appliances redundante Instances bereit, um eine hohe Verfügbarkeit in verschiedenen Availability Zones zu gewähren.
- **Bereitstellen einer hochverfügbaren Netzwerkkonnektivität für die Benutzer der Workload**: Verwenden Sie ein hochverfügbares DNS, CloudFront, API Gateway, Load Balancing sowie einen Reverse-Proxy als öffentlichen Endpunkt Ihrer Anwendung. Erwägen Sie gegebenenfalls AWS Marketplace-Appliances für Load Balancing oder Proxying.
- **Erzwingen von sich nicht überschneidenden privaten IP-Adressbereichen in mehreren privaten Adressbereichen, mit denen sie verbunden sind**: Die einzelnen IP-Bereiche Ihrer VPCs dürfen bei einem Peering oder einer Verbindung über VPNs nicht in Konflikt stehen. Dies gilt auch für die private Konnektivität zu Ihren lokalen Umgebungen und anderen Cloud-Anbietern. Sie müssen bei Bedarf private IP-Bereiche zuweisen können.
- **Berücksichtigung von Erweiterungen und Verfügbarkeit bei der Zuweisung von IP-Adressen für Subnetze**: Die einzelnen IP-Adressbereiche für Amazon VPC müssen ausreichend groß sein, um die Anforderungen einer Anwendung zu erfüllen. Dabei sind zukünftige Erweiterungen und Zuweisungen von IP-Adressen zu Subnetzen in verschiedenen Availability Zones zu berücksichtigen. Dies betrifft Load Balancer, AWS Lambda-Funktionen, EC2-Instances sowie containerbasierte Anwendungen. Halten Sie darüber hinaus IP-Adressen für mögliche zukünftige Erweiterungen bereit.

# Änderungsmanagement

### REL 3 Wie gut ist Ihr System bei Bedarfsänderungen anpassbar?

Ein skalierbares System bietet die Elastizität, Ressourcen automatisch entsprechend dem aktuellen Bedarf hinzuzufügen oder zu entfernen.

Bewährte Methoden:

- **Automatisches Beschaffen von Ressourcen beim Skalieren von Workloads**: Nutzen Sie automatisch skalierbare Services wie Amazon S3, Amazon CloudFront, Amazon Auto Scaling und AWS Lambda. Sie können die Skalierung auch mit Tools von Drittanbietern und AWS SDKs automatisieren.
- **Bereitstellen von Ressourcen bei Erkennung eines Engpasses innerhalb einer Workload**: Ressourcen werden manuell skaliert, um die Verfügbarkeit sicherzustellen.
- **Manuelles Bereitstellen von Ressourcen bei Erkennung eines demnächst steigenden Bedarfs einer Workload**: Manuelles Skalieren der Rechen- und Speicherkapazität anhand von Bedarfsprognosen
- **Durchführen von Lasttests der Workload**: Messen Sie anhand von Lasttests, ob die Skalierung den Workload-Anforderungen gerecht wird.

### REL 4 So überwachen Sie Ihre Ressourcen

Protokolle und Kennzahlen sind wertvolle Tools, um einen Einblick in den Zustand Ihrer Workloads zu gewinnen. Sie können Ihren Workload so konfigurieren, dass Protokolle und Kennzahlen überwacht und bei Über- oder Unterschreiten von Schwellenwerten oder signifikanten Ereignissen Benachrichtigungen gesendet werden. Im Idealfall sollte sich der Workload bei einem Fehler oder einem unterschrittenen Leistungsschwellenwert automatisch selbst reparieren oder entsprechend skalieren.

Bewährte Methoden:

- **Überwachen des Workloads auf allen Ebenen**: Überwachen Sie die Ebenen des Workloads mit Amazon CloudWatch oder Tools von Drittanbietern. AWS-Services können Sie mit dem Personal Health Dashboard überwachen.
- **Senden von Benachrichtigungen basierend auf der Überwachung**: Sorgen Sie dafür, dass bei signifikanten Ereignissen die entsprechenden Organisationen benachrichtigt werden.
- **Automatisieren von Reaktionen bei Ereignissen**: Automatisieren Sie bei Erkennung von Ereignissen erforderliche Maßnahmen, wie etwa den Austausch fehlerhafter Komponenten.
- **Durchführen regelmäßiger Prüfungen**: Überprüfen Sie regelmäßig, ob der Workload zuverlässig hinsichtlich signifikanter Ereignissen und Änderungen überwacht wird, um die Architektur und die Implementierung zu bewerten.

### REL 5 So implementieren Sie Änderungen

Unkontrollierte Änderungen in Ihrer Umgebung machen es schwierig, die Auswirkung einer Änderung vorherzusagen. Kontrollierte Änderungen an bereitgestellten Ressourcen und Workloads sind erforderlich, um sicherzustellen, dass die Workloads und die Betriebsumgebung bekannte Software ausführen und auf vorhersagbare Weise durch Patches aktualisiert oder ersetzt werden können.

Bewährte Methoden:

- **Durchführen geplanter Änderungen**: Bereitstellungen und das Patching erfolgen nach einem dokumentierten Verfahren.
- **Automatisieren von Änderungen**: Bereitstellungen und das Patching werden automatisiert.

## Fehlerverwaltung

### REL 6 So sichern Sie Ihre Daten

Sichern Sie Daten, Anwendungen und Betriebsumgebungen (Betriebssysteme samt der darin ausgeführten Anwendungen), um Anforderungen hinsichtlich der mittleren Reparaturdauer (Mean Time to Repair, MTTR) sowie des Wiederherstellungszeitpunkts (Recovery Point Objective, RPO) zu erfüllen.

Bewährte Methoden:

- **Identifizieren aller zu sichernden Daten und diese sichern oder die Daten aus Quellen reproduzieren**: Sichern Sie wichtige Daten mit Amazon S3, Amazon EBS-Snapshots oder Drittanbietersoftware. Wenn die Daten zur Einhaltung des RPO aus Quellen reproduziert werden können, ist möglicherweise keine Sicherung erforderlich.
- **Automatisieren von Datensicherungen oder der Datenreproduktion aus Quellen**: Automatisieren Sie Sicherungen oder die Reproduktion aus Quellen mithilfe von AWS-Funktionen (z. B. Amazon RDS- und Amazon EBS-Snapshots, Versionen in Amazon S3 usw.), AWS Marketplace-Lösungen oder Lösungen von Drittanbietern.
- **Verifizieren der Sicherungsintegrität und -verfahren durch regelmäßiges Wiederherstellen der Daten**: Überprüfen Sie mit einem Wiederherstellungstest, ob sich mit Ihrem Sicherungsverfahren die Wiederherstellungsdauer und der Widerherstellungszeitpunkt einhalten lassen.
- **Schützen und Verschlüsseln von Sicherungen oder für die Reproduzierbarkeit der Daten aus einer sicheren Quelle sorgen**: Es ist wichtig, dass Sie Zugriffe anhand der Authentifizierung und Autorisierung etwa mit AWS IAM erkennen und mittels Verschlüsselung Verletzungen der Datenintegrität feststellen können.

### REL 7 Wie stellen Sie die Systemverfügbarkeit bei Komponentenfehlern sicher?

Wenn Ihre Workloads implizit oder explizit eine hohe Verfügbarkeit sowie eine kurze mittlere Reparaturzeit (Mean Time to Recovery, MTTR) erfordern, ist es wichtig, dass sie ausfallsicher sind und verteilt ausgeführt werden.

Bewährte Methoden:

- **Überwachen aller Ebenen des Workloads auf Fehler**: Überwachen Sie den Systemzustand kontinuierlich, und melden Sie Funktionsminderungen und Komplettausfälle.
- **Implementieren lose gekoppelter Abhängigkeiten**: Abhängigkeiten etwa zwischen Warteschlangensystemen, Streaming-Systemen, Workflows und Load Balancern sind lose gekoppelt.
- **Implementieren einer ordnungsgemäßen Funktionsminderung, um harte Abhängigkeiten in weiche zu ändern**: Wenn eine Komponente über nicht funktionsfähige Abhängigkeiten verfügt, werden diese von der Komponente selbst nicht als solches gemeldet. Sie kann Anfragen weiter in eingeschränkter Form verarbeiten.
- **Automatisieren der gesamten Wiederherstellung aufgrund von technologischen Einschränkungen in Teilen oder der gesamten Workload, die einen einzelnen Standort erforderlich machen**: Elemente des Workloads können nur in einer Availability Zone oder einem Rechenzentrum ausgeführt werden. Dadurch muss der Workload auf der Basis spezieller Wiederherstellungsziele komplett neu erstellt und implementiert werden.
- **Bereitstellen des Workloads an mehreren Standorten**: Verteilen Sie die Workload-Last auf mehrere Availability Zones und AWS-Regionen (z. B. DNS, ELB, Application Load Balancer und API Gateway). Die Standorte können so vielfältig wie nötig sein.
- **Automatische Reparatur auf allen Ebenen**: Sorgen Sie nach einer Fehlererkennung dafür, dass dieser automatisch behoben wird.
- **Senden von Benachrichtigungen bei Ereignissen, die die Verfügbarkeit beeinträchtigen**: Bei Erkennung signifikanter Ereignisse werden Benachrichtigungen gesendet, selbst wenn der Fehler automatisch behoben wurde.

### REL 8 So testen Sie die Ausfallsicherheit

Ermitteln Sie anhand von Tests der Ausfallsicherheit Ihres Workloads latente Bugs, die erst während der Produktion auftreten. Führen Sie diese Tests regelmäßig durch.

Bewährte Methoden:

- **Verwenden von Playbooks für unvorhergesehene Fehler**: Sie haben Playbooks für unvorhergesehene Fehlerszenarien, mit deren Hilfe Sie die Ursache ermitteln und Strategien zur Prävention oder Schadenminimierung entwickeln können.
- **Durchführen von Ursachenanalysen und Weitergeben der Ergebnisse**: Untersuchen Sie Systemfehler basierend auf signifikanten Ereignissen, um die Architektur zu bewerten und die Ursache zu ermitteln. Etablieren Sie eine Kommunikationsmethode, um andere bei Bedarf über die Ergebnisse zu informieren.
- **Simulieren von Fehlern zum Testen der Ausfallsicherheit**: Testen Sie Fehler regelmäßig, um sicherzustellen, dass diese erfolgreich behoben werden.
- **Regelmäßiges Abhalten von Gamedays**: Üben Sie im Rahmen regelmäßiger Gamedays Notfallmaßnahmen mit den in tatsächliche Fehlerszenarien involvierten Mitarbeitern.

### REL 9 So planen Sie die Notfallwiederherstellung

Die Notfallwiederherstellung ist wichtig, um gesicherte Daten bei Bedarf wiederherzustellen. Ihre Definition der Ziele, Ressourcen, Standorte und Funktionen der Daten sowie deren Ausführung müssen den Vorgaben für die Wiederherstellungsdauer (RTO) und den Wiederherstellungszeitpunkt (RPO) entsprechen.

Bewährte Methoden:

- **Definieren von Wiederherstellungszielen bei Ausfällen und Datenverlusten**: Für den Workload gelten eine Wiederherstellungsdauer (Recovery Time Objective, RTO) und ein Wiederherstellungszeitpunkt (Recovery Point Objective, RPO).
- **Erfüllen der Wiederherstellungsziele mit definierten Wiederherstellungsstrategien**: Zum Erfüllen der Ziele wurde eine Notfallwiederherstellungsstrategie definiert.
- **Testen der implementierten Notfallwiederherstellung**: Testen Sie regelmäßig den Failover zur Notfallwiederherstellung, um sicherzustellen, dass die Wiederherstellungsdauer und der Wiederherstellungszeitpunkt eingehalten werden.
- **Verwalten von Konfigurationsabweichungen bei allen Änderungen**: Stellen Sie sicher, dass die AMIs und die Systemkonfiguration am Standort oder in der Region, in der eine Notfallwiederherstellung erforderlich sein könnte, auf dem aktuellen Stand sind. Prüfen Sie außerdem die Limits der AWS-Services.
- **Automatisieren der Wiederherstellung**: Automatisieren Sie die Systemwiederherstellung mit Tools von AWS oder Drittanbietern.

# Leistungseffizienz

## Auswahl

### PERF 1 Was ist bei der Wahl einer leistungsfähigen Architektur zu beachten?

Oft sind mehrere Ansätze erforderlich, um eine optimale Leistung für einen Workload zu erzielen. Architektonisch gute Systeme umfassen mehrere Lösungen und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung.

Bewährte Methoden:

- **Verfügbare Services und Ressourcen verstehen**: Informieren Sie sich über die breite Auswahl an Services und Ressourcen, die Ihnen auf AWS zur Verfügung stehen. Finden Sie heraus, welche Services und Konfigurationsoptionen für Ihren Workload relevant sind, und erfahren Sie, wie Sie damit eine optimale Leistung erzielen.
- **Prozess für die Architekturwahl definieren**: Nutzen Sie interne Erfahrungen und Kenntnisse zu AWS oder ziehen Sie externe Ressourcen heran, z. B. veröffentlichte Anwendungsbeispiele, relevante Dokumentation oder Whitepapers, um einen Prozess zum Wählen von Ressourcen und Services zu definieren. Dies könnte beispielsweise ein Prozess sein, der das Experimentieren und Benchmarking unterschiedlicher Services unterstützt, die für Ihren Workload relevant sein könnten.
- **Kosten und Budgets in Entscheidungen einbeziehen**: Für Workloads gelten oft Budgets, die nicht überschritten werden dürfen. Das Budget ist ein kritischer Aspekt beim Sicherstellen eines effizienten Betriebs. Nutzen Sie beim Auswählen von Ressourcentypen und -größen interne Kostenkontrollen und berücksichtigen Sie das Budget. Stützen Sie sich dabei auf den prognostizierten Ressourcenbedarf.
- **Richtlinien und Referenzarchitekturen verwenden**: Ziehen Sie interne Richtlinien oder bestehende Referenzarchitekturen heran, um eine optimale Architektur für Ihren Workload zu wählen. Prüfen Sie, mit welchen Services und Konfigurationen sich eine möglichst hohe Leistung und Effizienz für Ihren Workload erzielen lässt.
- **Material von AWS oder einem APN-Partner verwenden**: Stützen Sie Ihre Entscheidungen auf AWS-Ressourcen wie Solutions Architects oder auf Material eines APN-Partners. Diese Ressourcen können Ihnen das Überprüfen und Ableiten von Verbesserungen für Ihre Architektur erleichtern und dazu beitragen, ein optimales Leistungsniveau zu erzielen.
- **Benchmarking vorhandener Workloads**: Führen Sie einen Benchmark-Vergleich für einen bereits bestehenden Workload durch, um sich ein Bild über die Leistung auf AWS zu verschaffen. Nutzen Sie die anhand dieser Benchmarks erfassten Daten zum Ableiten architektonischer Entscheidungen.
- **Lasttests für den Workload durchführen**: Stellen Sie die neueste Version Ihres Systems unter Verwendung unterschiedlicher Ressourcentypen und -größen auf AWS bereit. Erfassen Sie mittels Überwachung geeignete Leistungskennzahlen, die Aufschluss über Engpässe oder Kapazitätsüberschüsse geben. Ziehen Sie diese Leistungsdaten beim Entwerfen oder Verbessern Ihrer Architektur- und Ressourcenwahl heran.

## PERF 2 Was ist bei der Wahl der Computing-Lösung zu beachten?

Die optimale Computing-Lösung für ein System ist vom Anwendungsdesign sowie von Nutzungsmustern und Konfigurationseinstellungen abhängig. Architekturen verwenden mitunter unterschiedliche Computing-Lösungen für verschiedene Komponenten und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung. Die Wahl der falschen Computing-Lösung für eine Architektur kann die Leistungseffizienz schmälern.

Bewährte Methoden:

- **Verfügbare Computing-Optionen prüfen**: Analysieren Sie die Leistungsmerkmale der Ihnen zur Verfügung stehenden Computing-Optionen. Befassen Sie sich damit, wie Funktionen, Instances und Container funktionieren und welche Vor- und Nachteile sich daraus für den Workload ergeben.
- **Verfügbare Konfigurationsoptionen für Computing verstehen**: Analysieren Sie, wie die verschiedenen Optionen Ihre Workloads ergänzen und welche Konfigurationsoptionen am besten für Ihr System geeignet sind. Beispiele für diese Optionen sind Instance-Familien, Größen, Merkmale (GPU, I/O), Funktionsgrößen, Container-Instances, ein Mandant oder mehrere Mandanten usw.
- **Computing-Kennzahlen erfassen**: Eine der besten Methoden zum Bestimmen der Leistung Ihrer Systeme besteht darin, die tatsächliche Nutzung der verschiedenen Ressourcen zu erfassen und zu verfolgen. Diese Daten können dann als Grundlage für die exakte Bestimmung der Ressourcenanforderungen herangezogen werden.
- **Erforderliche Konfiguration durch Dimensionieren bestimmen**: Analysieren Sie die verschiedenen Leistungsmerkmale Ihres Workloads und bewerten Sie, wie sich diese auf Arbeitsspeicher, Netzwerk und CPU-Auslastung auswirken. Ziehen Sie diese Daten heran, um die für das Workload-Profil am besten geeigneten Ressourcen zu wählen. Beispiel: Für einen arbeitsspeicherintensiven Workload wie eine Datenbank dürften Instances der r-Familie optimal sein, während sich für einen Bursting Workload eher ein elastisches Containersystem empfiehlt, wie Amazon Elastic Container Service.
- **Verfügbare Elastizität von Ressourcen nutzen**: AWS bietet Ihnen die Flexibilität, Ressourcen dynamisch durch verschiedene Mechanismen zu erweitern oder zu reduzieren (z. B. AWS Auto Scaling, Amazon Elastic Container Service und AWS Lambda), um einer veränderten Nachfrage gerecht zu werden. In Kombination mit Computing-Kennzahlen kann ein Workload automatisch auf derartige Änderungen reagieren und die optimalen Ressourcen nutzen, um ihre Zielvorgabe zu erreichen.
- **Computing-Bedarf anhand von Kennzahlen neu bewerten**: Identifizieren Sie anhand von Kennzahlen auf Systemebene das Verhalten und die Anforderungen Ihres Workloads in einem bestimmten Zeitraum. Bewerten Sie die Anforderungen Ihres Workloads, indem Sie die verfügbaren Ressourcen mit diesen Anforderungen vergleichen. Passen Sie die Computing-Umgebung so an, dass sie dem Profil Ihres Workloads optimal entspricht. Beispiel: Im Laufe der Zeit stellen Sie vielleicht fest, dass ein System mehr Arbeitsspeicher benötigt, als anfangs gedacht. Durch einen Wechsel zu einer anderen Instance-Familie oder Größe lassen sich eventuell Leistung und Effizienz verbessern.

## PERF 3 Was ist bei der Wahl der Speicherlösung zu beachten?

Die optimale Speicherlösung für ein System richtet sich nach der Zugriffsmethode (Block, Datei oder Objekt), den Zugriffsmustern (Zufallsprinzip oder sequenziell), dem erforderlichen Durchsatz, der Zugriffshäufigkeit (online, offline, Archiv), der Aktualisierungshäufigkeit (WORM, dynamisch) sowie den Einschränkungen hinsichtlich Verfügbarkeit und Langlebigkeit. Architektonisch gute Systeme nutzen mehrere Speicherlösungen und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung und effizienten Ressourcennutzung.

Bewährte Methoden:

- **Speichermerkmale und -anforderungen verstehen**: Machen Sie sich mit den unterschiedlichen Merkmalen vertraut (z. B. Freigabefähigkeit, Dateigröße, Cache-Größe, Zugriffsmuster, Latenz, Durchsatz und Datenpersistenz). Dadurch fällt es Ihnen leichter, die Services auszuwählen, die am besten für Ihren Workload geeignet sind, wie Amazon S3, Amazon EBS, Amazon Elastic File System (Amazon EFS) und Amazon EC2-Instance-Speicher.
- **Verfügbare Konfigurationsoptionen bewerten**: Bewerten Sie die verschiedenen Merkmale und Konfigurationsoptionen und ermitteln Sie, welche Auswirkungen sie auf den Speicher haben. Finden Sie heraus, wo und wie Sie PIOPS, SSDs, magnetischen Speicher, Amazon S3, Amazon Glacier oder flüchtigen Speicher idealerweise einsetzen, um Speicherplatz und Leistung Ihres Workloads zu optimieren.
- **Zugriffsmuster und Kennzahlen in die Entscheidung einbeziehen**: Wählen und konfigurieren Sie Ihre Speichersysteme danach, wie der Workload auf Daten zugreift. Optimieren Sie die Leistung, indem Sie beispielsweise Caching-Services oder Instances wählen, die für Ihre Zugriffsmuster am besten geeignet sind. Nutzen Sie die optimale Schlüsselverteilung, wenn Sie Daten in Amazon S3 oder DynamoDB speichern, nutzen Sie Speichervolumen-Striping oder partitionieren Sie Daten basierend auf Systemmessungen. Steigern Sie die Speichereffizienz durch Verwenden von Objektspeicher wie Amazon S3 oder von Blockspeicher wie Amazon Elastic Block Store. Konfigurieren Sie die von Ihnen gewählten Speicheroptionen so, dass sie den Datenzugriffsmustern entsprechen.

### PERF 4 Was ist bei der Wahl der Datenbanklösung zu beachten?

Welche Datenbanklösung sich am besten für ein System eignet, hängt von der erforderlichen Verfügbarkeit, Konsistenz, Partitionstoleranz, Latenz, Langlebigkeit, Skalierbarkeit und Abfragefähigkeit ab. Viele Systeme nutzen für verschiedene Untersysteme unterschiedliche Datenbanklösungen und bieten verschiedene Möglichkeiten zur Leistungsoptimierung. Die Wahl der falschen Datenbanklösung und -funktionen kann die Leistungseffizienz eines Systems schmälern.

Bewährte Methoden:

- **Datenmerkmale verstehen**: Machen Sie sich mit den verschiedenen Merkmalen der Daten Ihres Workloads vertraut. Bestimmen Sie, ob der Workload Transaktionen erfordert, wie sie mit Daten interagiert, welche Leistungsanforderungen erfüllt werden müssen usw. Wählen Sie auf Grundlage dieser Daten den leistungsfähigsten Datenbankansatz für Ihren Workload aus (z. B. relationale Datenbanken, NoSQL, Data Warehouses oder In-Memory-Speicher).
- **Verfügbare Optionen prüfen**: Prüfen Sie die Services und Speicheroptionen, die im Rahmen des Auswahlprozesses für die Speichermechanismen des Workloads zur Verfügung stehen. Bestimmen Sie, wie und wann ein bestimmter Service oder ein bestimmtes System für die Datenspeicherung zu verwenden ist. Machen Sie sich mit den verfügbaren Konfigurationsoptionen vertraut, mit denen sich Leistung oder Effizienz der Datenbank weiter optimieren lassen, wie PIOPs, Arbeitsspeicher- und Computing-Ressourcen, Caching usw.
- **Kennzahlen zur Datenbankleistung erfassen**: Nutzen Sie Tools, Bibliotheken und Systeme zum Aufzeichnen von Messungen zur Datenbankleistung. Messen Sie beispielsweise die Transaktionen pro Sekunde, langsame Abfragen oder die Systemlatenz beim Aufrufen der Datenbank. Anhand dieser Daten lässt sich die Leistung Ihrer Datenbanksysteme nachvollziehen.
- **Datenspeicher nach Zugriffsmuster wählen**: Bestimmen Sie anhand der Zugriffsmuster des Workloads, welche Services und Technologien sich anbieten. Setzen Sie beispielsweise eine relationale Datenbank für Workloads ein, die Transaktionen erfordern, oder einen Schlüssel-Wert-Speicher, der einen höheren Durchsatz bietet und konsistent ist.
- **Datenspeicher nach Zugriffsmuster und Kennzahlen wählen**: Optimieren Sie anhand der Leistungsmerkmale und Zugriffsmuster die Art und Weise, in der Daten gespeichert oder abgefragt werden. So lässt sich die bestmögliche Leistung erzielen. Messen Sie, wie sich Optimierungen wie Indizierung, Schlüsselverteilung, Data Warehouse Design oder Caching-Strategien, auf die Systemleistung oder Gesamteffizienz auswirken.

## PERF 5 Was ist beim Konfigurieren der Netzwerklösung zu beachten?

Welche Netzwerklösung für ein System optimal ist, richtet sich unter anderem nach der Latenz und dem erforderlichen Durchsatz. Physische Einschränkungen wie Benutzer- oder Hardwareressourcen können durch Edge-Techniken oder Ressourcenplatzierungen behoben werden.

Bewährte Methoden:

- **Auswirkungen des Netzwerks auf die Leistung verstehen**: Analysieren Sie, wie sich Netzwerkentscheidungen auf die Leistung des Workloads auswirken. Netzwerklatenz beispielsweise beeinträchtigt oft das Benutzererlebnis. Ferner kann die Verwendung ungeeigneter Protokolle zu erhöhtem Overhead führen und die Netzwerkkapazität drosseln.
- **Verfügbare Produktoptionen verstehen**: Machen Sie sich mit den verfügbaren Servicefunktionen vertraut, mit denen sich die Netzwerkleistung optimieren lässt. Dazu gehören etwa EC2-Instance-Netzwerkfähigkeit, erweitertes Networking, Amazon EBS-optimierte Instances, Amazon S3 Transfer Acceleration sowie dynamische Inhaltsbereitstellung mit Amazon CloudFront.
- **Verfügbare Netzwerkfunktionen bewerten**: Bewerten Sie die leistungsfördernden Netzwerkfunktionen in AWS. Messen Sie die Auswirkungen der Funktionen anhand von Tests, Kennzahlen und Analysen. Nutzen Sie die verfügbaren Netzwerkfunktionen etwa zum Reduzieren von Latenz, Entfernung oder Instabilität (einschließlich latenzbasierte Weiterleitung mit Amazon Route 53, Amazon VPC-Endpunkte oder AWS Direct Connect).
- **Anzahl der Netzwerk-ACLs minimieren**: Legen Sie Ihr Netzwerk so aus, dass eine minimale Anzahl von ACLs verwendet wird und Ihre Anforderungen dennoch erfüllt werden. Zu viele ACLs können die Netzwerkleistung beeinträchtigen und Leistung oder Effizienz des Systems schmälern.
- **Verschlüsselung auslagern und Lastausgleich anwenden**: Nutzen Sie Lastausgleich, um die Terminierung von Verschlüsselung auszulagern (TLS). So lässt sich die Leistung optimieren und Datenverkehr effektiv weiterleiten. Verteilen Sie Datenverkehr auf mehrere Ressourcen oder Services, um von der durch AWS bereitgestellten Elastizität zu profitieren.
- **Leistungsfördernde Netzwerkprotokolle wählen**: Berücksichtigen Sie bei der Wahl der Protokolle für die Kommunikation zwischen Systemen und Netzwerken, wie sich diese Protokolle auf die Workload-Leistung auswirken.
- **Standort basierend auf Netzwerkanforderungen wählen**: Nutzen Sie die verfügbaren Standortoptionen (z. B. AWS-Region, Availability Zone, Platzierungsgruppen und Edge-Standorte) zum Reduzieren von Netzwerklatenz oder Verbessern des Durchsatzes.
- **Netzwerkkonfiguration basierend auf Kennzahlen optimieren**: Ziehen Sie die erfassten und analysierten Daten heran, um informierte Entscheidungen zum Optimieren Ihrer Netzwerkkonfiguration zu treffen. Messen Sie die Auswirkungen dieser Änderungen und treffen Sie Ihre zukünftigen Entscheidungen auf der Grundlage dieser Ergebnisse.

# Prüfung

## PERF 6 Wie profitiert Ihren Workload von neuen Releases?

Bei der Architektur von Workloads sind die Wahlmöglichkeiten begrenzt. Im Laufe der Zeit werden jedoch immer wieder neue Technologien und Ansätze zur Leistungsoptimierung des Workloads entwickelt.

Bewährte Methoden:

- **Neue Ressourcen und Services nutzen**: Prüfen Sie, inwieweit neue Services, Designmuster oder Produktangebote Möglichkeiten zur Leistungsoptimierung bieten. Ermitteln Sie anhand von Ad-hoc-Bewertungen, internen Diskussionen oder externen Analysen, wie sich diese positiv auf Leistung oder Effizienz des Workloads auswirken könnten.
- **Prozess zum Verbessern der Workload-Leistung definieren**: Definieren Sie einen Prozess, mit dem sich neu verfügbare Services, Designmuster, Ressourcentypen und Konfigurationen bewerten lassen. Führen Sie beispielsweise vorhandene Leistungstests an neuen Instance-Angeboten durch, um zu ermitteln, welche Verbesserungen sich hinsichtlich Leistung oder Effizienz erzielen ließen.
- **Workload-Leistung allmählich anpassen**: Nutzen Sie die aus dem Bewertungsprozess gewonnenen Informationen, um aktiv die frühzeitige Einführung neuer Services oder Ressourcen zu fördern und so Leistung oder Effizienz Ihres Workloads zu verbessern.

# Überwachung

**PERF 7 Wie lassen sich Ressourcen überwachen, um sicherzustellen, dass sie die erwartete Leistung liefern?**

Die Systemleistung kann sich mit der Zeit verschlechtern. Überwachen Sie die Systemleistung, um eine solche Verschlechterung frühzeitig zu erkennen und ihr entgegenzuwirken, etwa indem Sie interne oder externe Faktoren wie das Betriebssystem oder die Anwendungslast korrigieren.

Bewährte Methoden:

- **Leistungskennzahlen erfassen**: Erfassen Sie Leistungskennzahlen mit Amazon CloudWatch, dem Service eines Drittanbieters oder selbstverwalteten Überwachungstools. Erfassen Sie beispielsweise Datenbanktransaktionen, langsame Abfragen, I/O-Latenz, den Durchsatz von HTTP-Anforderungen, Servicelatenz und andere wichtige Daten.
- **Kennzahlen bei Eintreten von Ereignissen oder Vorfällen analysieren**: Ziehen Sie während eines Ereignisses oder Vorfalls oder als Reaktion darauf Überwachungs-Dashboards oder Berichte heran, um die Auswirkungen nachzuvollziehen und zu diagnostizieren. Diese Ansichten bieten Einblick in die Bereiche des Workloads, die nicht die erwartete Leistung liefern.
- **KPIs zum Messen der Workload-Leistung definieren**: Machen Sie diejenigen KPIs ausfindig, die Aufschluss über die ordnungsgemäße Systemleistung geben. Bei einem API-basierten Workload beispielsweise kann die Gesamtreaktionslatenz als Indikator für die Gesamtleistung fungieren. Im Falle einer E-Commerce-Website kann die Anzahl der Einkäufe als KPI herangezogen werden.
- **Alarmbasierte Benachrichtigungen mit Überwachungstool generieren**: Nachdem Sie geeignete Leistungs-KPIs definiert haben, setzen Sie ein Überwachungssystem ein, das automatisch Alarme generiert, wenn Messwerte außerhalb des erwarteten Bereichs liegen.
- **Kennzahlen regelmäßig überprüfen**: Überprüfen Sie als routinemäßige Wartungsmaßnahme oder als Reaktion auf Ereignisse oder Vorfälle, welche Kennzahlen erfasst werden. Ermitteln Sie anhand dieser Überprüfung, welche Kennzahlen für die Behebung von Problemen maßgeblich waren und welche zusätzlichen Kennzahlen hilfreich wären, um Probleme zu identifizieren, zu beheben oder zu verhindern.
- **Proaktive Überwachung und Alarmgebung**: Beheben Sie Leistungsprobleme proaktiv, indem Sie KPIs in Verbindung mit Überwachungs- und Alarmsystemen einsetzen. Beheben Sie Probleme möglichst mithilfe von Alarmen, die automatische Aktionen auslösen. Falls keine automatische Reaktion möglich ist, sollte der Alarm eskaliert werden, sodass eine manuelle Reaktion eingeleitet werden kann. Nutzen Sie beispielsweise ein System, das erwartete KPI-Werte prognostiziert und bei Überschreiten bestimmter Schwellenwerte einen Alarm ausgibt. Denkbar ist auch ein Tool, das Bereitstellungen automatisch anhält oder zurücksetzt, wenn sich KPIs außerhalb der erwarteten Werte befinden.

# Kompromisse

**PERF 8 Wie lässt sich Leistung durch Kompromisse verbessern?**

Durch aktives Einbeziehen von Kompromissen beim Gestalten von Lösungen lässt sich der optimale Ansatz einfacher bestimmen. Leistung lässt sich oft durch Zugeständnisse in anderen Bereichen verbessern, etwa bei Konsistenz, Beständigkeit, Zeit und Latenz.

Bewährte Methoden:

- **Bereiche mit kritischem Leistungsbedarf identifizieren**: Ermitteln Sie diejenigen Bereiche, in denen sich durch Steigern der Workload-Leistung positive Auswirkungen auf die Effizienz oder das Kundenerlebnis realisieren lassen. Beispiel: Eine Website mit zahlreichen Kundeninteraktionen profitiert durch Nutzen von Edge-Services wie Amazon CloudFront von einer näher am Kunden stattfindenden Inhaltsbereitstellung.
- **Designmuster und Services kennenlernen**: Holen Sie Informationen zu den verschiedenen Designmustern und Services ein, die zu Leistungsoptimierungen beitragen, und machen Sie sich mit ihnen vertraut. Ermitteln Sie im Rahmen Ihrer Analyse, welche Kompromisse in Frage kämen, um eine höhere Leistung zu erzielen. Mithilfe von Amazon ElastiCache beispielsweise lässt sich die Last auf Datenbanksystemen reduzieren. Allerdings bedarf es einer gewissen Entwicklungstätigkeit, um sicheres Caching zu implementieren oder letztendliche Datenkonsistenz in bestimmten Bereichen einzuführen.
- **Auswirkungen von Kompromissen auf Kunden und Effizienz identifizieren**: Überlegen Sie beim Bewerten von leistungsbezogenen Verbesserungen, wie sich die einzelnen Szenarien auf Kunden und Workload-Effizienz auswirken. Beispiel: Wenn die Systemleistung durch Verwenden von Schlüssel-Wert-Speicher wie Amazon DynamoDB erheblich gesteigert werden könnte, sollte auch geprüft werden, wie sich die letztendlich datenkonsistente Beschaffenheit von Amazon DynamoDB auf Kunden auswirkt.
- **Auswirkung von Leistungsoptimierungen messen**: Wenn Sie Änderungen zugunsten einer höheren Leistung vornehmen, prüfen Sie die erfassten Kennzahlen und Daten. Bestimmen Sie, wie sich die Leistungsoptimierung auf den Workload, ihre Komponenten und auf Kunden auswirkt. Anhand dieser Messungen lassen sich die dank des Kompromisses möglichen Verbesserungen einfacher nachvollziehen und Sie können feststellen, ob mit dem Kompromiss eventuell unerwünschte Nebeneffekte hervorgerufen wurden.
- **Verschiedene Leistungsstrategien anwenden**: Wenden Sie nach Möglichkeit mehrere Strategien zur Leistungsoptimierung an. Verwenden Sie beispielsweise Strategien wie Daten-Caching, um exzessive Netzwerk- oder Datenbankaufrufe zu verhindern. Verwenden Sie Lesereplikate für Datenbankmodule, um eine höhere Leserate zu erzielen. Setzen Sie möglichst Sharding und Datenkomprimierung ein, um Datenvolumen zu reduzieren und nutzen Sie Pufferung und Streaming von Ergebnissen, sobald diese verfügbar sind, um Blockieren zu vermeiden.

# Kostenoptimierung

## Ausgabenbewusstsein

### COST 1 Wie können Sie die Nutzung steuern?

Definieren Sie Richtlinien und Verfahren, um sicherzustellen, dass sich die Kosten auf dem Weg zur Erreichung Ihrer Ziele in einem angemessenen Rahmen bewegen. Durch den Einsatz eines Kontrollsystems können Sie Innovationen vorantreiben, ohne das Budget zu überschreiten.

Bewährte Methoden:

- **Entwickeln von Richtlinien auf Basis Ihrer Organisationsanforderungen**: Entwickeln Sie Richtlinien, die definieren, wie Ressourcen von Ihrer Organisation verwaltet werden. Die Richtlinien sollten sich auch mit den Kostenaspekten der Ressourcen und Workloads befassen, einschließlich Erstellung, Änderung und Außerbetriebnahme während der gesamten Lebensdauer der Ressourcen. Sie sollten auch Kostenvorgaben und Ziele für Workloads ausarbeiten.
- **Implementieren einer Kontenstruktur**: Implementieren Sie eine Kontenstruktur, die für Ihre Organisation geeignet ist. Dadurch werden die Zuweisung und Verwaltung der Kosten in der gesamten Organisation erleichtert.
- **Implementieren von Gruppen und Rollen**: Implementieren Sie Gruppen und Rollen, die sich an Ihren Richtlinien orientieren, und steuern Sie, wer in den einzelnen Gruppen (beispielsweise in den Gruppen "Entwicklung", "Test" und "Produktion") Instances und Ressourcen erstellen, ändern oder außer Betrieb nehmen darf. Dies gilt sowohl für AWS-Services als auch für Lösungen anderer Anbieter.
- **Implementieren von Kostenkontrollen**: Implementieren Sie Kontrollmechanismen, die auf den Organisationsrichtlinien sowie auf definierten Gruppen und Rollen basieren. Damit wird sichergestellt, dass die Kosten den Rahmen der festgelegten Organisationsanforderungen nicht sprengen; mithilfe von IAM-Richtlinien können Sie beispielsweise den Zugriff auf Regionen oder Ressourcentypen steuern.
- **Verfolgen des Projektlebenszyklus**: Verfolgen, bewerten und überprüfen Sie den Lebenszyklus von Projekten, Teams und Umgebungen, damit Sie keine unnötigen Ressourcen nutzen, für die Sie zahlen müssen.

### COST 2 Wie können Sie die Nutzung und Kosten überwachen?

Definieren Sie Richtlinien und Verfahren, um Ihre Kosten überwachen und richtig zuordnen zu können. Dadurch können Sie die Kosteneffizienz des Workloads bewerten und verbessern.

Bewährte Methoden:

- **Konfigurieren des AWS-Kosten- und -Nutzungsberichts**: Konfigurieren Sie den AWS-Kosten- und -Nutzungsbericht, um detaillierte Informationen zur Nutzung und Fakturierung zu erhalten.
- **Ermitteln von Kostenzuordnungskategorien**: Ermitteln Sie Organisationskategorien, die für die Kostenzuordnung innerhalb Ihrer Organisation genutzt werden können.
- **Definieren von Organisationsmetriken**: Definieren Sie die Organisationsmetriken, die für diesen Workload erforderlich sind. Beispiele für Metriken eines Workloads sind erstellte Kundenberichte oder Webseiten, die den Kunden angezeigt werden.
- **Definieren und Implementieren von Tagging**: Definieren Sie ein Tagging-Schema auf Basis der Organisation sowie Workload-Attribute und Kostenzuordnungskategorien. Implementieren Sie das Tagging für alle Ressourcen.
- **Konfigurieren von Tools für die Fakturierung und Kostenverwaltung**: Konfigurieren Sie AWS Cost Explorer und AWS-Budgets in Übereinstimmung mit Ihren Organisationsrichtlinien.
- **Berichte und Benachrichtigungen zur Kostenoptimierung**: Konfigurieren Sie AWS-Budgets, um Benachrichtigungen über die Kosten und Nutzung im Vergleich mit den Zielen zu ermöglichen. Analysieren Sie in regelmäßig abgehaltenen Besprechungen die Kosteneffizienz des betreffenden Workloads und fördern Sie das Kostenbewusstsein im Unternehmen.
- **Proaktive Überwachung der Kosten**: Implementieren Sie Tools und Dashboards zur proaktiven Überwachung der Kosten für diese Workload; begnügen Sie sich nicht damit, die Kosten und Kategorien lediglich beim Erhalt von Benachrichtigungen zu beachten. Auf diese Weise lassen sich positive Trends feststellen, die dann in der gesamten Organisation gefördert werden können.
- **Kostenzuordnung auf Basis von Workload-Metriken**: Ordnen Sie die Kosten des betreffenden Workloads anhand von Metriken oder geschäftlichen Ergebnissen zu, um die Kosteneffizienz des Workloads bewerten zu können. Implementieren Sie einen Prozess für die Analyse des AWS-Kosten- und -Nutzungsberichts mit Amazon Athena, um von genaueren Einblicken und Rückbelastungsmöglichkeiten zu profitieren.

### COST 3 Wie können Sie Ressourcen außer Betrieb nehmen?

Implementieren Sie vom Beginn bis zum Abschluss eines Projekts eine Änderungskontrolle und Ressourcenverwaltung. Auf diese Weise können Sie ungenutzte Ressourcen herunterfahren oder beenden, um Verschwendungen zu minimieren.

Bewährte Methoden:

- **Verfolgen von Ressourcen über ihre gesamte Lebensdauer hinweg**: Definieren und implementieren Sie eine Methode zur Verfolgung von Ressourcen und deren Verknüpfungen mit Systemen über ihre gesamte Lebensdauer hinweg. Mit einem entsprechenden Tagging können Sie den Workload oder Funktion der Ressource identifizieren.
- **Implementieren eines Prozesses für die Außerbetriebnahme**: Implementieren Sie einen Prozess für die Identifizierung und Außerbetriebnahme von verwaisten Ressourcen.
- **Ungeplante Außerbetriebnahme von Ressourcen**: Sie können Ressourcen auch außerplanmäßig außer Betrieb nehmen. In diesem Fall wird die Außerbetriebnahme üblicherweise durch Ereignisse wie regelmäßige Prüfungen ausgelöst und in der Regel manuell vorgenommen.
- **Automatische Außerbetriebnahme von Ressourcen**: Gestalten Sie Ihren Workload so, dass er die Beendigung von Ressourcen reibungslos handhabt, wenn Sie unkritische Ressourcen, nicht benötigte Ressourcen oder Ressourcen mit geringer Auslastung identifizieren und außer Betrieb nehmen.

# Kostengünstige Ressourcen

**COST 4 Wie können Sie die Kosten bei der Auswahl von Services einschätzen?**

Bei Amazon EC2, Amazon EBS und Amazon S3 handelt es sich um AWS-Services, die als einzelne Bausteine angeboten werden. Verwaltete Services, etwa Amazon RDS und Amazon DynamoDB, sind AWS-Services auf einer höheren Ebene oder Anwendungsebene. Wenn Sie sich für die richtigen Bausteine und verwalteten Services entscheiden, können Sie die Kosten dieses Workloads optimieren. Durch die Nutzung von verwalteten Services können Sie einen Großteil Ihres administrativen und betrieblichen Overheads reduzieren oder beseitigen und damit Kapazitäten für anwendungs- und geschäftsbezogene Aktivitäten gewinnen.

Bewährte Methoden:

- **Ermitteln der Organisationsanforderungen zur Kosteneinschätzung**: Definieren Sie gemeinsam mit den Teammitgliedern das Gleichgewicht zwischen Kostenoptimierung und anderen Säulen, wie Leistung und Zuverlässigkeit, für diese Workload.
- **Analysieren sämtlicher Komponenten dieser Workload**: Stellen Sie sicher, dass jede Workload-Komponente unabhängig von der derzeitigen Größe oder den aktuellen Kosten analysiert wird. Der Überprüfungsaufwand sollte in einem angemessenen Verhältnis zu dem potenziellen Nutzen stehen, z. B. bei einer Prüfung der derzeitigen und prognostizierten Kosten.
- **Führen Sie eine gründliche Analyse der einzelnen Komponenten durch.**: Nehmen Sie die Gesamtkosten, die der Organisation durch die einzelnen Komponenten entstehen, unter die Lupe. Betrachten Sie die Gesamtbetriebskosten unter Berücksichtigung der Betriebs- und Verwaltungskosten, insbesondere bei der Nutzung von verwalteten Services. Der Überprüfungsaufwand sollte in einem angemessenen Verhältnis zu dem potenziellen Nutzen stehen, z. B. muss die Zeit, die für die Analyse benötigt wird, den Komponentenkosten entsprechen.
- **Auswählen von Komponenten dieses Workloads zur Optimierung der Kosten im Einklang mit den Organisationsprioritäten**: Berücksichtigen Sie bei der Auswahl sämtlicher Komponenten die Kosten. Dies beinhaltet auch die Verwendung von Services auf Anwendungsebene und verwalteten Services wie etwa Amazon RDS, Amazon DynamoDB, Amazon SNS und Amazon SES zur Reduzierung der Gesamtorganisationskosten. Verwenden Sie Serverless-Lösungen und Container für die Datenverarbeitung, zum Beispiel AWS Lambda, Amazon S3 für statische Websites und Amazon ECS. Minimieren Sie Lizenzkosten mithilfe von Open-Source-Software oder Software, für die keine Lizenzgebühren anfallen. Nutzen Sie beispielsweise Amazon Linux für Datenverarbeitungs-Workloads oder migrieren Sie Datenbanken zu Amazon Aurora.
- **Durchführen einer Kostenanalyse für unterschiedliche Nutzungen im Lauf der Zeit**: Workloads können sich mit der Zeit ändern, und manche Services oder Features sind kostengünstiger, wenn sie anders genutzt werden. Wenn Sie jede Komponente im zeitlichen Verlauf und mit einer prognostizierten Nutzung analysieren, stellen Sie sicher, dass dieser Workload über ihre gesamte Lebensdauer hinweg kostengünstig bleibt.

### COST 5 Wie können Sie bei der Auswahl des Ressourcentyps und -umfangs Kostenziele erfüllen?

Stellen Sie sicher, dass Sie den richtigen Ressourcenumfang für die jeweilige Aufgabe wählen. Durch die Auswahl des kostengünstigsten Typs und Umfangs minimieren Sie Verschwendungen.

Bewährte Methoden:

- **Durchführen einer Kostenmodellierung**: Ermitteln Sie die Organisationsanforderungen und führen Sie eine Kostenmodellierung des Workloads und ihrer einzelnen Komponenten durch. Führen Sie Benchmark-Aktivitäten für den Workload unter verschiedenen prognostizierten Belastungen durch und vergleichen Sie die Kosten. Der Modellierungsaufwand sollte in einem angemessenen Verhältnis zu dem potenziellen Nutzen stehen, z. B. muss der Zeitaufwand den Komponentenkosten entsprechen.
- **Auswahl des Ressourcentyps und -umfangs auf Basis von Schätzungen**: Schätzen Sie den Ressourcenumfang oder -typ auf Basis des Workloads und Ressourcenmerkmale; zu berücksichtigen sind hier beispielsweise Datenverarbeitung, Speicher, Durchsatz oder Schreibintensität. Diese Schätzung erfolgt in der Regel unter Verwendung einer früheren Version des Workloads (z. B. einer lokalen Version), der Dokumentation oder anderer Informationsquellen über den Workload.
- **Auswahl des Ressourcentyps und -umfangs auf Basis von Metriken**: Nutzen Sie Metriken aus dem derzeit aktiven Workload für die Auswahl des richtigen Umfangs und Typs, um Kosten zu optimieren. Sorgen Sie für die richtige Bereitstellung von Durchsatz, Größe und Speicher für Services wie Amazon EC2, Amazon DynamoDB, Amazon EBS (PIOPS), Amazon RDS, Amazon EMR und Netzwerkbetrieb. Dies kann mit einer Feedbackschleife wie der automatischen Skalierung oder durch einen manuellen Prozess der Größenänderung erfolgen.

### COST 6 Wie können Sie Kosten mithilfe von Preismodellen senken?

Verwenden Sie das Preismodell, das sich für Ihre Ressourcen am besten eignet. So halten Sie die Ausgaben möglichst niedrig.

Bewährte Methoden:

- **Durchführen einer Preismodellanalyse**: Analysieren Sie den Workload mithilfe der AWS Cost Explorer-Empfehlungsfunktion für Reserved Instances.
- **Implementieren Sie unterschiedliche Preismodelle mit einer geringen Abdeckung**: Implementieren Sie reservierte Kapazität, Spot-Instances, Spot-Blöcke oder eine Spot-Flotte in der Workload, allerdings mit geringer Abdeckung, die weniger als 80 % der Gesamtempfehlungen entspricht.
- **Implementieren von Regionen auf Basis der Kosten**: Die Ressourcenpreise können je nach Region abweichen. Die Berücksichtigung der Regionskosten stellt sicher, dass Sie den niedrigsten Gesamtpreis für diesen Workload zahlen.
- **Implementieren von Preismodellen für alle Komponenten dieser Workload**: Permanent aktive Ressourcen haben eine hohe Abdeckung mit reservierter Kapazität, wobei mindestens 80 % der Empfehlungen implementiert sind. Die kurzfristige Kapazität wird für die Verwendung von Spot-Instances, Spot-Blöcken oder einer Spot-Flotte konfiguriert. On-Demand-Instances werden nur für kurzfristige Workloads verwendet, die nicht unterbrochen werden können und nicht lange genug für reservierte Kapazitäten ausgeführt werden: typischerweise 25 bis 75 % des Jahres, je nach Ressourcentyp.

### COST 7 Wie können Sie die Kosten für Datenübertragungen planen?

Damit Sie architekturbezogene Entscheidungen zur Kostenminimierung treffen können, müssen Sie unbedingt die Datenübertragungskosten einplanen und überwachen. Eine geringfügige, aber effektive Änderung an der Architektur kann Ihre Betriebskosten über einen längeren Zeitraum hinweg erheblich senken.

Bewährte Methoden:

- **Modellierung einer Datenübertragung**: Stellen Sie die Organisationsanforderungen zusammen und führen Sie eine Datenübertragungsmodellierung des Workloads und ihrer einzelnen Komponenten durch. Dadurch wird der niedrigste Kostenpunkt für die jeweiligen aktuellen Datenübertragungsanforderungen ermittelt.
- **Auswählen von Komponenten zur Optimierung der Datenübertragungskosten**: Alle Komponenten sind ausgewählt und die Architektur ist so konzipiert, dass die Datenübertragungskosten gesenkt werden. Dies umfasst auch die Verwendung von Komponenten wie WAN-Optimierung und Multi-AZ-Konfigurationen.
- **Implementieren von Services zur Senkung der Datenübertragungskosten**: Implementieren Sie Services, mit denen die Datenübertragungen reduziert werden. Sie können beispielsweise ein CDN wie Amazon CloudFront für die Übermittlung von Inhalten an Endbenutzer, Caching-Layer mit Amazon ElastiCache oder AWS Direct Connect anstelle von VPN für die Verbindung mit AWS verwenden.

# Abstimmen von Angebot und Bedarf

**COST 8 Wie können Sie das Ressourcenangebot auf den Bedarf abstimmen?**

Stellen Sie bei einem Workload mit ausgewogenen Ausgaben und Leistungen sicher, dass alles, wofür Sie bezahlen, genutzt wird, und vermeiden Sie eine erhebliche Unterauslastung der Instances. Eine verschobene Auslastungsmetrik in einer der Richtungen wirkt sich nachteilig auf Ihr Unternehmen aus, entweder im Hinblick auf die Betriebskosten (verschlechterte Leistung aufgrund von Überbelegung) oder auf die verschwendeten AWS-Ausgaben (aufgrund von Überversorgung).

Bewährte Methoden:

- **Analyse des Workload-Bedarfs**: Analysieren Sie den Bedarf des Workloads im gesamten Zeitverlauf. Stellen Sie sicher, dass die Analyse saisonale Trends berücksichtigt und die Betriebsbedingungen über die gesamte Lebensdauer des Workloads genau wiedergibt. Der Analyseaufwand sollte in einem angemessenen Verhältnis zu dem potenziellen Nutzen stehen, z. B. muss der Zeitaufwand den Workload-Kosten entsprechen.
- **Reaktive oder ungeplante Bereitstellung von Ressourcen**: Der Ressourcenbestand ändert sich aufgrund der Nachfrage, jedoch erfolgt die Bereitstellung ungeplant, in der Regel manuell, und wird durch unerwünschte Ereignisse oder Änderungen im Workload ausgelöst. Die Ressourcenbeschaffung ändert sich nur langsam und führt häufig zu einer Über- oder Unterversorgung.
- **Dynamische Bereitstellung von Ressourcen**: Ressourcen werden geplant bereitgestellt. Dies kann bedarfsorientiert sein, z. B. durch automatische Skalierung, pufferbasiert, wobei der Bedarf über den zeitlichen Verlauf verteilt ist und weniger Ressourcen insgesamt genutzt werden, oder zeitbasiert, wobei der Bedarf vorhersehbar ist und die Ressourcen auf Basis des Zeitpunkts bereitgestellt werden. Diese Methoden führen dazu, dass die Über- oder Unterversorgung am geringsten ist.

# Schrittweises Optimieren

**COST 9 Wie können Sie neue Services bewerten?**

Im Zuge der Veröffentlichung neuer Services und Funktionen durch AWS empfiehlt es sich, dass Sie Ihre bestehenden Entscheidungen zur Architektur überdenken, um sicherzustellen, dass diese weiterhin so kostengünstig wie möglich sind.

Bewährte Methoden:

- **Implementieren einer Kostenoptimierungsstelle**: Stellen Sie ein Team zusammen, das in regelmäßigen Abständen die Kosten und Nutzung in der gesamten Organisation prüft.
- **Entwickeln eines Prüfprozesses für Workloads**: Entwickeln Sie einen Prozess, der die Kriterien und den Prozess für die Workload-Prüfung definiert. Der Überprüfungsaufwand sollte in einem angemessenen Verhältnis zum potenziellen Nutzen stehen; beispielsweise ist es sinnvoll, zentrale Workloads oder Workloads mit einem Wert von mehr als 10 % der Rechnung vierteljährlich zu prüfen, während Workloads mit einem Wert von weniger als 10 % jährlich überprüft werden.
- **Prüfung und ungeplante Implementierung von Services**: Führen Sie neue Services außerplanmäßig ein.
- **Regelmäßige Prüfung und Analyse des betreffenden Workloads**: Bestehende Workloads werden gemäß vordefinierter Prozesse regelmäßig überprüft.
- **Verfolgen neuer Service-Veröffentlichungen**: Konsultieren Sie regelmäßig Experten oder APN-Partner, um zu prüfen, welche Services und Funktionen kostengünstiger sind. Lesen Sie AWS-Blogs und sonstige Informationsquellen.